ASSER PRESS

NL ARMS Netherlands Annual Review of Military Studies 2020

Deterrence in the 21st Century—Insights from Theory and Practice

Frans Osinga
Tim Sweijs *Editors*

OPEN ACCESS

Springer

NL ARMS

Netherlands Annual Review of Military Studies

Ministry of Defence

Series Information

This peer-reviewed series offers an overview of cutting-edge scientific research on military sciences drawing on scholarship from researchers at the Faculty of Military Sciences (FMS) of the Netherlands Defence Academy and colleagues around the world. Research at the Faculty is military-relevant and typically multi-disciplinary in nature. It is concerned with themes including but not limited to:

- The conduct of contemporary war
- Military strategy
- Leadership and ethics
- Military law and history
- Command and control in military operations
- Cyber security
- Operational analysis
- Navigation
- Combat systems

With NL ARMS the Netherlands Defence Academy seeks to contribute to a growing body of international comparative research in military sciences.

Editorial Office

Faculty of Military Sciences
Netherlands Defence Academy
P.O. Box 90 002
4800 PA Breda
The Netherlands

More information about this series at http://www.springer.com/series/13908

Frans Osinga · Tim Sweijs
Editors

NL ARMS Netherlands Annual Review of Military Studies 2020

Deterrence in the 21st Century—Insights from Theory and Practice

ASSER PRESS

Springer

Editors
Frans Osinga
Faculty of Military Sciences
Netherlands Defence Academy
Breda, The Netherlands

Tim Sweijs
Faculty of Military Sciences
Netherlands Defence Academy
Breda, The Netherlands

ISSN 1387-8050 ISSN 2452-235X (electronic)
NL ARMS
ISBN 978-94-6265-418-1 ISBN 978-94-6265-419-8 (eBook)
https://doi.org/10.1007/978-94-6265-419-8

Published by T.M.C. ASSER PRESS, The Hague, The Netherlands www.asserpress.nl
Produced and distributed for T.M.C. ASSER PRESS by Springer-Verlag Berlin Heidelberg

This T.M.C. ASSER PRESS imprint is published by the registered company Springer-Verlag GmbH, DE part of Springer Nature.
The registered company address is: Heidelberger Platz 3, 14197 Berlin, Germany

Foreword

This subject of this volume—deterrence—deserves, indeed demands, attention, and not just of scholars, for understanding the challenges and dynamics of deterrence is of paramount importance in today's rapidly changing international security environment. Deterrence has never gone out of fashion. It is one of the core strategic functions of any defense organization. Immediately following the end of the Cold War, NATO found itself involved in peacekeeping operations in the Balkans, which often called for coercive diplomacy and demonstrations of resolve in order to convince the warring parties to cease fighting or to stop harassing UN peacekeepers executing their UN mandate. In short, NATO aimed to deter aggression but the context this time was much different from that of the Cold War and success was often difficult to achieve in the politically constrained environment despite NATO's military superiority.

Whether terrorist groups could be deterred became a topic of intense academic and political debate following the terrorist attacks in September 2001, and much has been learned since then. And of course, following the Russian annexation of the Crimea in 2014, interstate deterrence has moved centre stage again. Western governments ponder the challenges of creating an effective nuclear and conventional deterrence posture while they are also concerned about the so-called hybrid threats including the constant intensity of cyber-attacks. Artificial intelligence and other new technologies such as autonomous weapon systems will add to the complexity and challenges of deterrence in the near future. Meanwhile insight is emerging on the specific conceptualization of deterrence; deterrence means different things for different polities, complicating deterrence dynamics in times of crisis.

This research project capitalizes on the extensive national and internal network of the Department of War Studies. The editors succeeded in bringing together a wealth of expertise for this book project as the list of authors demonstrates, including scholars from Israel, the US, Denmark, Canada, the UK, Iran, Russia, and Switzerland. The volume benefited greatly from the author's workshop the faculty organized at the Netherlands Defence Academy in Winter 2020. The contributors, spanning a variety of academic disciplines, explore deterrence in the full breadth of the concept, update and refine extant knowledge, debate novel technological

features on the strategic landscape, examine deterrence applications in nontraditional and non-Western contexts, and consider the relevance of these findings for our understanding of deterrence in theory and practice in the twenty-first century. The impressive result showcases the great scholarly value of this cross-disciplinary and cross-cultural approach.

But the relevance of this book extends beyond academia. Deterrence is an area of knowledge where theory informs policies, strategies, and behavior and those in turn inform subsequent theorizing, as various chapters in this book attest to. It is a book with direct relevance for thinking about today's security challenges, challenges that feature prominently on the policy agenda of the Netherlands Ministry of Defence, the Ministry of Foreign Affairs, and international security organizations such as NATO and the EU. If history is any guide, that will remain so for a very long time.

Breda/Den Helder, The Netherlands

Prof. Dr. Patrick Oonincx
Dean of Faculty Military Sciences
Netherlands Defence Academy

Preface

Deterrence as a distinct subfield of study recently celebrated its seventy-fifth birthday. Over the past three-quarters of a century, it has co-evolved with changing strategic conditions to address the pressing strategic challenges of the day. Over the years, it has experienced ups and downs. Periods of sustained stasis have alternated with periods of rapid development, pushed along both by critical scholarly inquiry and by professional policymaker concern. Tellingly, deterrence does not wither away but persists in the portfolio of concepts and strategies employed by nation states. Also in the third decade of the twenty-first century, its use continues to bedazzle strategists even if its efficacy under different conditions has not always been firmly established. That is why we need to continue studying deterrence—in its changing incarnations and in its adaptive applications—which provides the rationale for yet another book on deterrence.

In the context of the sizeable body of deterrence literature, we take two oft-cited articles as our point of departure. In a 2012 article, Patrick Morgan attempted to take stock of deterrence, in theory and practice, to assess where it is now and where it might be headed in security affairs'.[1] Morgan observed the cooperative nature of the relations between leading powers and observed how they had 'remained relatively cooperative and remarkably free of profound security concerns'. As a result, deterrence had become 'less central and salient', especially in the nuclear realm with nuclear weapons having been 'relegated by most nuclear powers to residual functions, primarily hedging against the possible return of serious conflicts.'[2]

At the same time the principal remaining threats, according to Morgan, were failed, weak, and rogue states alongside non-state actors. As a result, deterrence had become much more complicated and difficult to achieve. It had become more of a

[1]Patrick M. Morgan (2012) The State of Deterrence in International Politics Today, *Contemporary Security Policy*, 33:1, 85–107, 85.

[2]Ibid., 88.

'tactical resource' than a fundamental building block of a more general security strategy.[3] Deterrence was also affected by other developments, both technological and ideological. Increased precision in long-range weapons on the one hand, and the deployment of intercontinental ballistic missiles (ICBMs) with conventional warheads on the other, alongside the parallel emergence of strategic cyberattack capabilities, posed a considerable challenge to deterrence stability. Dominant states had started openly disavowing the indiscriminate use of force. Both in conceptual and in practical terms, theorists and strategists wrestled how to design emerging notions of tailored deterrence against different types of actors.

Morgan noted 'insufficient appreciation of how and why Cold War conceptions of deterrence are of limited relevance now and also of the ways in which Cold War deterrence thinking remains relevant'.[4] More specifically, he observed considerable progress in thinking about the role of deterrence in counterterrorism efforts; growing recognition of the diminished utility of nuclear deterrence; the need for more attention to the political and normative dimensions of deterrence; a rapidly expanding body of scholarship to better understand cyberspace dynamics and the logic of deterrence in this context; deficiencies in our comprehension of the challenges associated with collective deterrence and extended deterrence; and the limited inclusion of arms control perspectives in managing deterrence relationships in an interconnected world.[5]

Since Morgan's article, some of these topics have been explored in numerous articles and excellent in-depth, book-length volumes. For instance, Andreas Wenger and Alex Wilner edited a timely study on the nexus of deterrence and terrorism,[6] Lukas Kello published a great analysis on the impact of cyber capabilities on international order,[7] Kelly Greenhill and Peter Krause addressed a range of topics also highlighted by Morgan in their volume *Coercion, The Power to Hurt*,[8] and Eric Gartzke and Jon R. Lindsay have analyzed the dynamics of deterrence across traditional and new domains.[9] More recently think tanks and research institutes have produced a stream of more policy-oriented studies analyzing deterrence in the context of hybrid conflict and gray zone competition. Other scholars have explored the ramifications of emerging technologies for deterrence making use of a slowly

[3]Ibid., 89.

[4]Ibid., 85.

[5]Ibid.

[6]Andreas Wenger, Alex Wilner, *Deterring Terrorism*, Stanford University Press, Stanford, 2012.

[7]Lucas Kello, *The Virtual Weapon and International Order*, Yale University Press, Hartford, Ct, 2017.

[8]Peter Krause (eds), *Coercion, the power to hurt in international politics*, Oxford University Press, Oxford, 2018.

[9]Erik Gartzke and Jon R. Lindsay, Cross-Domain Deterrence. Strategy in an Era of Complexity, Oxford University Press, 2019.

but steadily emerging empirical database pertaining to the characteristics of such technologies.[10]

Ten years after Morgan, the use and utility of deterrence in today's strategic environment, therefore, continues to be a topic of paramount concern to scholars, strategists, and policymakers. Because of a combination of military-strategic, technological, and social–political developments, contemporary conflict actors exploit a wider gamut of coercive instruments which they apply across a wider range of domains for strategic gain. These encompass both nuclear and conventional military instruments, but also include non-military instruments of state power that are deployed in grey zone conflicts under the threshold of military violence. The prevalence of multi-domain coercion across but also beyond traditional dimensions of conflict raises an important question: what does effective deterrence look like in the twenty-first century? Answering that question requires a re-appraisal of key theoretical concepts and dominant strategies of the deterrence literature in order to assess how they hold up in today's world.

The second article that this volume takes as a point of departure is Jeffrey Knopf's article of 2010 in which he usefully distinguishes between four waves in deterrence research.[11] The initial wave of deterrence theorizing appeared after the Second World War prompted by the need to respond to a real-world problem—the invention of the atom bomb.[12] The second wave came in the late 1950s and 1960s was dominated by formal theorems that sprang from deductive reasoning and game theory.[13] Starting in the 1960s but really taking off in the 1970s, the third wave used statistical and case-study methods to empirically test deterrence theory. The case-study literature also challenged rational actor assumptions employed in

[10]To name but a few, see Michael Mazarr et al, *Gaining Competitive Advantage in the Gray Zone*, RAND, Santa Monica, 2019, at www.rand.org. Thomas G. Mahnken, et al, *Countering Comprehensive Coercion, Competitive Strategies Against Authoritarian Political Warfare*, CSBA, Washington, D.C., 2018, at www.CSBA.org; Yuna Huh Wong, et al, *Deterrence in the Age of Thinking Machines*, RAND, Santa Monica, 2020. Gregory Treverton, *Addressing Hybrid Threats*, Swedish Defence University, 2018, at www.fhs.se, Sean Monaghan, *Countering Hybrid Warfare*, MCDC, Shrivenham, 2019; Vytautas Kersanskas, *Deterrence: Proposing a more strategic approach to countering hybrid threats*, March 2020, https://www.hybridcoe.fi/publications/hybrid-coe-paper-2-deterrence-proposing-a-more-strategic-approach-to-countering-hybrid-threats/.

[11]Jeffrey W. Knopf, The Fourth Wave in Deterrence Research, Contemporary Security Policy 31, no. 1 (April 1, 2010): 1–33, https://doi.org/10.1080/13523261003640819.

[12]Robert Jervis, Deterrence Theory Revisited, *World Politics* 31, no. 2 (January 1979): 289–324, https://doi.org/10.2307/2009945.

[13]Daniel Ellsberg, The Theory and Practice of Blackmail (Santa Monica California: RAND, 1968), http://www.rand.org/pubs/papers/P3883.html; Glenn Herald Snyder, *Deterrence and Defense: Toward a Theory of National Security* (Princeton: Princeton University Press, 1961); Thomas C. Schelling, *Arms and Influence: With a New Preface and Afterword* (Yale University Press, 2008); Thomas C. Schelling, *The Strategy of Conflict* (Harvard University Press, 1981); Herman Kahn, *On Escalation: Metaphors and Scenarios*, vol. 1 (Transaction Publishers, 2009).

second-wave deterrence theory.[14] The rational actor perspective was complemented with perspectives from the psychological and decision-making literature.[15] Following the end of the Cold War, a new body of work emerged that focused on asymmetric deterrence especially in the context of the question how to deter so called rogue states and their leaders, and, post 9/11, terrorist groups.[16] Core concepts and assumptions concerning the role of credibility and reputation were reassessed in light of real world deterrence cases between Western states and political leaders such as Milosevic, Ghaddafi, and Saddam Hussein. Studies suggested that deterrence outside of the realm of nuclear peer-competition involving threats with conventional weapons in situations in which relative limited vital interests were at stake, is distinctly more complex and dynamic than traditional first and second wave assumed. Overall these four waves were partly reflective of the strategic issues of the day and partly of the dominant methodological orientation of the field.

About This Book

Our volume—and the selection of themes—mirrors many of the themes flagged by Morgan and tracks a lively debate in deterrence research from the past decade. It addresses several of these themes to assess where deterrence strategy and theory stand right now against the background of the four waves distinguished by Knopf. The individual chapters synthesize emerging insights from a wealth of literature that has been published since the time of the publication of Morgan's article. They offer fresh perspectives, reassess assumptions, review the validity of extant theories, and reflect on the implications of novel strategic developments. They do so fully cognizant of the fact that only 2 years after Morgan's article was published, the geopolitical context changed significantly, invalidating some of Morgan's comments concerning the prevailing peaceful conditions of the international security environment.

This volume, therefore, surveys the current state of the field to examine whether a fifth wave of deterrence theory is emerging—both in the Western world but also outside of it—to address the pressing strategic challenges of today. Ours is a period of considerable strategic turbulence, which in recent years has featured a renewed

[14]Alexander L. George and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice* (New York: Columbia University Press, 1974); Glenn Herald Snyder and Paul Diesing, *Conflict Among Nations: Bargaining Decision Making and System Structure in International Crises* (Princeton: Princeton University Press, 1978).

[15]Robert Jervis, *Perception and Misperception in International Politics*, 1st ed. (Princeton University Press, 1976); Jervis, "Deterrence Theory Revisited"; Richard Ned Lebow, Deterrence Failure Revisited, *International Security* 12, no. 1 (Summer 1987): 197–213; Richard Ned Lebow and Janice Gross Stein, Deterrence: The Elusive Dependent Variable, *World Politics* 42 (1990 1989): 336–69, https://doi.org/10/b3hsmx.

[16]Knopf, 2010.

emphasis on nuclear weapons used in defense postures across different theaters; a dramatic growth in the scale of military cyber capabilities and the frequency with which these are used; and rapid technological progress including the proliferation of long-range strike and unmanned systems and Artificial Intelligence (AI). These military-strategic developments occur in a polarized international system, where cooperation between leading powers on arms control regimes is breaking down, states widely make use of hybrid conflict strategies, and the number of internationalized intrastate proxy conflicts has quintupled over the past two decades.[17] Scholarly and strategic communities, both in the West and elsewhere, are updating, refining, and further developing the analytical portfolio of deterrence concepts that take into account both actor-specific and domain-specific features to address these challenges.[18]

This edited volume brings together insights from world-leading experts from three continents. It identifies the most pressing strategic issues, frames theoretical concepts, and describes new strategies. As such it offers a critical contribution to an as-of-yet nascent body of fifth wave deterrence literature.

Concepts of Deterrence: Historical, Conceptual, Conventional, Nuclear, Extended, Cross-domain

The volume is thematically structured. Following an elegant overview of the evolution of deterrence strategy and research by Sir Lawrence Freedman that concludes with a warning not to over-estimate what deterrence can be expected to achieve, seven chapters explore our understanding of familiar deterrence concepts, assumptions, and strategies. Michael Mazarr offers a synthesis of basic deterrence concepts which is impressive in both its comprehensiveness and its brevity. Sten Rynning follows on from this survey of deterrence and its challenges with an incisive analysis of how the renewed strategic competition with Russia is challenging NATO´s ability to develop a coherent deterrence strategy in light of the diversity of strategic perspectives among NATO member states. Karl Mueller informs us about extant insights on the utility of conventional deterrence and the dilemmas associated with it. Alexey Arbatov and Paul van Hooft, both focusing on the renewed prominence of nuclear weapons as deterrence instruments for great powers, respectively, address the crucial role of arms control regimes and the problematic credibility of US extended nuclear deterrence. Jörg Noll and colleagues analyze the types of deterrence expectations harbored by policy elites in three countries that border Russia and rely on NATO for an effective deterrence posture.

[17]Tim Sweijs and Danny Pronk, *Interregnum: Strategic Monitor Annual Report 2019* (The Hague, Netherlands: The Hague Centre for Strategic Studies & The Clingendael Institute, April 2019).

[18]Michael Mazarr, *Understanding Deterrence* (RAND Corporation, 2018), https://doi.org/10.7249/pe295.

The central question is to what extent their expectations coincide with NATO's deterrence strategy. Finally, Tim Sweijs and Samuel Zilincik survey the literature on cross-domain deterrence which has emerged in response to the cross-domain nature of contemporary conflict. They critically assess its theoretical logic, practical feasibility, and degree of novelty, and reflect on the insights for deterrence theory and practice that can be gained from it.

Non-Western Concepts of Deterrence

The second set of chapters offers a fascinating panorama of the ways in which deterrence is conceptualized and operationalized in different strategic cultures. Indeed, as Dmitry Adamsky and Dean Cheng both demonstrate in their respective chapters, Russian and Chinese conceptualizations of deterrence look dramatically different from their Western equivalents, which may translate into dramatic misunderstandings in the real world. Nori Katagiri in turn shows how post Second World War constitutional constraints hamper Japan's ability to mount an effective deterrence posture, demonstrating the validity of Morgan's observation of the impact of normative considerations on deterrence strategy. The ways in which particular strategic contexts shape both the nature of deterrence strategies and their effects are highlighted in two fascinating case studies. Sander Ruben Aarten details how nuclear deterrence strategies have been developed in India and Pakistan, how they have resulted in a modicum of stability, but also how the risk of nuclear escalation has not resulted in an absence of frequent conventional skirmishes. The final contribution in this exploration of non-Western concepts of deterrence is provided by Hassan Ahmadian and Payam Mohseni who explain the evolution of Iran's deterrence strategy through the enlisting of regional partners and non-state proxies such as Hezbollah against the background of Iran's distinct historical experience.

Deterrence of Non-State Actors

The subsequent set of chapters examines deterrence against non-state actors. Eitan Shamir offers an overview of various deterrence strategies against violent non-state actors and analyzes how these have been employed by Israel. Once again, like previous chapters, his argument forces us to acknowledge the limits of classical Western Cold War conceptualizations of absolute deterrence. Martijn Kitzen and Christina van Kuijck extend the application of deterrence concepts to influencing non-state actors by showing how deterrence concepts are, or can fruitfully be, applied in counter-insurgency contexts at the tactical and operational levels. Like

Shamir's chapter, their analysis also illustrates the benefits of multidisciplinary work. Shamir's includes insights from criminology and communication studies. Kitzen and van Kuijck connect deterrence studies to the literature on irregular warfare. Maarten Rothman stretches deterrence concepts into yet another, and indeed novel, terrain and considers how Russia seeks to deter democratic revolts in its neighboring countries. Peter Viggo Jakobsen completes the set in an extension of his previous original research on the use and challenges of deterrence strategies in peace operations. Such operations have often required applying pressure on recalcitrant local military commanders to prevent them from frustrating the activities of peacekeepers. Often, however, such deterrence efforts have failed, as witnessed in the Balkan crisis. In addition to explaining the minimum set of requirements for successful deterrence, Jakobsen explains how the deterring actor needs to acknowledge the different audiences—combatants, combatant allies, combatant supporters, and bystanders—as part of a comprehensive multilevel deterrence strategy.

New Instruments and Domains of Deterrence

New technologies and instruments are the subjects of the fourth part of the book. Francesco Giumelli very informatively brings together the sanctions and deterrence literature. Sanctions often precede and accompany deterrent efforts with military threats, yet they are generally ill-understood in terms of what the aims of sanctions are, and what is to be expected of them. Giumelli details how the use of sanctions has evolved since the 1990s from comprehensive sanctions to targeted sanctions both to mitigate the humanitarian suffering associated with comprehensive sanctions and to be more effective in coercing target actors. Another deterrence instrument, a defensive one this time, is explored by Cees van Doorn and Theo Brinkel. Their chapter homes in on the concept of resilience as a form of deterrence by denial, which has been popping up in policy papers of Western governments and the EU since 2014 as a response to the increasing threat of hybrid threats. Using the aftermath of the tragic downing of Flight MH/17 in 2014 as a case study, they argue that the transparent approach taken by the Dutch government in various ways boosted societal resilience which made Russian influence efforts less effective. Whether resilience is also the solution to mitigate the risk of cyberattacks is uncertain. The key question whether such attacks can be deterred at all, and to what extent cyber-capabilities can be employed effectively as an instrument of deterrence, is the topic of a rich survey by Max Smeets and Stefan Soesanto. They canvass the various strands of arguments that have appeared in the growing scholarly body on cyber deterrence and outline future directions for cyber deterrence research. Assessing the impact on deterrence is also the key aim of Alex Wilner and Casey Babb in their analysis of the potential impact of AI on deterrence strategy and strategic stability.

Even more than the debate on cyber deterrence, the discussion of the impacts of AI largely takes place in an empirical vacuum as the technology is still immature. The fact that many analysts expect that AI is likely to have a major impact on international stability, warrants the inclusion of this in-depth, and balanced yet exploratory assessment of the impact of AI on deterrence dynamics.

Deterrence and Decision-making: Rationality, Psychology, and Emotions

Rationality, or the problem of that assumption, is the core theme of the final part of the book. Roy Lindelauf re-assesses game-theoretical assumptions. He reminds us of its utility, captures recent refinements that have been proposed by scholars and discusses the potential impact of AI-enhanced command and control processes on the dynamics of deterrence. Tom Bijlsma returns to third-wave deterrence research in his chapter in which he surveys and concisely summarizes the ways the human mind actually filters incoming data, turns it into information and reaches decisions. His synthesis of insights from cognitive sciences, including prospect theory, substantiates once again that deterrence theorists and strategists should never assume that targets of deterrence will respond according to rational actor model precepts. That notion becomes even more explicit in the original and innovative analysis provided by Samuel Zilincik and Isabelle Duyvesteyn of emerging insights into the effects of emotions on decision-making processes. As Frank Harvey briefly touched upon in 2011 with respect to deterring authoritarian leaders, it seems that emotions such as honor, prestige, or the fear of losing face may actually result in enhanced risk taking.[19] But even when actors behave rationally in a crisis, larger organizations may not, or, there may be confusion what deterrent response is warranted, executed by which organization, and governed by which legal framework. This legal and bureaucratic perspective has been discussed relatively infrequently in deterrence studies. Yet, as analyses of the Cuban Missile Crisis have convincingly demonstrated, organizational dynamics are crucial.[20] These days, when NATO, the EU, and various European governments discuss a whole of society approach to counter unwanted external hybrid influence activities, they assume governmental agencies can and will cooperate to create cohesive responses. Paul Ducheine and Peter Pijpers complete this part of the book by looking into that thorny issue.

[19]Keith B. Payne (2011) Understanding Deterrence, *Comparative Strategy*, 30:5, 393–427.

[20]Graham Allison and Philip Zelikow (1971), *Essence of Decision Explaining the Cuban Missile Crisis*, Harper Collins Publishers, 1971.

Conclusion: Insights from Theory and Practice

The conclusion synthesizes key insights that have emerged from the different contributions, evaluates their relevance to deterrence theory and practice, and considers to what extent research and current strategic issues give credence to the notion that a fifth wave is emerging. On that basis, it offers an appraisal of contemporary deterrence thinking and it outlines avenues for future research going forward.

Breda, The Netherlands

Frans Osinga
Tim Sweijs

Acknowledgements

This book greatly benefited from the Author Workshop *Deterrence in the 21st Century* held at the Netherlands Defence Academy in the Castle of Breda from 9–11 February 2020. We would like to express our thanks in particular to Thania Patrick of the War Studies Department at the Defence Academy, who was instrumental in arranging all the logistical and administrative details. We also express our thanks to Royce Zaadnoordijk, who managed to mold all the draft chapters into the format required by our publisher. Thanks also to Arthur Eveleens, Lecturer English Language at the Defence Academy, for his assistance. Finally, we thank the RAND Corporation, the Carnegie Foundation (Moscow) and Oxford University Press for allowing us to include three chapters that had been published previously as standalone papers.

Contents

Editors and Contributors

About the Editors

Air Commodore Prof. Dr. Frans Osinga is Professor of Military Operational Art and Sciences, Chair of the War Studies Department at the Netherlands Defence Academy (Faculty of Military Sciences). He is also the Special in War Studies at Leiden University. A graduate of the Royal Military Academy, the Advanced Staff Course of the Netherlands Defence College and a former F-16 pilot, he obtained his Ph.D. at Leiden University in 2005 following a tour as the MoD Senior Research Fellow at the Clingendael Institute. He is the author of more than 70 publications.

Dr. Tim Sweijs is the Director of Research at The Hague Centre for Strategic Studies and a Research Fellow at the Netherlands Defence Academy. He is the initiator, creator, and author of numerous studies, methodologies, and tools for horizon scanning, early warning, conflict analysis, national security risk assessment, and strategy and capability development. He serves as an Adviser Technology, Conflict and National Interest to the UK Government's Stabilisation Unit. Tim holds degrees in War Studies (Ph.D., M.A.), International Relations (M.Sc.) and Philosophy (B.A.) from King's College, London and the University of Amsterdam.

Contributors

Sander Ruben Aarten Netherlands Defence Academy, Breda, The Netherlands

Dmitry Adamsky School of Government, Diplomacy and Strategy, IDC Herzliya University, Herzliya, Israel

Hassan Ahmadian Harvard Kennedy School, Belfer Center for Science and International Affairs, Cambridge, MA, USA; The Center for Strategic Research, University of Tehra, Tehran, Iran

Alexey Arbatov Center for International Security, Primakov National Research Institute of World Economy and International Relations (IMEMO), Moscow, Russia

Casey Babb The Norman Paterson School of International Affairs, Carleton University, Ottawa, Canada

Tom Bijlsma Netherlands Defence Academy, Breda, The Netherlands

Osman Bojang Netherlands Defence Academy, Breda, The Netherlands

Theo Brinkel Netherlands Defence Academy, Breda, The Netherlands

Dean Cheng Asian Studies Center, Davis Institute for National Security and Foreign Policy, The Heritage Foundation, Washington, D.C., USA

Paul Ducheine Netherlands Defence Academy (NLDA), Breda, The Netherlands; University of Amsterdam, Amsterdam, The Netherlands

Isabelle Duyvesteyn Institute of History, Leiden University, Leiden, The Netherlands

Lawrence Freedman Department of War Studies, King's College London, London, UK

Francesco Giumelli University of Groningen, Groningen, The Netherlands

Peter Viggo Jakobsen The Institute for Strategy, The Royal Danish Defence College, Copenhagen, Denmark; Center for War Studies, University of Southern Denmark, Odense, Denmark

Nori Katagiri Saint Louis University, St. Louis, USA

Martijn Kitzen Netherlands Defence Academy, Breda, The Netherlands

Roy Lindelauf TU Delft, Delft, The Netherlands; Netherlands Defence Academy, Breda, The Netherlands

Michael J. Mazarr RAND Corporation, Santa Monica, USA

Payam Mohseni Department of Government, Harvard University, Cambridge, MA, USA

Karl Mueller RAND Corporation, Washington, USA

Jörg Noll Netherlands Defence Academy, Breda, The Netherlands

Peter Pijpers Netherlands Defence Academy (NLDA), Breda, The Netherlands

Sebastiaan Rietjens Netherlands Defence Academy, Breda, The Netherlands

Maarten Rothman Faculty of Military Sciences, Netherlands Defence Academy, Breda, The Netherlands

Sten Rynning University of Southern Denmark, Odense, Denmark

Eitan Shamir Political Science Department, The Begin Sadat Center for Strategic Studies (BESA Center), Bar Ilan University, Ramat Gan, Israel

Max Smeets Center for Security Studies (CSS), ETH Zurich, Zurich, Switzerland; Center for International Security and Cooperation, Stanford University, Stanford, CA, USA; Centre for Technology and Global Affairs, University of Oxford, Oxford, UK

Tim Sweijs The Hague Centre for Strategic Studies, The Hague, The Netherlands

Stefan Soesanto The Risk and Resilience Team, Center for Security Studies (CSS), ETH Zurich, Zurich, Switzerland

Cees van Doorn Netherlands Defence Academy, Breda, The Netherlands

Christina van Kuijck Netherlands Ministry of Defence, The Hague, The Netherlands

Paul van Hooft The Security Studies Program (SSP), Massachusetts Institute of Technology (MIT), Boston, USA; The Hague Centre for Strategic Studies (HCSS), The Hague, The Netherlands

Alex Wilner The Norman Paterson School of International Affairs, Carleton University, Ottawa, Canada

Samuel Zilincik Masaryk University, Brno, Czech Republic; University of Defence, Brno, Czech Republic

Chapter 1
Introduction—The Evolution of Deterrence Strategy and Research

Lawrence Freedman

Contents

1.1 Introduction

The concept of deterrence has dominated Western strategic thought for some seven decades. It shows no signs of easing its grip. In the face of any new security threat, such as terrorism or cyber-attacks, one of the first questions to be asked is 'can this be deterred?' Even when the answer is not very encouraging the inclination is to persevere until some way is found at least to reduce if not remove the threat through some form of deterrence. This may have less to do with deterrence's reliability or effectiveness as a strategy and more because of its inherent normative appeal. When a state adopts a deterrence strategy it signals that it does not seek a fight but still considers some interests to be so vital that they are worth fighting for. It implies a defensive intent without weakness. It seeks to prevent aggression while being non-aggressive. It sustains rather than disrupts the status quo. For these reasons, it has positive associations that other potential strategies lack. Appeasement as a

L. Freedman (✉)
Department of War Studies, King's College London, London, UK
e-mail: lawrence.freedman@kcl.ac.uk

F. Osinga and T. Sweijs (eds.), *NL ARMS Netherlands Annual Review of Military Studies 2020*, NL ARMS, https://doi.org/10.1007/978-94-6265-419-8_1

deliberate strategy has been discredited since the 1930s; conquering other states is now seen to be as demanding as it is illegal. There is no dishonour in deterrence.

The main objections to deterrence strategies are because they provide the core rationale for possessing nuclear weapons. Those arguing for nuclear abolition often argue that the deterrence effect is a chimera. What were thought to be deterrent successes either had other causes or could be achieved by other means. This can lead to playing games with history to make a point. It was of course entirely possible that there would have been no Third World War even if nuclear weapons had never been invented but in the post-1945 world at crucial points nuclear weapons acted as a vital source of restraint.[1] A stronger, more moderate argument is that nuclear deterrence was a thin reed upon which to rely and might have let governments down at crucial moments. But that was an argument about the limits of deterrence and not its potential validity. There is nothing effortless about deterrence. It demands close attention to how threats are designed, conveyed and, if necessary, implemented.

The concept itself is simple enough. Deterrence occurs when A persuades B not to take a specified step by convincing B that whatever the anticipated gains the likely costs will be higher. When A issues a threat, its effectiveness will depend on B's perception of what it might mean as much as A's intent. If B does not take A's threat seriously and concludes that it can be safely ignored then deterrence will fail. Or A may fail to deter through negligence. It knows that B needs deterring but does not realise exactly what B is up to until too late and so is caught by surprise. Once A needs to retrieve a lost position deterrence has become irrelevant. The tables may be turned as B is now deterring A to preserve a new status quo. Nor is there a standard formula suitable for application in any situation where deterrence is required. What might work when vital interests are involved might not work when the stakes are low. A's stern threats might hit home when B is paying attention but miss completely when B is distracted or if there is a lot of background noise. What worked last time might not work this time, not least because B knows what to expect. And, as deterrence depends on the status quo holding, when nothing much changes can we be sure that this is because of the deterrent threat? Is that why B has held back? Perhaps no hostile action was ever intended. Or if it has not happened that might be for reasons unrelated to deterrence. Deterrence is therefore simple in principle and a natural strategy to adopt but it is not so straightforward when it comes to implementation. It poses both a conceptual and a practical challenge.[2]

[1] Mueller 1989; Gaddis et al. 1999.

1.2 The Cold War Focus: General Nuclear Deterrence

The Cold War flattered deterrence. It was credited with the success of the West in containing the Soviet threat. It was also during the Cold war that deterrence acquired a compelling conceptual framework. The idea of deterrence had a long history. Its origins lay in criminology. The utilitarian philosopher Jeremy Bentham supposed that criminals were sufficiently rational and self-interested to calculate when the costs of punishment would outweigh the potential benefits of crime. On this basis he proposed the term 'determent'.[2] The same idea was understood in international affairs even when the word was not used. The antecedents of Cold War thinking can be found in debates about how to deal with the prospect of mass air raids during the 1930s.[3] But it was nuclear weapons that made the difference, especially once the Soviet Union tested an atomic device in August 1949 and as both superpowers moved to 'city-busting' thermonuclear weapons. After this point, even when military planners and civilian think-tankers tried to think of clever ways of employing nuclear weapons to win wars, prudence kept on pulling policy-makers back to deterrence.

During the 1950s and into the 1960s most of the important conceptual work on deterrence was undertaken. At the start of the thermonuclear age there was a natural assumption that two equivalent, deadly multi-megaton arsenals would lead to a 'balance of terror' which would lead to an uncomfortable but potentially durable peace. But what if the 'balance of terror' was not so stable? In the mid-1950s analysts at the RAND Corporation demonstrated that a well-designed first-strike directed against the opponent's nuclear weapons might deny it the chance to retaliate. To guard against being caught out in this way a second strike capability was required—the ability to absorb a first strike and still retaliate.[4] Such thinking encouraged a technological arms race, for defensive as much as offensive reasons. Vulnerability to a first strike might lead to vulnerability to political pressure. Eventually second-strike capabilities won out over first-strike capabilities, largely as the result of the development of relatively invulnerable ballistic missile carrying submarines.

Another early response to the problem of the balance of terror, prompted by the Korean War, was to accept that this might preclude total war but then suggest that limited wars might still be possible.[5] Out of the exploration of these possibilities came the notion of escalation. This was at first a tragic concept, suggesting that any serious fighting between the superpowers, even if at first limited, would soon erupt into total war. This concept came about as a critique of the proposition that even if low-yield, short-range 'tactical' nuclear weapons were used, a war could still be kept 'limited'. In the 1960s escalation was presented in more positive terms. Instead

[2]Bentham 1830.

[3]Quester 1966.

[4]Wohlstetter 1959.

[5]Osgood 1957.

of a quick route to tragedy the idea of an 'escalation ladder' was used to show how a war might expand in stages.[6] At least in the early stages it would be possible to control the process. The basic idea was to establish sufficient dominance at one step on the ladder to put the onus on the adversary to take the risk of moving to the next step, with the violence becoming more destructive and less controllable. This was therefore intra-war deterrence. The mutual danger had been insufficient to stop the onset of war but still sufficient to encourage caution when the escalatory process was pointing to total war. This turned war into a competition in risk-taking, with deterrence failing by degrees. At some point escalation dominance would become impossible. There would no longer be a way to limit nuclear use or discriminate in targeting. The only remaining possibility was utter catastrophe.

The fear of escalation and uncertainty over the stability of the balance combined to generate anxieties that war might come about, and therefore deterrence might fail, not out of deliberate choice but because of miscalculation or even system malfunctions. A rogue order to attack or a faulty early warning system could set in motion terrible events. Such fears encouraged the idea that the superpowers should find ways to cooperate in order to reduce the risk of inadvertent escalation.[7] Arms control was a way of agreeing on how to structure nuclear forces in order to bring stability to the balance. In this way the notion of Mutually Assured Destruction was embraced and consolidated in arms control agreements, describing a situation in which nuclear exchanges would be unavoidably catastrophic for all belligerents. The superpowers had to accept that they had no route to victory in a nuclear war.

This left an awkward question, especially for the United States and its NATO allies. The original idea behind the alliance was that the US would not wait, as it had done in the previous two world wars, to come to the aid of the western democracies if they were attacked. As the Soviet Union and its satellite states enjoyed conventional superiority deterrence was assumed to depend from the start on America's readiness to initiate nuclear war. The need therefore was to deter all war and not just nuclear war. But if mutual assured destruction meant that the nuclear arsenals neutralised each other, then might the Soviets not feel free to see what could be done with conventional war without risking the devastation of their homeland? How could US nuclear threats be credible when any implementation risked retaliation in kind? How could allies be confident in the US nuclear umbrella if that meant an American government must put American cities at risk to protect European cities? This was the problem of extended deterrence.[8] It was one thing if nuclear arsenals were geared solely to national defence and nothing else, which was the original French concept. That had a sort of credibility. It was quite another to prepare to wage nuclear war on behalf of third parties. The obvious credibility problems surrounding US nuclear guarantees were the greatest stimulus to

[6]Kahn 1965.

[7]Schelling and Halperin 1961.

[8]Bobbitt 1988.

creativity in deterrence theory. It led to a number of distinctive and sometimes contradictory lines of thought that still influence thinking about deterrence.

The most influential of these lines of thought distinguished between deterrence by denial and deterrence by punishment.[9] This followed from the basic definition of deterrence as persuading an adversary that prospective costs would outweigh prospective gains. Because of the nuclear association deterrence was presumed to work through the threat of severe punishment. But this definition allowed for a completely different approach based on denying the enemy gains. In the NATO context deterrence by denial came to be associated with conventional capabilities.[10] If the Warsaw Pact could not mount an effective invasion then NATO would need to rely on the threat of nuclear first use. Against this it was argued that conventional deterrence would be expensive while the lack of a nuclear dimension might encourage exploratory Soviet aggression. With the end of the Cold War the problem of dependence on nuclear first use switched from NATO to Russia that now had to cope with conventional inferiority. While the alliance could not quite bring itself to move to a no first use promise the assumption in practice was that conventional superiority would deter most forms of aggression against NATO countries.

1.3 Moving on: Including Conventional Deterrence

Conventional deterrence was much more credible in principle and also had many more potential applications. There were still a few—and generally extreme—contingencies when it would be appropriate to talk about nuclear threats but there were no similar restrictions with conventional capabilities. The shift to conventional denial opened up a whole range of deterrence possibilities that were of no interest before. Nor was it necessary to confine conventional forces to denial—as weapons became more accurate over long ranges they could be used to inflict tailored punishments as well. Liberating deterrence from its nuclear associations also made the concept analytically more interesting. Explicit nuclear threats were few and far between but in principle there were numerous instances of conventional deterrence, going well back into history. This made possible what Robert Jervis called the 'third wave' of deterrence theory based on empirical case studies.[11] These tended to be instances where it could be shown that one side was prepared to act, and another had tried to deter, sometimes with success and sometimes without. By comparing many cases it might be possible in principle to see what factors made deterrence more or less likely to succeed.

[9]Snyder 1961.

[10]Mearsheimer 1983.

[11]Jervis 1979, pp. 289–324.

Whether or not these helped illuminate the problems of Cold War deterrence was another matter. In this context, whatever reliance might be placed on conventional denial the possibility of nuclear punishment was always present. Whatever the doubts about the credibility of extended nuclear deterrence it was hard to ignore the possibility that with so many nuclear weapons deployed, often as part of army, air and naval formations, there was always a risk that in the heat of battle some might be launched. This moved the appreciation of the deterrent effect of nuclear weapons away from the credibility and specificity of threatened use and toward the residual risk that even if policy-makers were desperate for this not to happen, they might nonetheless be used. It might be hard to describe a chain of events that would lead to a rational decision to initiate nuclear war but it was impossible to preclude its possibility once a major war had begun. Despite the efforts to imagine controlled steps up an escalation ladder it was much easier to imagine how the more tragic concept of escalation would influence events. It continued to remind of how the best efforts to keep a war limited might be dashed as matters got out of hand. Nuclear use would be propelled to the fore by the passions and uncertainties of a bitter conflict, leading to a terrible conclusion. This prospect on its own should lead to caution and restraint at a time of crisis. All that was necessary for a deterrent effect was for nuclear weapons to exist in a usable form. This was described as 'existential deterrence'.[12] It was not one side's threats of action that deterred but the risk of an event in which such escalation might occur.

In the circumstances of the Cold War this worked. One reason for this was that there were no obvious flashpoints, at least in Europe, once the anomaly of Berlin was sorted out, first in August 1961 by the construction of the wall that divided the city and then at the end of that decade by a set of agreements encouraged by West Germany's 'Ostpolitik' leading to a détente in Europe. Instead of a direct attack by one alliance against the other scenarios for future war tended to postulate unrest within the satellite states of the Warsaw Pact or else a crisis imported from the Middle East where matters were more dynamic and fluid. Alternatively, anything that might threaten the cohesion of NATO, including an American decision to withdraw its forces from Europe on the grounds that they were no longer needed, potentially risked unsettling the status quo.

1.4 Beyond the Cold War and General Deterrence

From this three large conclusions might be drawn about deterrence. The first was that it was not good enough to consider it in terms of a particular configuration of forces and articulation of threats. Deterrence relationships had to be given context. The state of affairs at risk from aggression or disruption had to be addressed along with the national interests of the key actors. In situations marked by turbulence and

[12]McGeorge 1983.

volatility, and with so much going on, identifying the specific move that needed to be deterred might not be straightforward. The second was to recognise the importance of alliance as a source of deterrence. When NATO was formed, the deterrent effect was the result of the United States becoming committed to the security of the West European democracies. So long as that remained the case aggression against Western Europe would be high risk. Should the commitment be withdrawn the situation would change dramatically. The Europeans would need to look to other means to resist Soviet pressure. The third conclusion was that because the European situation stabilised, with neither NATO nor the Warsaw Pact in disarray and no crisis forcing matters to a head, other than occasional flurries of anxiety, deterrence became embedded in the thinking of all key actors and lost all sense of urgency. It became internalised. The preparations for war continued as part of the routines of alliance but political leaders saw no need to put their countries on a war footing.

Patrick Morgan made an important distinction between general and immediate deterrence.[13] With general deterrence the situation is one in which relations between states are still antagonistic yet the antagonism has long lost its edge. With immediate deterrence the antagonism is sharp and dangerous and A must act at once to deter B's likely aggression. Most deterrence relationships start with an immediate crisis. If it is managed successfully the threats and forces may still stay in place until eventually a point is reached when a resumption of crisis conditions appears unlikely. This should allow underlying political relations to improve. If on the other hand the conflict shows signs of resuming it should be possible to provide timely reminders of why aggression is still a bad idea. Much of the empirical literature is dominated by instances of immediate deterrence. By definition these are situations when not only has deterrence not been internalised but it is barely working at all, for that is why the crisis has occurred. General deterrence, when there is an embedded expectation that nothing much will happen, described a truly successful deterrence strategy. The would-be aggressor not only holds back for the moment but also then stops thinking of aggression as a serious option.

Focussing on the political context helps explain what happened to deterrence after the end of the Cold War. The East-West conflict had reached its own equilibrium between two superpower-led alliances. Both appreciated the possibility of mutually assured destruction and as a result had internalised deterrence. This equilibrium was lost as one alliance collapsed (with most of its members then joining NATO) leaving Russia feeling more vulnerable and insecure. Political relations generally became more complex and fluid, so it was less clear where deterrence was needed and how it might be achieved, especially as non-state actors, including vicious terrorist groups grew in importance. Deterrence was no longer required to solve one big problem. Instead it was called in aid to solve many small ones. Instead of the dominant strategy it was a stratagem available for addressing a

[13]Morgan 1977.

variety of contingencies, some quite unique, using a variety of means, non-military as well as military, although without confidence that it could solve any. This was described as 'fourth-generation deterrence', much broader than the earlier generations reflecting the changes in the international system, and so lacking the theoretical coherence or consistent sense of purpose.[14]

1.5 The Enduring Relevance of Deterrence Strategy and Research

The big problem of a great power war of course did not go away. Indeed, after a relatively relaxed period it returned, with Russia using force to look after its interests, first in Ukraine and then in Syria, and China flexing its muscles in the Asia-Pacific region. This led to a degree of continuity. The same questions were raised as they had been during the Cold War about the durability of America's alliances and whether nuclear weapons have a dampening effect on tendencies towards open warfare. There were now other actors whose nuclear arsenals needed to be taken into account, including India, Pakistan, Israel and North Korea. In this way the fourth-generation of deterrence was shaped by the 'second nuclear age'.[15] A secure second-strike capability was still seen as vital to the practice of nuclear deterrence. There was now an added concern, which had been growing steadily since the 1970s, about the vulnerability of command and control systems. It may not matter if all sorts of enemy military capabilities, including nuclear weapons, are left if a first strike directed against the 'national command authority' has left the enemy brainless and paralysed, although it would need considerable confidence to be sure that a decapitation attack would leave the enemy so brainless and paralysed that it would be completely unable to take retaliatory action. Such attacks also raised the question of how a peace can be arranged if there was no one left with whom to negotiate. Yet it is an issue that bothers military planners, especially when governments might be taken out by non-nuclear systems, such as hypersonic weapons. It is also an issue that is not confined to major war. The targeted killing of leaders has become a feature of counter-terrorism and counter-insurgency campaigns. The aim has been more to reduce the effectiveness although it might give someone an opportunity to take on a leadership role pause for thought!

As major war is still best avoided attention has moved to the so-called 'grey area' between a comfortable peace and serious fighting, involving proxies, information campaigns and cyber-operations. In the grey area it may be hard to attribute actions to particular actors. So while denial might work in that a degree of resilience and protection can be built in to any system that might be attacked, punishment is

[14]Knopf 2010.

[15]Bracken 2000.

less straightforward unless the guilty party can be identified with accuracy and some appropriate sanction identified.

Deterrence works best with unambiguous red lines, established over time, linked with vital interests, and backed by clear and credible messages, reinforced by known capabilities, about what will happen if they are crossed. It will work less well as more uncertainties are introduced—about where the lines actually are, how much any transgressions will actually matter, whether there will be much of a response if they are crossed and what difference they will actually make. A decades-long stand-off in the centre of Europe between two great alliances was one thing: sudden crises emerging out of a complex, multi-faceted and fast changing set of political relationships is another. If only for its presentational advantages, deterrence will continue to be seen as the ideal response to most types of security threats. In some situations it should work well—often so well that it is taken for granted. But it would be unwise to play down the challenges of making deterrence work when threats have to be constructed in a hurry to deal with one-off situations with lots of unique complications, amid expressions of doubt and dissent about whether they could or should be acted upon.

References

Bentham J (1830) The Rationale of Punishment (derived from manuscripts by Bentham written in the 1770s). In: Heward R (ed), London. http://www.la.utexas.edu/labyrinth/rp/index.html

Bobbitt P (1988) Democracy and Deterrence: The History and Future of Nuclear Strategy. Macmillan, London

Bracken P (2000) The Second Nuclear Age. Foreign Affairs (January/February 2000)

Gaddis J L, Gordon P H, May E R, Rosenberg J (1999) Cold War Statesmen Confront the Bomb: Nuclear Diplomacy Since 1945. Oxford University Press, Oxford

Jervis R (1979) Deterrence Theory Revisited. World Politics XXXI.2:289-324 (January 1979)

Kahn H (1965) On Escalation: Metaphors and Scenarios. Pall Mall, London

Knopf J W (2010) The Fourth Wave in Deterrence Research. Contemporary Security Policy, 31.1

McGeorge B (1983) The Bishops and the Bomb. The New York Review of Books (16 June 1983)

Mearsheimer J (1983) Conventional Deterrence. Cornell University Press, Ithaca

Morgan P (1977) Deterrence: A Conceptual Analysis. Sage Publications

Mueller J (1989) Retreat from Doomsday

Osgood R E (1957) Limited War: The Challenge to American Strategy. The University of Chicago Press

Quester G (1966) Deterrence Before Hiroshima: The Influence of Airpower on Modern Strategy. Wiley, New York

Schelling T, Halperin M (1961) Strategy and Arms Control. Twentieth Century Fund, New York

Snyder G (1961) Deterrence and Defense. Princeton University Press, Princeton NJ

Wohlstetter A (1959) The delicate balance of terror. Foreign Affairs XXXVII.2 (January 1959)

Lawrence Freedman (CBE) has been Professor of War Studies at King's College London since 1982, and Vice-Principal since 2003. He was educated at the Universities of Manchester, York and Oxford. Before joining King's, he held research appointments at Nuffield College Oxford, IISS and the Royal Institute of International Affairs. Elected a Fellow of the British Academy in 1995 and awarded the CBE (Commander of the British Empire) in 1996, he was appointed Official Historian of the Falklands Campaign in 1997. He was awarded the KCMG (Knight Commander of St Michael and St George) in 2003 and in 2009 was appointed to serve as a member of the official inquiry into Britain and the 2003 Iraq War.

Part I
Concepts of Deterrence (Evolution, Rediscovery, Conventional, Nuclear, Cross-Domain)

Chapter 2
Understanding Deterrence

Michael J. Mazarr

Contents

Abstract The challenge of deterrence—discouraging states from taking unwanted actions, especially military aggression—has again become a principal theme in U.S. defence policy. This chapter reviews the fundamentals of deterrence in theory and practice. It surveys basic definitions and types of deterrence, including central versus extended deterrence and techniques of deterring by denial or punishment. The chapter argues that it in inaccurate to equate deterrence strength with the local

This chapter is a slightly revised reprint of Michael Mazarr, Understanding Deterrence, RAND, Santa Monica, 2018. Reprinted with permission.

M. J. Mazarr (✉)
RAND Corporation, Santa Monica, USA
e-mail: Michael_Mazarr@rand.org

F. Osinga and T. Sweijs (eds.), *NL ARMS Netherlands Annual Review of Military Studies 2020*, NL ARMS, https://doi.org/10.1007/978-94-6265-419-8_2

military balance, which is one important factor in deterrence success, but not the only one. It examines three essential conditions for deterrence success: The level of aggressor motivation, clarity about the object of deterrence and the actions the defender will take, and the defender's capability and will to fulfil threats.

Keywords classical deterrence theory · fundamentals · motivations · perceptions · psychology · motivation · dissuasion

2.1 Introduction

The challenge of deterrence—discouraging states from taking unwanted actions, especially military aggression—has again become a principal theme in U.S. defence policy. In Europe, the United States and its allies seek to deter potential Russian adventurism in the Baltic states, as well as "grey-zone" activities (ongoing belligerence below the threshold of major war). In Korea, the United States and the Republic of Korea work to deter not only an outright invasion but also a spectrum of North Korean provocations. Elsewhere in Asia, the United States and its allies are dealing with Chinese belligerence and grey-zone encroachments on areas subject to territorial disputes. Across the globe and in many different domains, the United States now confronts a more immediate requirement for effective deterrence than at any time since the end of the Cold War. Because many potential adversaries are significantly more capable than they were a decade or more ago, moreover, the risks of actually fighting a major war are more significant than ever—making it even more imperative to deter conflict.

Yet much of the emerging dialogue on deterrence remains characterized by unsupported assertions, claims that contradict the empirical record, and little reference to classic analyses.[1] Meanwhile, changes in the international security environment have altered the context for deterrence, possibly challenging long-held assumptions and creating new requirements. This Perspective draws on a range of recent and classic RAND Corporation studies to revisit fundamental concepts and principles about deterrence. The most important overarching lesson of this review is that deterrence and dissuasion must be conceived primarily as an effort to shape the thinking of a potential aggressor. Deterrent policies are often viewed through the perspective of the country doing the deterring—in this case, the United States—and focus on actions that it takes to raise the costs and risks of an attack. But the value of those steps depends entirely on their effect on the perceptions of the target state. Any strategy to prevent aggression must begin with an assessment of the interests, motives, and imperatives of the potential aggressor, including its theory of

[1]There are many important studies of the requirements of deterrence. A number of especially classic or important sources include George and Smoke 1974; Beaufre 1965; Schelling 1980, 2008; Morgan 1983; Freedman 2004; and Huth 1988.

deterrence (taking into account what it values and why). In the process, as will be argued, history strongly suggests that aggressor motivations are varied and complex, and as often grounded in a desperate sense of a need to act as they are the product of aggressive opportunism.[2] Deterrence turns out to be about much more than merely threatening a potential adversary: It demands the nuanced shaping of perceptions so that an adversary sees the alternatives to aggression as more attractive than war.

2.2 Definitions and Types

Deterrence is the practice of discouraging or restraining someone—in world politics, usually a nation-state—from taking unwanted actions, such as an armed attack. It involves an effort to stop or prevent an action, as opposed to the closely related but distinct concept of "compellence", which is an effort to force an actor to do something.

2.2.1 Denial Versus Punishment

The classic literature distinguishes between two fundamental approaches to deterrence. Deterrence by denial strategies seek to deter an action by making it infeasible or unlikely to succeed, thus denying a potential aggressor confidence in attaining its objectives—deploying sufficient local military forces to defeat an invasion, for example.[3] At their extreme, these strategies can confront a potential aggressor with the risk of catastrophic loss. Deterrence by denial represents, in effect, simply the application of an intention and effort to defend some commitment. A capability to deny amounts to a capability to defend; "deterrence and defence are analytically distinct but thoroughly interrelated in practice".[4] The most common way of measuring the health of a deterrence threat grounded in denial capabilities is the immediate balance of forces in the contested territory—but, as will be explained, the local balance of forces is not the only, or even always the most important, factor. Deterrence by denial should not be equated with military balances alone.

Deterrence by punishment, on the other hand, threatens severe penalties, such as nuclear escalation or severe economic sanctions, if an attack occurs. These penalties are connected to the local fight and the wider world. The focus of deterrence by

[2]See Mueller et al. 2006, in particular Chap. 2.

[3]Beaufre argues that in the prenuclear era, a capacity to deter simply meant a capacity to win (Beaufre 1965, p. 23). Later (p. 51), he describes the conventional deterrence dynamic as the "dialectic of expectation of victory on the part of the two opponents".

[4]Morgan 1983, p. 32.

punishment is not the direct defence of the contested commitment but rather threats of wider punishment that would raise the cost of an attack. Most classic studies suggest that denial strategies are inherently more reliable than punishment strategies.[5] Steps taken to deny, such as placing significant military capabilities directly in the path of an aggressor, speak loudly and clearly. An aggressor might doubt, on the other hand, a defender's willingness to impose punishments. As Snyder argued, "To have an adequate denial capability, preferably one situated near or in a threatened area, is the surest sign we can make to the enemy that the area is valued highly by us."[6] An aggressor might also convince itself that the defender will hesitate to follow through on threats to punish because of attendant risks, such as further escalation, that the deterring state may not be willing to run once the moment arrives.[7] As Thomas Schelling noted, there are threats that a state would rather not fulfil, and weakness in deterrence can emerge when an aggressor believes the defender will ultimately prove unwilling to carry out its threats.[8]

2.2.2 *Direct Versus Extended*

Deterrence can be used in two sets of circumstances. Direct deterrence consists of efforts by a state to prevent attacks on its own territory—in the U.S. case, within the territorial boundaries of the United States itself. Extended deterrence involves discouraging attacks on third parties, such as allies or partners. During the Cold War, direct deterrence involved discouraging a Soviet nuclear attack on U.S. territory; extended deterrence involved preventing a Soviet conventional attack on North Atlantic Treaty Organization (NATO) members.[9]

For obvious reasons, extended deterrence is more challenging than direct deterrence. This is partly true for military operational reasons: It is more difficult to deny an attack far from home, a mission that demands the projection of military force sometimes thousands of miles away and often much closer to the territory of the aggressor state. However, it is also true for reasons of credibility. An aggressor can almost always be certain a state will fight to defend itself, but it may doubt that a defender will fulfil a pledge to defend a third party. During the Cold War, for example, there were constant debates about the credibility of the U.S. promise to "sacrifice New York for Paris". Reinforcing extended deterrence involves taking steps to convince a potential aggressor that the distant defender will definitely respond to an attack, or at least as promptly as it can in accordance with national laws. Such steps include actions like stationing significant numbers of troops from

[5]Huth and Russett 1988, p. 42.
[6]Snyder 1959, pp. 4–6, 38.
[7]Snyder 1959, p. 35.
[8]Schelling 1980, p. 123.
[9]Huth and Russett 1988, pp. 15–18.

the deterring state on the territory of the threatened nation, as the United States has done in many cases. The defender seeks to create the perception that it has, in effect, no choice but to respond if its ally is attacked. Yet this is a demanding standard to meet, in part because a state will seldom commit to anything like an automatic response if vital national interests are not at stake—and often, even if they are. The most famous cases of extended deterrence failure involving the United States—such as Korea in 1950 and Iraq-Kuwait in 1990—can be partly traced to the fact that the United States was unwilling to demonstrate automaticity of response before the fact. Even the most powerful treaty commitments generally contain some degree of leeway. Article 5 of the North Atlantic Treaty, which is arguably the strongest U.S. commitment of extended deterrence, does not oblige parties to take an automatic response to aggression against any other ally. It calls on parties to take "forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area."[10] This language reflected a compromise between the United States' European allies, which sought as close as possible to an automatic response in the event of aggression, and the U.S. Congress, which wanted to preserve its war powers. Similar conditions can be found in all U.S. mutual security treaties.

The United States has sometimes hesitated to make less ambiguous deterrent threats, such as in the cases of Korea and Iraq, because of another complication in extended deterrence (and deterrence threats of all kinds): Such threats can be very costly to make. This is partly true because of the implied commitment involved—once the United States has threatened to respond to a certain sort of attack, it must then plan and prepare to do so. Much of the current U.S. defence budget is devoted to building the capacity and capabilities necessary to engage in the large-scale contingencies that represent the U.S. global deterrence posture. But threats can also be costly in diplomatic terms, generating deeper tensions with rivals who may or may not have been intending to attack.

Defenders, therefore, are constantly engaged in a tenuous balancing act. They are trying to gauge the national interests they have at stake in a potential contingency, the costs and risks of being very explicit about their response, and the dangers of aggression if they do not make such explicit threats. Such complex dynamics are apparent in the U.S. and NATO efforts to warn Russia off aggression in the Baltic States today.

2.2.3 General Versus Immediate

Finally, the theoretical literature distinguishes between two overlapping time periods in which deterrence policies can be employed. General deterrence is the ongoing, persistent effort to prevent unwanted actions over the long term and in

[10]North Atlantic Treaty Organization 1949.

non-crisis situations. Immediate deterrence represents more short-term, urgent attempts to prevent a specific, imminent attack, most typically during a crisis.[11] For example, the United States employed general deterrence for decades by publicizing ongoing promises of defence and punishment if the Soviet Union attacked Western Europe. The United States engaged in the related but distinct task of immediate deterrence during crisis periods, when the United States feared that Soviet aggression against Berlin was imminent.

Most classic studies suggest that general deterrence is easier than immediate deterrence. A potential aggressor may pass long periods without being tempted to take aggressive actions. It is in the specific moments when aggression seems especially enticing or desperately required that deterrence is most at risk, and these moments call for very aggressive and urgent efforts to bolster immediate deterrence. Succeeding during such crises can be especially challenging because the aggressor may have become so committed to a course of action, and so opposed to the idea of backing down, that it has become almost impossible to deter.[12] Therefore, part of the goal of general deterrence is to reduce the need for immediate deterrence—to create deterrent and dissuasion effects that become so ingrained that hesitation to attack becomes habitual.

2.2.4 Narrow Versus Broad Concepts of Deterrence

One of the most important decisions about how to view deterrence involves its scope: Is it viewed narrowly or broadly? The narrowest definitions hold that deterrence refers solely to military tools of statecraft—using the threat of military response to prevent a state from taking an action.[13] A broader conception keeps the focus on threats but expands the scope to non-military actions: A state can deter using threats of economic sanctions, diplomatic exclusion, or information operations.[14]

These two approaches agree with the basic definition that deterrence is "dissuasion by means of threat". It can be based on "the capability of defence denying the adversary its immediate objectives" or on "the threat of inflicting heavy

[11]Huth and Russett 1988, p. 30; Freedman 2004, pp. 40–42; Lebow and Gross Stein 1990, pp. 336, 342; Levy 1988; and Huth 1999, pp. 27–28.

[12]Morgan 1983, pp. 42–44; for a broader discussion of the distinction, see pp. 27–47.

[13]See Freedman 2004, pp. 26–27, 36–40.

[14]Another understanding of the term deterrence equates the very notion of deterrence with one specific domain—nuclear deterrence. The strategy of deterring someone from taking unwanted action, however, long predates the nuclear era and applies to many more issues than nuclear weapon use. Defining "deterrence" and "nuclear" as somehow synonymous misses the larger context for the term.

punishment in a larger struggle".[15] Either way, it is an effort to affect the calculus of risk and cost by threatening either the potential success or the other interests of the aggressor.[16]

A third, broader way of approaching deterrence is to understand the idea of discouraging unwanted actions as including means beyond threats—to think of deterrence as only one part of a larger process of dissuading an actor. The goal of dissuasion is to convince a potential attacker that the cost-benefit calculus of aggression is unfavourable, partly through emphasizing the costs of aggression but also through offering reassurances and benefits that make a world without aggression more attractive.

It is an approach designed to make aggression as unnecessary as it is costly.[17] "In its most general form," Alexander George and Richard Smoke have written, "deterrence is simply the persuasion of one's opponent that the costs and/or risks of a given course of action he might take outweigh its benefits."[18] This concept suggests that deterrent strategies can help prevent an action by including steps to make an action unnecessary—including offering concessions or reassurances. In real-world situations, the United States often combines threats and inducements in this way. In cases of non-proliferation, for example, the United States seeks to dissuade certain states from developing nuclear capabilities by threatening (mostly non-military) consequences—but also by offering possible benefits if that state agrees to constrain its nuclear ambitions.

Using such a broader concept of dissuasion to describe what a deterring state is trying to do turns out to be especially important because of the ways in which threat-based deterrence strategies can go tragically wrong and provoke the very conflicts they are meant to avoid.[19] Capabilities deployed to deter, for example, can end up convincing the other side that the deterring state is preparing an attack, making war look more necessary, rather than less. Actions taken to punish an aggressor can create a desperate situation in which the aggressor ends up believing that war is its only option.

In many Cold War cases, for example, such as Berlin and the Cuban Missile Crisis, U.S. leaders ended up undertaking various initiatives to convince the Soviet Union that it would be secure without aggression. Especially when dealing with a peer rival that believes it has a rightful claim to international status, it can be very difficult to merely threaten a potential aggressor into submission. Some form of reassurance is almost always part of any successful dissuasion strategy.

---

[15]Huth and Russett 1988, p. 30. Robert Jervis similarly suggests that "One actor deters another by convincing him that the expected value of a certain action is outweighed by the expected punishment," the term "punishment" seeming to imply threats". See Jervis 1983, p. 4.

[16]Morgan 1983, p. 37.

[17]See Huth 1999, pp. 29, 38; and Freedman 2004, pp. 55–59.

[18]George and Smoke 1974, p. 11.

[19]Jervis 1983, p. 3; Jervis 1989, p. 183.

2.3 The Local Balance of Forces: Important but Not Always Decisive

While potent capabilities for denying aggressors' objectives typically form the foundation of any wider deterrence strategy, the variable of the local balance of forces does not, on its own, consistently explain the success or failure of deterrence. In many cases, potential aggressors never challenged local weakness: The Soviet Union could have seized Norway during the Cold War at just about any time, but chose not to because of the larger ramifications. Sometimes states with dominant power refused to fully deploy it, as with the United States in Vietnam. Viewed strictly in percentage terms, the number of states with a military advantage that do not start wars is overwhelming. In other cases, aggressors ignored clear evidence that the defender was superior and attacked anyway.[20] Decisions for war reflect a kaleidoscope of fears, goals, preferences, motives, and other considerations. An aggressor's belief about the relative military strength at the point of attack is only one of those factors. "Wars rarely start because one side believes that it has a military advantage," the scholar Richard Ned Lebow explains. "They occur when leaders become convinced that force is necessary to achieve important goals."[21]

Even if the defender has the advantage, deterrence can fail because aggressors engage in wishful thinking—as Japan did in 1941, convincing itself that it could win a war against the United States. Such wishful thinking often supports an implicit decision that has already been made: The aggressor has determined that, for geostrategic or domestic political reasons, it has to act. In such cases, even a strong military advantage for the defender will not prevent war from occurring. The defender need not have superiority for deterrence to work. Sometimes it can be in an inferior position and still succeed even when an adversary is inclined to attack—as NATO was compared with massive Soviet armies during much of the Cold War.

The question for deterrence is more complex and nuanced: How much military capability, especially in the local area of potential aggression, is enough to deny an aggressor the opportunity for an easy victory? Both classic deterrence literature and more-recent empirical analyses suggest that the answer need not be an unquestioned ability to "win". A defender can succeed by deploying sufficient local forces to raise the cost of a potential attack, to make escalation inevitable, and to deny the possibility of a low-risk fait accompli. Such a strategy is based on the idea that even

[20]Russett 1963, pp. 102–103. One complication in the relationship between local military strength—denial capabilities—and a broader threat to retaliate is that, if denial forces are less than sufficient for defence, their weakness may be as evident as their potential strength. The deterrent value of punishment, on the other hand, while uncertain, is always present and does not depend on local strength (Snyder 1959, p. 6). George and Smoke actually list the "defender's military capability" as a "minor condition", "less critical" than the leading ones that affect deterrence outcomes (George and Smoke 1974, p. 530).

[21]Lebow 1982, pp. 195–197.

incomplete denial capabilities can create the risks of escalation, raising "a spectre of costs for the enemy well beyond those which the surface forces themselves are capable of inflicting".[22] Even if an attacker believes it might be successful in such cases, the costs of a long and painful war are a powerful preventive deterrent. The United States employed this strategy with great success in Europe during the Cold War. Glenn Snyder, a member of the original post-war generation of deterrence theorists, recognized as early as 1959 that U.S. forces were "incapable of denying any territory to the Soviets that they wish to take with full force". That was not the forces' main purpose—but nor, on the other hand, were they mere "hostages", a force serving only as a trip wire for U.S. involvement.

The sizeable U.S. presence had deterrent value "in its indirect complementary effects—that is, in the extent to which it strengthens the probable or evident willingness of the West to activate the strategic airpower deterrent". These forces could achieve these effects in several ways: by serving a classic trip-wire function, forcing Moscow to kill Americans in an attack; by placing U.S. national prestige on the line; and by requiring a larger Soviet attack, making a short-notice fait accompli less possible. By playing such roles, Snyder concluded, "Forces beyond those necessary for the trip-wire and yet too weak to defend against a full-scale attack nevertheless do contribute to the deterrence of such an attack."[23]

2.4 The Dominant Variable: Perceptions

Over the past three decades, further research on deterrence has emphasized a crucial fact: It is the perceptions of the potential aggressor that matter, not the actual prospects for victory or the objectively measured consequences of an attack. Perceptions are the dominant variable in deterrence success or failure.[24] The classic, game-theoretic version of deterrence theory was a form of rationalist cost-benefit calculus. It relied for its success on a foundation of the objective, rational evaluation

[22]"Even if [the United States'] denial force were incapable of holding," Snyder contends, "the enemy would have to reckon that the stronger it is, the more likely [the United States is] to believe that the application of strategic airpower would be the marginal factor that would clinch victory"—thus encouraging escalation on the United States' part (Snyder 1959, p. 4).

[23]Snyder 1959, pp. 8–10. Schelling seems to agree: "Forces that might seem to be quite 'inadequate' by ordinary tactical standards," he argues, "can serve a purpose, particularly if they can threaten to keep the situation in turmoil for some period of time. The important thing is to preclude a quick, clean Soviet victory that quiets things down in short order" (Schelling 2008, p. 112).

[24]Jervis 1983, p. 4.

of ends, costs, and risks by a potential aggressor[25] and demanded a shared and coherent value system of clearly defined objectives. Yet more-recent research has made clear that these assumptions often do not hold: Deterrence succeeds, when it does, by creating a subjective perception in the minds of the leaders of the target state.[26]

The importance of aggressor perceptions explains why deterrence can fail even when a defender has seemingly sufficient military strength. As noted above, potential aggressors sometimes decide that they must act—because they believe they face national ruin otherwise (as in Japan in 1941),[27] because a geopolitical commitment is on the line (as in the Soviet Union in Afghanistan), or because domestic factors make aggression a seeming necessity.

States this powerfully motivated can become essentially immune to deterrence. History is full of examples of states that seemingly ought to have been deterred nonetheless going to war because they had potent domestic or perceptual reasons for thinking they simply had no choice. "Almost without exception," Lebow has suggested, crises "could most readily be traced to grave foreign and domestic threats which leaders believed could only be overcome through an aggressive foreign policy."[28] Lebow points to research outlining at least four avenues to perception-driven aggression: the aggressor's fear of a looming collapse in the global balance of power, the need to redirect attention from domestic political instability, the weaknesses of a specific set of leaders, and competition for power among a state's elites. Deterrence strategies will have great difficulty in addressing any of these motives.

Perceptions, in turn, point to the critical role of specific leaders and their preconceptions, beliefs, and cognitive styles.[29] Some may be risk avoidant and relatively easy to deter. Others, such as Saddam Hussein, may repeatedly engage in megalomaniacal wishful thinking in ways that make deterrence a constant struggle. These examples demonstrate the importance of pairing deterrent threats with compromises and reassurances in a larger strategy of dissuasion. Otherwise, the defender's threats can mount to the point that they convince a potential aggressor that it must attack because the deterring power is seeking its destruction. U.S.

[25]"If we confine our study to the theory of strategy," Schelling writes, "we seriously restrict ourselves by the assumption of rational behavior—not just of intelligent behavior, but of behavior motivated by a conscious calculation of advantages, a calculation that in turn is based on an explicit and internally consistent value system" (Schelling 1980, pp. 4, 16–17). He adds that deterrence critically depends on the "rationality and self-discipline on the part of the person to be deterred" (p. 11). See also Lebow and Gross Stein 1989; Jervis et al. 1985; Morgan 1983; Morgan 2003, pp. 133–148; and Paul 2009.

[26]As Schelling explains, "A strategic move is one that influences the other person's choice . . . by affecting the other person's expectations on how one's self will behave" (Schelling 1980, p. 160).

[27]See, for example, Hotta 2013.

[28]Lebow 1983, p. 334. See also Lebow 2007.

[29]Gross Stein 2009; Morgan 2003, pp. 42–79.

strategy toward North Korea could run this risk if steps taken to deter end up convincing Pyongyang that the United States is preparing for war.

The importance of perception also illustrates the importance of developing deterrence strategies custom-made for the interests, preferences, and perceptions of a specific adversary. The notion of "tailored deterrence" has gained renewed attention in recent years. While, in essence, it merely calls for applying classic deterrence notions to specific cases, it is nonetheless a useful reminder that deterrence does not work in general—it works in specific ways against specific potential aggressors. As the unclassified public version of the 2018 U.S. nuclear posture review put it, there is no "one size fits all" for deterrence. The requirements for effective deterrence vary given the need to address the unique perceptions, goals, interests, strengths, strategies, and vulnerabilities of different potential adversaries. The deterrence strategy effective against one potential adversary may not deter another.[30]

2.5 Three Fundamental Conditions for Successful Deterrence

Hundreds of studies on deterrence—some entirely theoretical, some grounded in game theory, some based on large statistical analyses of deterrence cases, and some grounded in detailed case studies of specific examples—identify three essential factors as the most important determinants of the success or failure of deterrence strategies.

2.5.1 Level of Aggressor Motivation

As suggested by the importance of perceptual variables to deterrence, the intentions of the potential aggressor are the beginning point for any analysis of deterrence success or failure. If a state sees little reason to undertake aggression, it will not be hard to deter; if it has acquired an urgent sense that only an attack will safeguard its interests, it may become almost impossible to stop. Patrick Morgan concludes that "challenger motivation is the most important factor in deterrence success or failure."[31] Possible motivation to attack can stem from many perceptions, not all of them opportunistic. In fact, the degree to which a potential aggressor is dissatisfied with the status quo is one of the most powerful engines of aggressive intent. A state that believes that it is being constricted to the point of regime collapse, such as Iraq in 1990 or Japan in 1941, will accept many more risks than a state that believes it

[30]Office of the Secretary of Defense 2018, p. 26.

[31]Morgan 2003, p. 164. See also George and Smoke 1974, p. 532.

can achieve its national goals without war. The empirical record strongly indicates that states that initiate aggression are not merely opportunistic or aggressive but are often responding to situations they perceive as highly dangerous. Combinations of threats and concessions appear to be most associated with deterrence success; as one scholar has concluded, "Mixing deterrence and conciliation is best—be tough but not bullying, rigid, or unsympathetic."[32]

These decisions are typically comparative rather than binary. Decision makers seldom weigh the cost-benefit calculus of starting aggression in the abstract; they are considering the relative merits of several alternative courses. If leaders view attacking as less risky or costly than any of the alternatives, they will not be deterred. But this comparative decision-making process also suggests, as Schelling argued, that "the pain and suffering" embodied in the deterrent threats "have to appear contingent on their behaviour."[33] If deterrent threats come to be perceived as a general policy of hostility, they may lose their ability to be applied to deter specific actions.

2.5.2 *Clarity About the Object of Deterrence and Actions the Defender Will Take*

A second broad criterion for deterrence success is that the defender should be as clear as possible about what it is trying to deter, as well as what it will do if the threat is ignored.[34] Korea in 1950 and Iraq in 1990 provide two powerful examples of the dangers of a striking absence of clarity. In both cases, the United States refused to be clear in its deterrent threat. This failure left two highly motivated aggressors ample room to convince themselves that they could achieve a fait accompli that would not provoke a decisive U.S. response. By its nature, deterrence is a demand that another state refrain from doing something. The more ambiguous the demand is, the more chance there is for failure in the deterrent policy. Not only must the deterring state be precise in its commitments, but its target must understand them clearly. A key challenge of deterrent threats is to ensure that a potential aggressor perceives the message "through the din and noise" of world politics.[35] This demands both public and private efforts to communicate an unambiguous message. It also points to the danger of statements or actions that seemingly throw into doubt the sincerity of the commitment. Yet as explained earlier, making

[32]Morgan 2003, pp. 162–163. Morgan writes, "strength of the challenger's motivation is crucial—weakening it by concessions and conciliation can make chances of success much higher."

[33]Schelling 2008, p. 4.

[34]George and Smoke 1974, pp. 561–565.

[35]Schelling 1980, p. 11; see also pp. 26–28, 47. Elsewhere, Schelling writes, "If he cannot hear you, or cannot understand you, or cannot control himself, the threat cannot work" (Schelling 2008, p. 38).

unqualified deterrent threats can be costly, both in terms of the military requirements they generate and because of the hostility and tensions they provoke—tensions that can end up making a conflict more rather than less likely. States trying to deter attack must always balance these essential considerations, trying to find the degree of clarity that will make their intentions apparent without provoking. And in the process, the defender is always calculating the degree of national interests involved: It may prefer not to see a certain form of aggression, but if the target of that attack is not vitally important to the deterring state, it will seldom be capable of broadcasting unambiguous deterrent threats in peacetime.

2.5.3 *Aggressor Must Be Confident That Deterring State Has Capability and Will to Carry Out Threats*

Much of classic deterrence theory can be boiled down to a simple proposition: The potential aggressor must believe that the defender has the capability and will to do what it threatens.[36] This criterion is, again, perceptual: The question is not whether the defender actually has such capabilities or will, it is whether the aggressor believes that it does. Deterrence depends on the perception of the "threatener's determination to fulfil the threat if need be"—and, more importantly, on the potential aggressor's "conviction that the threat will be carried out".[37] Deterrence fails, Bruce Russett concludes, "when the attacker decides that the defender's threat is not likely to be fulfilled."[38] This axiom highlights two distinct factors—capability and will. Perceived weakness in either can undermine deterrence. Capability is straightforward enough. As suggested earlier, the immediate, local balance of forces is not always a key determinant of deterrence success—but a defender's broadly perceived suite of capabilities, military and otherwise, must be strong enough to convince a potential attacker that it is likely to pay a heavy price for aggression. Will is a much more abstract variable and easily subject to misperception. Aggressors have repeatedly convinced themselves that a defender did not have the will to respond, especially in cases of extended deterrence. Will is partly a function of the national interests involved: If a defender is seen to have vital interests at stake, a potential attacker will believe threats of response. Aggressors can try to undermine a defender's willingness to respond by using "salami slicing" approaches—using a long series of low-level aggressions to change the facts on the ground without ever taking action that would justify a major response. Such strategies are designed to put the defender in a dilemma: It cannot respond to every small violation, but if it does not begin to punish minor transgressions, its strategic

[36]Paul 2009, p. 2. See Knopf 2009, pp. 31–57.

[37]Schelling 1980, p. 11. "The important thing is not merely having a capability—it is projecting the willingness, indeed the requirement, to use it" (Schelling 2008, p. 36).

[38]Russett 1963, p. 98.

position will erode over time. The United States confronts this challenge with Chinese and Russian grey-zone campaigns today.

As noted earlier, classic deterrence theory spoke in terms not only of making credible threats but also, where possible, of creating a perceived obligation to respond. Schelling believed that, once a war loomed, the deterring state would often want to avoid the consequences of its commitments by wriggling free of its deterrent threats. Anticipating this, some aggressors can convince themselves that threats will be abandoned once the risks grow too high, and deterrence can thus fail even when rhetorical commitments are in place. Sustaining a potential aggressor's belief in the threats became a major preoccupation of the deterrence literature, and Schelling brought the line of thinking to its natural conclusion: In order to deter, stating a commitment is not enough; a defender must show that it has no choice but to react.[39] The literature suggests several specific mechanisms for creating such unbreakable commitments: making clear public commitments and staking national prestige on a powerful response; agreeing to formal treaties of mutual defence; deploying trip wire forces; constructing a basing and logistical infrastructure that signals an intent to reinforce in case of war; and selling arms to the threatened state to reinforce defence ties.[40] Yet as noted above, creating commitments that cannot be abandoned imposes very significant political costs and will often be more than a defender is willing to do in peacetime.

Finally, one long-held claim about the credibility of deterrent threats has now been largely discredited: the idea that a state's general reputation for toughness and resolve is essential to deterrence. This claim supported the idea, which guided much of U.S. Cold War policy, that no example of Soviet aggression could be ignored. Because reputation was thought to accumulate through individual actions, standing firm across the board seemed essential. Reputations, either national or individual, can matter in specific cases. States and leaders sometimes act partly based on impressions of national resolve that border on stereotypes, and individual leaders do cultivate images in the international system. But recent scholarship has mostly debunked the idea that national reputation is a single unified good, like a bank account, whose overall value affects potential aggressors' calculations and is a dominant variable in determining deterrence outcomes. Multiple studies have demonstrated that leaders make situational, rather than dispositional, judgments about resolve—they ask whether a possible defender would fulfil a commitment in a specific case or context, rather than inferring general rules from a defender's overall track record.

Reputational commitments are not interdependent: A state's failing to respond in one case does not necessarily have any bearing on an adversary's belief that a state will respond on other issues. Some studies have modified this finding by explaining that relatively recent interactions with the same potential adversary can affect calculations of risk and thus the possibility of aggression. Conciliation toward a

[39]Schelling 1980, pp. 24–27, 36, 131, 134, 137, 187–188; and Schelling 2008, pp. 43–44. See also Russett 1963, pp. 98, 100–101. He stresses that public commitments themselves are not sufficient

[40]Crawford 2009, pp. 283–284.

specific potential aggressor, therefore, could increase the chances that it would challenge deterrence later.

2.6 Deterrence as a Complex and Nuanced Enterprise

This summary highlights three factors that should be kept in mind when considering the role of deterrence in U.S. national security strategy:

1. Preventing aggression is not strictly about making threats—it is also about offering assurances. Deterrence is best accomplished through broad-based strategies to dissuade a potential aggressor from seeing the need or opportunity for aggression.
2. Perceptions are everything, and the United States must always view a situation through the lenses of the potential aggressor's beliefs and preconceptions.
3. Successful deterrence typically involves a combination of taking the aggressor's motivations seriously, being clear about what the defender seeks to deter and what it will do if the threat is challenged, and taking steps to demonstrate both the capability and determination to fulfil a threat. In post–World War II cases where the United States has met these three criteria—such as Europe during the Cold War and Korea since 1953—it has generally succeeded in deterrence.

References

Beaufre A (1965) Deterrence and Strategy. Praeger, New York
Crawford T W (2009) The Endurance of Extended Deterrence. In: Paul T V, Morgan P M, Wirtz J J (eds) Complex Deterrence: Strategy in the Golden Age. University of Chicago Press, Chicago
Freedman L (2004) Deterrence. Polity Press, London
George A L, Smoke R (1974) Deterrence in American foreign policy: Theory and Practice. Columbia University Press, New York
Gross Stein J (2009) Rational deterrence against 'irrrational' adversaries? In: Paul T V et al (eds) Complex deterrence: strategy in the golden age. University of Chicago Press, Chicago, pp 58–82
Hotta E (2013) Japan 1941: Countdown to infamy. Alfred A. Knopf, New York
Huth P K (1988) Extended deterrence and the prevention of war. Yale University Press, New Haven, Connecticut
Huth P K (1999) Deterrence and international conflict: empirical findings and theoretical debates, annual review of political science 2:25–48
Huth P K, Russet B (1988) Deterrence Failure and Crisis Escalation. International Studies Quarterly 32:29–46
Jervis R (1983) Deterrence and perception. International Security 7:3–30
Jervis R (1989) Rational deterrence: theory and evidence. World Politics 41:183–207
Jervis R, Lebow RN, Gross Stein J (1985) Psychology and deterrence. Johns Hopkins University Press, Baltimore

Knopf J W (2009) Three items in one: deterrence as concept, research program and political issue. In: Paul T V, Morgan P M, Wirtz J J (eds) Complex deterrence: strategy in the golden age. University of Chicago Press, Chicago, pp 31–57
Lebow R N (1982) Misconceptions in American strategic assessment. Political Science Quarterly 97:187–206
Lebow R N (1983) The deterrence deadlock: is there a way out? Political Psychology 4:333–354
Lebow R N (2007) Thucydides and deterrence. Security Studies, 16:163–188
Lebow R N, Gross Stein J (1989) Rational deterrence theory: I think, therefore I deter. World Politics 41:208–224
Lebow N R, Gross Stein J (1990) Deterrence: the elusive dependent variable. World Politics 42:336–360
Levy J S (1988) When do deterrent threats work? British Journal of Political Science 18:485–512
Morgan P M (1983) Deterrence: a conceptual analysis. Sage Publications, Beverly Hills
Morgan P M (2003) Deterrence: now. Cambridge University Press, Cambridge
Mueller KP et al (2006) Striking first: pre-emptive and preventive attack in U.S. national security policy. RAND, Santa Monica
North Atlantic Treaty Organisation (1949) The North Atlantic treaty. Washington, D.C.
Office of the Secretary of Defense (2018) Nuclear posture review. Washington, D.C.
Paul T V (2009) Complex Deterrence: an introduction. In: Paul T V, Morgan P M, Wirtz J J (eds) Complex deterrence: strategy in the Golden Age. University of Chicago Press, Chicago
Russett B M (1963) The calculus of deterrence. Journal of Conflict Resolution 7:97–109
Schelling T (1980) The strategy of conflict. Harvard University Press, Cambridge
Schelling T (2008) Arms and influence. Yale University Press, New Haven
Snyder G H (1959) Deterrence by denial and punishment. Center of International Studies, Princeton

Michael Mazarr (Ph.D.) is a senior political scientist at the RAND Corporation. Previously he worked at the U.S. National War College, where he was professor and associate dean of academics; as president of the Henry L. Stimson Center; senior fellow at the Center for Strategic and International Studies; senior defense aide on Capitol Hill; and as a special assistant to the Chairman of the Joint Chiefs of Staff.

Chapter 3
Deterrence Rediscovered: NATO and Russia

Sten Rynning

Contents

Abstract The North Atlantic Treaty Organization (NATO) is back in the business of deterring aggression on the part of Russia. This return to great power deterrence has brought widely acknowledged military challenges related to power projection, force modernization, and burden sharing but also and notably a political challenge of defining NATO's collective political ambitions for a continental order in which Russia will not become like the West. Like during the Cold War, the most convincing posture for NATO has become one of deterrence by punishment, building on a fairly dynamic military ability to strike Russia at a point of choosing, as opposed to defending every entry point to Alliance territory. However, NATO, not sure of what political order it represents, struggles to read Russia's political character and intent and size its military posture accordingly. NATO's political deficit effectively robs it of a middle ground from where it can build its military posture and invest in its upkeep. In the 1960s, NATO forged such a middle ground as an essential platform for strategic adaptation; today, NATO's full deterrence posture is suffering from the absence of such a middle ground. Thus, a comprehensive

S. Rynning (✉)
University of Southern Denmark, Odense, Denmark
e-mail: sry@sam.sdu.dk

F. Osinga and T. Sweijs (eds.), *NL ARMS Netherlands Annual Review of Military Studies 2020*, NL ARMS, https://doi.org/10.1007/978-94-6265-419-8_3

politico-military posture of deterrence vis-à-vis Russia will require NATO's reengagement with its own political fundamentals.

Keywords North Atlantic Treaty Organization (NATO) · collective defence · grand strategy · reassurance · deterrence · access denial · horizontal escalation · burden sharing

3.1 Introduction

"We have debated this endlessly, and it is just not easy," one North Atlantic Treaty Organization (NATO) official remarked in early 2015 when asked to identify the principles underpinning NATO's new deterrence posture.[1] Russia had in the course of 2014 "fundamentally challenged our [NATO's] vision of a Europe whole, free, and at peace", and NATO spoke boldly of its determination to remain the "essential source of stability in an unpredictable world".[2] However, whether its deterrence would be by punishment or denial, how it would build on US extended deterrence, and how it would tie into dissuasion and persuasion, that was the question.

NATO authorities could take solace in the fact that, throughout Alliance history, the establishment of deterrence had been a delicate affair. The very first Strategic Concept for the Defence of the North Atlantic Area, of November 1949, put the creation of a "powerful deterrent" at its heart.[3] Still, the military chiefs of the Alliance responsible for strategic guidance and regional defence plans had to cope with changing political and organizational conditions within the Alliance—Greece and Turkey acceded to the treaty; Western Germany was on the horizon as a defence obligation; and NATO gained major commands to take over from its disparate regional planning groups—and then the fact, as they dryly noted, that the Strategic Concept "contains no assessment of the capabilities or possible intentions of the enemy".[4]

Through generations of debate illuminated earlier in this volume,[5] the scholarly deterrence community has been brought back to this square one where NATO chiefs at one time found themselves and where deterrence first and foremost is a question of tailoring threats to specific actors and their political desires. Fittingly, the argument of this chapter is that NATO, today as during the Cold War, is largely wedded to deterrence by punishment and maintains a solid and fairly dynamic military posture. However, then as now, NATO's political ability to read and adapt to Russia's political character and intent is limited.

[1]Background interview by author at NATO headquarters.

[2]NATO 2014, para 1.

[3]Donnelly 1949.

[4]Standing Group and Military Representatives Committee 1952.

[5]Mazarr 2018.

The chapter builds on the distinction between strategic planning and strategic improvisation, arguing that NATO's contains a far greater degree of improvisation than its reliance on plans, policies, and procedures indicate.[6] The ability to improvise in the face of an agile adversary is a quality, but, as we shall see, NATO improvisation occurs not least because of shortcomings in the Alliance's ability to set its own political compass. In terms of the three distinct components of grand strategy—"grand principles", "grand behaviour", and "grand plans"[7]—NATO's strong suit is unquestionably the pattern of military deployments and exercises that underpin "grand behaviour", whereas its distinct weakness is its inability to settle on "grand principles" and apply them in a reading of Russia's ambitions and intent. NATO's "grand plans" are thus sandwiched between solid military practice and the improvisation that flows from limited political abilities.

The literature on NATO deterrence of Russia post-2014 quite rightly highlights NATO challenges in terms of limited muscle and institutional memory when it comes to joint high-intensity warfare;[8] a political geography that favours Russian interior lines and confounds NATO plans of reinforcement;[9] and discomfort with a new interface between conventional and nuclear deterrence.[10] As the discussion of NATO's "grand behaviour" and "grand plans" will outline, NATO, rather than plugging every hole in its armour, must develop a posture of strength that unmistakably promises punishment in relation to Russian aggression. This is not simple, and among the issues to navigate are burden sharing and a common approach to manoeuvre warfare and new technology,[11] and ultimately, and as this chapter argues, it presupposes a clear understanding of the adversary. This is where NATO's forced improvisation should be of concern because it tells the story of Alliance hesitation on the key prioritization of politico-strategic intransigence[12] versus dialogue.[13] Whether one or the other should have priority in a grand strategic effort to bolster deterrence can only be determined after careful deliberation on the nature of the threat, and in this regard, NATO comes up short.

Sections 3.1 and 3.2 below examine these political shortcomings. Section 3.3 examines NATO's "grand behaviour", while Sect. 3.4 turns to NATO's politico-military planning—its "grand plan". The conclusion considers implications for NATO strategy.

[6]Popescu 2017, 2018.

[7]Silove 2018.

[8]Kroenig 2015; Sweijs and Osinga 2019.

[9]Shlapak and Johnson 2016; Veebel 2018; Zapfe 2017; and Zapfe and Haas 2016.

[10]Durkalec and Kroenig 2016; Larsen 2019.

[11]Simón 2016; Sweijs and Osinga 2019.

[12]Freudenstein 2016; German 2017.

[13]Kühn 2015.

3.2 Know Thyself, NATO

NATO is experiencing a gap between liberal values to which it is committed by treaty and a resurgence of national values that are not necessarily liberal. What NATO stands for is therefore up for debate, and the ramifications hereof run through all dimensions of its collective deterrence posture. In its official declarations, NATO remains steadfastly committed to "democracy, individual liberty, human rights, and the rule of law"—as reflected in its 1949 treaty and its London Declaration of December 2019 celebrating the Alliance's 70th anniversary.[14] The irony, though, is that NATO heads of state and government gathered in London a full eight months following this anniversary, and then in a lean and quick format that did not warrant the label "summit" but merely "meeting", because of underlying tensions between national values and outlooks.[15] At NATO's highest political level, discomfort about what NATO stood for had become patently visible.

NATO was thus in a situation where its conceptual coordinates were unable to guide allies in their search for grand objectives for grand strategy. Two such grand objectives were possible. One was to seek an accommodation with Russia along current lines of political influence in order to facilitate an explicit balance of power at the heart of Europe's security order. It would not imply the rollback of NATO, though some realists might advocate this course of action as a consequence of their distinctive criticism of NATO enlargement,[16] but a halt to the liberal ambition to aid in the transformation of Russian society and government and to ultimately build a continental order of liberal democracy.[17] The other option would be the inverse hereof—to support the aspirations of people wherever they may be for self-determination and greater freedom, and to use NATO as a mechanism for extending liberal-democratic norms into the former Eastern bloc.[18] It would be tantamount to harnessing power for political aspiration, where the other option would be to restrain aspiration for balanced power.

Multiple implications flow from these grand objectives. A strong aspirational commitment on the part of NATO would maintain enlargement in process, cause political discomfort in Moscow where it would be seen as invasive, and lead Moscow to instrumentalise conflicts outside of the Euro-Atlantic area for the purpose of diluting NATO. It would raise the requirements for NATO deterrence and, because the United States remains the sine qua non of collective defence and deterrence in NATO, markedly restrain the scope for the development of a European pillar.

NATO has been zigzagging on these objectives and remains perfectly willing to kick the can down the road, notably in regard to the membership prospects of

[14]NATO 2019.

[15]Burns 2019; Cook 2019.

[16]Mearsheimer 2014.

[17]Kissinger 2016; Rynning 2015.

[18]Gheciu 2005; Thies 2009.

Ukraine and Georgia. "We agreed today that these countries will become members of NATO," is how NATO heads of state and government put it in 2008,[19] but they have since postponed further formal steps with reference to political circumstance and conditions attached to the Alliance's Membership Action Plan. Ukraine and Georgia were thus not mentioned in the London Declaration of December 2019, and on Russia NATO remains steadfastly committed to the partnership framework, a Founding Act, agreed to in 1997.[20] How NATO can commit to the NATO-Russia Founding Act goal of an "undivided Europe" and simultaneously offer Ukraine NATO membership, strongly opposed by Russia, is the bullet NATO is dodging.

There is a direct link from NATO's inability to emphasize one or the other grand objective to the ongoing wider debate within NATO on whether collective and national interests can stand in opposition to one another. President Trump's "America First" agenda along with his reluctance to embrace NATO's Article V collective defence commitment and his contrasting frequent harsh criticism of allies' contributions lies at the heart of this agenda.[21] At issue is the extent to which the allies themselves can anchor their national interests in a common liberal framework, as opposed to having exclusive national interests that only on occasion coincide. In Henry Nau's perceptive assessment, the risk is one of nationalism within the NATO area developing into antagonisms based on blood (ethnicity), history (culture), soil (territory), or creed (ideology), which leads Nau to suggest pathways for "conservative internationalism" whereby traditional liberal concerns with free government and society get funnelled through renewed and reinvigorated national interests.[22] Conservative internationalism suggests that NATO can build on both liberal and national values: however, it would imply a diminished reliance on NATO as an institution, which to nationalists has become akin to an iron cage of rules and ties that inhibit political thinking and provide cover for freeriding, and an enhanced role for strong nations that step out front in the "political alliance" rather than the "constraining organization" (the "O" in NATO).

Such an alignment with a conservative merger of liberalism and nationalism would imply at least NATO's partial alignment with the balance-of-power option: the NATO institution would no longer serve as the anchor of liberal-democratic norm export and NATO nations looking to navigate a wider global context of Chinese power and other emerging issues would be inclined to want to reduce systemic tension with Russia. However, the attractiveness of such a set of conceptual coordinates is complicated by Russia's 2014 annexation of Crimea. The Alliance is strong in its opposition to this land grab and to any suggestion that there can be a return to "business as usual" for as long as Russia maintains it. The prospect of caving in to Russian coercion and manipulation is distinctively

[19]NATO 2008.

[20]NATO 1997.

[21]Kaufman 2017; Schreer 2019.

[22]Nau 2013, 2018.

unappealing across the Alliance. Unity on these points feeds a military deterrence posture we shall encounter below. However, it also feeds great uncertainty on the political objectives that deterrence is supposed to serve, and which, for now, remain the liberal set of values written into the 1997 Founding Act. Maintaining the 1997 vision of an undivided Europe is a way to stonewall Russian manipulation, of course, and the Alliance willingly exploits this irritant to Russian diplomacy, but it has de facto also become a substitute for moving NATO consensus on East–West political objectives forward.[23] President Trump's imbroglio in Russia investigations and an impeachment procedure motivated by his actions in Ukraine merely underscores how politically difficult it is for the Alliance as a whole to move forward politically on these issues.

Hal Brands has likened grand strategy to "the intellectual architecture that lends structure to foreign policy".[24] Going by this definition, NATO's grand strategy, within which Russia deterrence is embedded, is fractured in its intellectual architecture. NATO allies are unsure of their own value-base: of how longstanding liberal principles and renewed nationalism can coexist and perhaps even reinforce each other within the Alliance. This uncertainty inhibits collective reflection, and thus policy, on intransigent issues related to Russia. The default intellectual architecture NATO leans on dates back to 1997, and while this is politically convenient in terms of stonewalling Russia and buying time for NATO's internal diplomacy, it does little to give political direction to the Alliance's renewed deterrence posture.

3.3 Know Thy Enemy

As a consequence of NATO's uncertain value base, the Alliance struggles to come to grips with Russia's political intent. There can be no question that the allies are united in their opposition to Russia's annexation of Crimea. Equally, there is no question that the Alliance perceives and reacts to Russia's "new generation warfare" that is essentially a strategy of coercion centred on the "informational space" of Western societies.[25] New generation warfare is a cross-domain tool for compelling and deterring Western policy, and it makes no distinction between war and peace—a building block for Western thinking.

NATO has confronted Russia's new thinking in a number of policy respects, including societal resilience, enhanced intelligence cooperation, cyber security, and rapid decision-making. NATO's challenge lies elsewhere, namely in respect to the holistic assessment of Russia's political nature and intent on which policy must be based. A series of background interviews with NATO officials (conducted in May

[23]Ringsmose and Rynning 2017.

[24]Brands 2014, p. 1.

[25]Adamsky 2018.

and December 2019, as well as January 2020) convey the imagine of an Alliance that at the decision-making level—in the North Atlantic Council (NAC)—tends to be circumscribed and reactive. The NAC certainly addresses Russia but by and large in specific contexts, be it in regard to hypersonic weapons, intermediate range missiles, Black Sea presence, or other pressing issues. The advantage hereof is that NATO is able to interact with some agility with Russia without getting bogged down in difficult discussions of political philosophy. NATO has always heralded its operational, as opposed to philosophical, character, setting it apart from, say, the European Union. However, the disadvantage is that NATO, never really confronting the sum total of Russian actions, can come to rely on crude assessments of or mere assumptions about the nature and architecture of Russian ambitions.

NATO does possess institutionalized mechanisms designed to deliver holistic assessments of Russia—it is just that they connect poorly to the decision-making level.[26] The Joint Intelligence and Security Division established in 2014 is one such mechanism. The division at NATO's political-military headquarters does not gather its own intelligence but coordinates that offered by nations and integrates it into collective overviews of Russia's policy and actions. Such coordination is especially relevant in regard to "hybrid" threats that sow seeds of confusion in allied informational space. In addition, the deputy secretary general is in a unique position to guide the occasional and very scripted encounters between Russia and NATO in their NATO-Russia Council. Rose Gottemoeller, a Russian-speaking American diplomat, came to this post in 2016 and stayed on for three years, and by virtue of her extensive insight into Russian politics and security policy set a high standard for the position that her successors must seek to imitate. The Deputies' Committee—composed of the deputies to NATO ambassadors and in many ways the workhorse of the headquarters—holds monthly informal talks under the heading of "understanding Russia", and sometimes they invite external experts to share insights. Finally, and importantly, these collective mechanisms are open to the substantial Russia-knowledge that especially the larger NATO nations possess—and in particular the Quad (the United States, Britain, France, Germany)—which brings us back to the political level and the disconnect between collective expertise and political deadlock.

There was always a tension between NATO consultations on the one hand, which by nature are collective and cumbersome, and even more so in an enlarged Alliance, and informal big power consultations on the other. The Quad is a case in point, having emerged to manage German issues at the point where occupation rule came to a conclusion, in 1955, and then surviving and even prospering as a go-to format for big power coordination. The Quad became a "portable" format that the Quad countries deliberately kept apart from NATO in order to preserve confidentiality and flexibility.[27] This fault line between collective institutions and big power insight and diplomacy persists, but today it is aggravated by the underlying and

[26]Ringsmose and Rynning 2019, pp. 28–29.

[27]Haftendorn 1999.

widespread tension over basic NATO values. In other words, the Quad is as inflicted as other institutions by political disunion and is unable to come to the rescue of NATO.

NATO has appealed to the tried and tested dual-track approach of emphasizing both defence and dialogue, dating back to its Harmel doctrine of the late 1960s—after Belgian foreign minister Pierre Harmel—that offered the Soviet Union political dialogue within a framework of solid allied defence. Today, NATO sometimes adds "deterrence" to the equation and therefore speaks of 3 Ds—deterrence, defence, and dialogue.[28] However, in recognition of the poverty of dialogue without internal agreement, NATO in December 2019 agreed to undertake a "forward-looking reflection process" to "further strengthen NATO's political dimension including consultation".[29]

The mandate and composition of the group that must undertake this reflection process is contentious, though. The idea of setting up such a group was German, introduced into Alliance diplomacy in November 2019 to defuse tensions flowing from French President Macron's statement that NATO was "brain dead", but little was agreed apart from the lead role of their secretary general, Jan Stoltenberg. In the wake of the London meeting the idea was floated to turn this process into a precursor for revising NATO's capstone Strategic Concept, which would have forced NATO to define its broader Russia view, among other things, but this broad and ambitious idea was quickly and effectively killed.[30] What the reflection process will deliver remains to be seen, but it will likely be a workmanlike anticipation of how NATO can adjust to the outcome of the US presidential elections in November 2020. While NATO's broad understanding of the challenge posed by Russia is solidly anchored, NATO's holistic and detailed assessment of Russia's political nature and intent is lacking. There is ample expertise on Russia inside NATO and particularly within certain allied capitals, but the political framework for mobilizing and integrating it into an allied strategic assessment is weak and therefore ineffectual.

3.4 Grand Behaviour

In early 2020, the US Army began the exercise Defender-Europe 20, which involved the deployment of a division-size combat-credible force from the United States to Europe. Up to 30,000 US and allied troops would be involved in this "from fort to port" exercise that from a land forces standpoint, Lt. Gen. Cavioli, commander of US Army Europe, argued, shows how "the demonstration of our

[28]NATO 2016, para 11.

[29]NATO 2019, para 7.

[30]Background interviews, January 2020.

collective defence is our best deterrent".[31] With this, NATO was flexing its US-based follow-on force muscle that define the core of its ability to conduct major joint operations in Europe. Short of nuclear war, this capacity captures the essence of a NATO deterrence by punishment posture.

NATO had built up this capacity for deterrence by punishment with considerable care since 2014. Enhanced US investment in extended deterrence has formed the backbone hereof. This effort began in 2014 with the so-called European Reassurance Initiative which in the course of 2017 was upgraded to a European Deterrence Initiative, which has allowed the funding of a heel-to-toe presence (i.e., continued but rotational and not permanently stationed troops) of an Armoured Brigade Combat Team with enablers, a Combat Aviation Brigade, an Army Battalion, and a range of supporting infrastructure and exercise investments. What began as a one-year $1 billion emergency response to Russian aggression in 2014 had by 2020 grown into an ongoing $6 billion deterrence program and a primary funding source for the US European command.[32]

NATO allies have complemented this US investment in a number of ways. First of all, they have put more defence money on the table: NATO Europe and Canada invested $313 billion in defence in 2018 compared to $272 billion in 2014. Moreover, in June 2018 they committed to a NATO Readiness Initiative according to which they would have 30 battalions, 30 air squadrons, and 30 naval combat vessels ready to use within 30 days—with the details hereof being worked out through 2020. Also, in 2018, the allies agreed to reform their command structure, re-introducing the North Atlantic command in Norfolk, Virginia, and introducing a new support and logistics command in Ulm, Germany, both designed to secure lines of communications and enable transatlantic reinforcements to NATO's eastern frontiers. In addition, the reformed command structure gained a Cyberspace Operations Centre, following NATO's 2016 decision to recognize cyberspace as a domain of operations.

All these measures bolster NATO's conventional deterrence by punishment posture. The ultimate source of deterrence by punishment is nuclear, and NATO has in this regard undertaken significant but still limited steps. The Alliance revived its nuclear consultations in the course of 2015, including a nuclear consultation exercise based on an Article 5 (collective defence) scenario, and its Warsaw Summit communiqué contained an unprecedented number of references to nuclear forces, even if they mainly rehashed past language of restraint (i.e., "The circumstances in which NATO might have to use nuclear weapons are extremely remote").[33] NATO language will have to change and reflect doctrinal adaptation, according to the warning of two prominent analysts: Russian doctrine is premised

[31]Judson 2019. Defender Europe 20 has since been put on hold on account of COVID-19.

[32]The budget for EDI is not drawn from the Department of Defense's base budget, but its Overseas Contingency Operations fund. As the name indicates, this funding stream is contingent but has achieved a remarkable degree of permanence and an equally remarkable size of almost $175 billion per fiscal year (Department of Defense 2019).

[33]NATO 2016; Kamp 2019.

on the early introduction of nuclear weapons in armed conflict, and NATO must do away with its "extremely remote" doctrine in favour of a "decisive response" doctrine; and this doctrine must underpin NATO's ability to strike into Russia with conventional weapons to deter a limited Russian "land grab" operation in Estonia or elsewhere, they contend.[34] In short, NATO has taken steps to reinforce its nuclear deterrence but still has some work cut out at these upper levels of the ladder of escalation.

Deterrence by denial (i.e., an ability to deny Russian objectives by defensive measures) is only possible for NATO at the lower rungs of this ladder, and NATO has not been idle here either. In fact, most of the early measures taken by NATO in response to the annexation of Crimea fall into the deterrence of denial category and centre on rapid reaction capacities, especially in the shape of a NATO Response Force (NRF) upgraded for deterrence purposes. The NRF now has a reinforced, quicker spearhead—a Very High Readiness Joint Task Force potentially up to 13,000 troops strong, and then two complementing brigades with support (each 13,000 strong) forming a layered, sizeable reaction force explicitly linked to collective defence purposes and regularly exercised in Eastern Europe and the Baltic states.[35] In 2016, in response to the foreseeable difficulties of projecting mainly Western forces into zones of conflicts close to Russia, NATO decided to established an "enhanced forward presence"—four multinational battalion-sized battle groups—in the Baltic states and Poland, and a "tailored forward presence"—mainly naval forces—in the Black Sea region.

Whether these forces can credibly "deny" Russian objectives in the case of limited war is a bone of contention. Most observers and sometimes NATO itself employ the descriptor "tripwire" to these forces, thus indicating that they are triggers that promise to unleash NATO's big guns and therefore part and parcel of deterrence by punishment. However, US diplomats (interviewed on background) feel more confident that the US battalion embedded (in Poland) in the collective forward presence posture would actually be able to fight and survive, and thus deny Russian objectives. That may be so, in which case the conclusion is that NATO has a moderate-to-low—and geographically focused—capacity for deterrence by denial and then a more general and impressive capacity for deterrence by punishment.

NATO's unquestionable capacity for deterrence by denial is rather found at the level of grey zone, non-kinetic conflict. In this regard, NATO has upgraded not only its cyber defences and enhanced intelligence coordination, as mentioned, but has enhanced coordination with the European Union on hybrid threats, with a 2016 joint declaration leading to a common work program and a collaborative Centre of Excellence for Countering Hybrid Threats, located in Helsinki, the 2016 adoption of societal resilience benchmarks that, while mostly falling outside NATO's political-military remit, nations must meet, and finally the decision in 2018 to

[34]Binnendijk and Gompert 2019.

[35]Ringsmose and Rynning 2019.

organize counter-hybrid support teams that can tailor assistance to individual allies and circumstances.[36]

NATO's full range of actions in response to Russia's 2014 annexation of Crimea —a range to which this brief overview can do only limited justice—thus combines deterrence by denial (grey zone conflict, societal resilience, reaction and forward deployed forces to counter limited land grabs) and deterrence by punishment (the full chain of reaction and deployable forces, from conventional to nuclear). NATO's strong suit is the military piece of this posture, but it has considerably adapted to grey zone conflict scenarios in an effort to achieve a comprehensive deterrence posture vis-à-vis Russia's unified (kinetic and non-kinetic) and uninterrupted (all domains, in war and peace) doctrine of "new generation warfare".[37]

3.5 Grand Plans?

NATO's robust military response to Russian aggression is ultimately dependent on coherent politico-military guidance. In this regard NATO benefits from the routine and leadership embedded in its integrated military command structure, capped off by the double-hatted US general serving as both NATO's supreme allied commander (SACEUR) and commander of US forces Europe (EUCOM), currently General Tod D. Wolters. A number of challenges related to political priorities beset this planning, however.

NATO has adopted a revised "military strategy" (MC 400/4), which is a first since its adoption of its flexible response strategy in 1967 (MC 400/3). The long interlude can be explained by the appropriateness of MC400/3 through the remaining Cold War years and then NATO's post-Cold War need to improvise "other than war" crisis response operations, which had limited import for the strategy's peer-to-peer focus. This changed in 2014 with Russia's aggression in Ukraine, and by 2017 NATO's Military Committee, composed of allied Chiefs of Defence, who was tasked to work on an integrated new military strategy fit for purpose. The Military Committee was able to approve this new strategy, MC400/4, in May 2019.[38] Next steps are to operationalize it, secure political approval by Ministers of Defence in June 2020, and enable SACEUR to draw up concrete plans and directives for his subcommands.

Two key concepts inform the new military strategy: theatre-wide approach and horizontal escalation, with both largely tying into NATO's overarching strategy of deterrence by punishment. The theatre-wide approach is NATO's military answer to the complexity of NATO geography: it is to say that NATO will not divide its planning and forces regionally but instead insists on having an integrated and

[36]Rühle and Roberts 2019.

[37]Adamsky 2018.

[38]Peach 2019.

seamless approach to defence and deterrence in the Euro-Atlantic area. NATO initially responded to Russia by drawing up Graduated Response Plans (GRP) that were geographically compartmentalized, covering segments of NATO's frontier from the North Atlantic through Central Europe to the eastern Mediterranean. A key weakness in this response was NATO's limited ability to think and move across these GRP compartments, leading to the search for a truly "theatre-wide" capacity for defence and deterrence. The answer lay in the other key concept, horizontal escalation, by which NATO means military forces able to move across NATO territory at the "speed of relevance".[39] The aforementioned 4 × 30 Readiness Initiative along with the revised command structure are key enablers hereof.

NATO's military strategy largely builds on deterrence by punishment because of its theatre-wide and therefore asymmetrical threat of escalation. It leaves Russia guessing where NATO could respond to an attack, simply promising Russia that NATO has this asymmetrical capacity and intent. There remains an element of deterrence by denial in so far as NATO maintains high readiness forces along with enhanced forward presence forces to bolster its territorial defence, particularly in the Baltic area; for larger threats of Russian force, though, NATO resorts to its counter-threat of theatre-wide escalation and therefore deterrence by punishment.

It is with a degree of timidity that NATO agreed to this posture. Initially, in 2014–2015 when NATO agreed to the GRPs, the allies were divided between two opposite desires, one of developing Cold War-style elaborate defence plans against Russia, and another of sticking to broad stroke contingency plans. The GRPs were a compromise: they had distinct geographies and reaction forces attached to them, but the reaction forces were limited in number (essentially, the NATO Response Force), the GRPs were not coordinated, and there were only contingency plans for follow-on forces. SACEUR has been a primary institutional actor in the effort to solidify this compromise and move NATO to a more stringent—more deterring—posture of theatre-wide punishment. In December 2018 SACEUR delivered his "strategic thoughts" on the draft military strategy that had come out of internal consultations between NATO military authorities.[40] SACEUR used the occasion to great effect, challenging the allies to place the credible deterrence of Russia at the heart of their thinking. Put differently, the tendency to think broadly and inclusively, to give as much thought to counterterrorism and stability operations as to Russia, and to settle for diplomatically appealing but ineffective GRPs, muddled NATO's posture and failed to offer a robust allied response to Russia's challenge.[41]

While it was always impossible for political reasons in a diverse alliance to give sole attention to just one threat, namely Russia, SACEUR's intervention did succeed in upgrading allied thinking on this particular threat. The military strategy that the Chiefs of Defence approved in May 2019 thus involves a range of threats—from Russia over counterterrorism to stability operations—but its centre of gravity

[39]Background interviews NATO headquarters, May and December 2019.

[40]A so-called Bi-SC (Strategic Command) Strategic Considerations Report.

[41]Background interviews at NATO headquarters, May and December 2019.

is the emphasis on theatre-wide defence and horizontal escalation that SACEUR had in mind.

The military strategy ultimately depends on political support for its success, of course. Here the encouraging news is that NATO allies have approved not only the military strategy but also some of the key measures that enable it: from the readiness initiative over the enablement focus within the command structure to an intensified training and exercise schedule. As might be expected, though, the allies remain preoccupied by burden sharing issues that to a degree could delay implementation. The 4 × 30 readiness initiative is particularly cumbersome to stand up: readiness is costly because forces are paid to be on standby, just as training and exercises are costly; it is not clear how these ready units will combine and be integrated in the command structure, meaning SACEUR's command authority remains undefined as do implications of the ready forces in NATO's Response Force; and, finally, it is not clear how big a role US forces will play in the 4 × 30 package. The US approach is to steer clear of these wider questions—that some European allies are wanting to address right away—in order to keep the focus stringently on the readiness initiative itself. Put differently, the United States does not want some allies to be able to hide behind an organizational screen and defray costly reforms at home.

The political commitment to following through with the military strategy is therefore the question. NATO has politically chosen to emphasize deterrence by punishment: this is its theatre-wide approach with flexible, exercised, and ready forces. The alternative would be to deter by denial by identifying critical strong points that Russia would need to attack and building up strong defences around them. The alternative is appealing because it relies less on the ultimate deterrent of nuclear weapons.[42] However, given NATO's geography—where Russia has formidable access denial capacities in some areas and can ignore geographical constraints in others, considering its broad "new generation warfare" toolbox, and where every NATO ally sees itself as a valuable strong point—NATO cannot politically opt for denial. NATO has almost by default, though with some timidity, as we saw, opted for deterrence by punishment. Its military command has produced a coherent plan—a military strategy—for realizing this posture, but as with any military strategy, it is hostage to the clarity and collective strength offered by the Alliance's conceptual coordinates with which this chapter began.

3.6 Conclusion

NATO has committed largely to deterrence of Russia by punishment. The Alliance maintains certain elements of deterrence by denial—notably resilient societies and a degree of strong point defence (i.e., enhanced forward presence), but with the

[42]Gallagher 2019.

understanding that Russia cannot be denied if it throws its full military weight into an attack on allied territory at a point and time of its choosing. NATO's commitment to theatre-wide asymmetrical and horizontal escalation, premised on trained and tested response and reaction forces and an enablement command, follows. NATO's is a strategy of punishment intended to leave Russia in the dark as to the timing and nature of NATO's response to its aggression.

NATO has arrived at this posture gradually, moving from measures to reassure exposed allies to a posture of deterrence of Russia. In this movement, NATO has varied its emphasis on immediate reaction forces, in-place forces, and, now, reaction forces for the European theatre, just as it has varied its stance on contingency and defence planning. NATO has slowly but surely engaged a debate of its nuclear posture and doctrine, dusting off nuclear consultation mechanisms and exercises, though critics will say that there is room for improvement here, an argument that could applied equally to the conventional and nuclear domains. Still, in terms of "grand behaviour" and "grand plan", NATO's design for and commitment to deterrence by punishment is clear and emerging.

The conceptual coordinates flowing from "grand principles" are trickier. NATO allies are in disagreement on the extent to which it is possible to coexist with Putin's Russia in a balance of power arrangement or, inversely, the extent to which continental order depends on the transformation of the character of Russia's political regime. Worryingly, uncertainty in regard to Russia is tied to, and in many ways flows from, uncertainty within the Alliance on NATO or Western values. Nationalist doctrines are challenging classical liberal doctrines in many allied capitals, and what this means for NATO strategy is simply unclear. NATO's collective response has been to stick to old guns—the partnership vision of 1997—and attend to the military "behaviour" and "plans" on which allies can agree.

In the Cold War, NATO's flexible response strategy (MC 400/3) reflected a political compromise. The United States preferred as much conventional defence as possible, paid for by European allies, and thus as much deterrence by denial as possible. The European allies preferred deterrence by punishment and thus NATO's threat of quick and flexible escalation to nuclear war, effectively tying the fate of Western Europe to that of the United States. MC 400/3 captured the middle ground. Today, European allies are equally committed to deterrence by punishment but in doubt on how much to deliver, partly because the widespread refusal to fall back on flexible nuclear deterrence raises the costs of conventional reform, partly because they are not in agreement on the nature of the Russia threat. The United States is pushing the European allies to undertake these reforms and investing its own conventional muscle in Euro-Atlantic deterrence, but it is so mired in domestic disagreement on Russia and foreign policy that it can offer NATO little politico-strategic guidance here. There is thus no political middle ground from where MC 400/4, NATO's new military strategy, can be built.

NATO continues to face critical decisions in terms of future military technology, defence plans, and training and early warning regimes, and the challenge hereof should not be diminished by the encouraging reading offered here that in terms of "strategic plans" and "strategic behaviour", NATO has managed to put together a

fairly credible and dynamic deterrence posture. Less encouraging and ultimately more alarming is the conclusion that NATO's ability to dedicate its political mind to reading the character and intent of its rival is limited. Worryingly, the political and economic fallout from the 2020 Corona pandemic could likely exacerbate the internal political fractures that explain this poor condition.[43] NATO's political condition is thus of direct and immediate consequence for its deterrence posture, and the building of a political middle ground for its military strategy should be a primary concern for Alliance leaders.

References

Adamsky D (2018) From Moscow with coercion: Russian deterrence theory and strategic culture. Journal of Strategic Studies 41:33–60

Binnendijk H, Gompert D (2019) Decisive response: a new nuclear strategy for NATO. Survival 61(5):113–28. https://doi.org/10.1080/00396338.2019.1662119

Brands H (2014) What good is grand strategy?: power and purpose in American statecraft from Harry S. Truman to George W. Bush. Cornell University Press, New York NY

Burns N (2019) Trump Violates Diplomacy's Golden Rule. https://www.theatlantic.com/ideas/archive/2019/12/at-nato-summit-trump-abuses-americas-closest-friends/602959/. Accessed 22 January 2020

Cook L (2019) NATO under friendly fire as leaders ready for London summit. https://www.pbs.org/newshour/world/nato-under-friendly-fire-as-leaders-ready-for-london-summit

Department of Defense (2019) Fiscal Year 2020 Budget Request

Donnelly C H (1949) Note by the Secretary to the North Atlantic Defense Committee on the Strategic Concept for the Defence of the North Atlantic Area

Durkalec J, Kroenig M (2016) NATO's Nuclear Deterrence: Closing Credibility Gaps. Polish Quarterly of International Affairs 25:37–50

Freudenstein R (2016) Why there will be no Helsinki II-and why confidence building with Putin's Russia is a bad idea. European View 15:3–11

Gallagher M (2019) State of (Deterrence by) Denial. Washington Quarterly 42(2):31–45

German T (2017) NATO and the enlargement debate: enhancing Euro-Atlantic security or inciting confrontation? International Affairs 93:291–308

Gheciu A (2005) NATO in the "new Europe": the politics of international socialization after the Cold War. Stanford University Press, Stanford, CA

Gordon P H, Shapiro J (2020) The Atlantic Alliance had Preexisting Conditions: The Pandemic Will Worsen Them. https://warontherocks.com/2020/04/the-atlantic-alliance-had-preexisting-conditions-the-pandemic-will-worsen-them/

Haftendorn H (1999) The "Quad": Dynamics of Institutional Change. In: Haftendorn H, Keohane R O, Wallander C A (eds) Imperfect Unions: Security Institutions over Time and Space. Oxford University Press, Oxford, pp 162–193

Judson J (2019) Fighting the bureaucracy: For NATO, the Defender 2020 exercise in Europe will test interoperability. https://www.defencenews.com/digital-show-dailies/ausa/2019/10/11/fighting-the-bureaucracy-for-nato-the-defender-2020-exercise-in-europe-will-test-interoperability/. Accessed: 22 January 2020

[43]Gordon and Shapiro 2020.

Kamp K H (2019) NATO's nuclear resurgence In: Ozawa M (ed) The Alliance Five Years after Crimea: Implementing the Wales Summit Pledges. Research Paper No 07. NATO Defence College, pp 11–18
Kaufman J P (2017) The US perspective on NATO under Trump: lessons of the past and prospects for the future. International Affairs 93:251–266
Kissinger H (2016) Russia should be perceived as an essential element of any new global equilibrium. National Interest
Kroenig M (2015) Facing Reality: Getting NATO Ready for a New Cold War, Survival 57:49–70
Kühn U (2015) Deter and Engage: Making the Case for Harmel 2.0 as NATO's New Strategy. New Perspectives: Interdisciplinary Journal of Central & East European Politics & International Relations 23:127–157
Larsen J A (2019) NATO nuclear adaptation since 2014: the return of deterrence and renewed Alliance discomfort. Journal of Transatlantic Studies 17:174–193
Mazarr M J (2018) Understanding Deterrence. https://www.rand.org/pubs/perspectives/PE295.html
Mearsheimer JJ (2014) Why the Ukraine crisis is the West's fault: the liberal delusions that provoked Putin. Foreign Affairs 93(5):1–12
NATO (1997) Founding Act on Mutual Relations, Cooperation and Security between NATO … . http://www.nato.int/cps/en/natohq/official_texts_25470.htm. Accessed 15 January 2020
NATO (2008) Bucharest Summit Declaration - Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on 3 April 2008. http://www.nato.int/cps/en/natohq/official_texts_8443.htm. Accessed: 15 January 2020
NATO (2014) Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales. http://www.nato.int/cps/en/natohq/official_texts_112964.htm. Accessed: 15 January 2020
NATO (2016) Warsaw Summit Communiqué. https://www.nato.int/cps/en/natohq/official_texts_133169.htm
NATO (2019) London Declaration. http://www.nato.int/cps/en/natohq/official_texts_171584.htm. Accessed: 15 January 2020
Nau H R (2013) Conservative internationalism: armed diplomacy under Jefferson, Polk, Truman, and Reagan. Princeton University Press, Princeton, NJ
Nau H R (2018) Why "Conservative," Not Liberal, Internationalism? Orbis 62:22–29
Peach S (2019) Press statement by Air Chief Marshal Sir Stuart Peach, Chairman of the NATO Military Committee at the Joint Press Point with SACEUR and SACT following the Military Committee in Chiefs of Defence Session. NATO. 22 May 2019. http://www.nato.int/cps/en/natohq/opinions_166242.htm
Popescu I C (2017) Emergent strategy and grand strategy: how American presidents succeed in foreign policy. Johns Hopkins University Press, Baltimore
Popescu I C (2018) Grand Strategy vs. Emergent Strategy in the conduct of foreign policy. Journal of Strategic Studies 41:438–460
Ringsmose J, Rynning S (2017) Now for the Hard Part: NATO's Strategic Adaptation to Russia. Survival 59:129–146
Ringsmose J, Rynning S (2019) NATO og Rusland mellem strategisk konfrontation og stabilitet. DIIS Report No. 2019:07
Rühle M, Roberts C (2019) NATO's Response to hybrid threats. In: Ozawa M (ed) The alliance five years after crimea: implementing the wales summit pledges. Research Paper No 07. NATO Defence College, pp 61–70
Rynning S (2015) The false promise of continental concert: Russia, the West and the necessary balance of power. International Affairs 91:539–552
Schreer B (2019) Trump, NATO and the Future of Europe's Defence, The RUSI Journal 164:10–17
Shlapak D A, Johnson M (2016) Reinforcing Deterrence on NATO's Eastern Flank: Wargaming the Defence of the Baltics

Silove N (2018) Beyond the Buzzword: The Three Meanings of "Grand Strategy". Security Studies 27:27–57
Simón L (2016) The 'Third' US Offset Strategy and Europe's 'Anti-access' Challenge. Journal of Strategic Studies 39:417–445
Standing Group and Military Representatives Committee (1952) Decision on S.G. 1/7, The Strategic Concept for the Defence of the North Atlantic Treaty Area (S.G. 1/7 Final)
Sweijs T, Osinga F (2019) Maintaining NATO's Technological Edge. Whitehall Papers 95:104–118
Thies W J (2009) Why NATO endures. Cambridge University Press, Cambridge, NY
Veebel V (2018) NATO options and dilemmas for deterring Russia in the Baltic States. Defence Studies 18:229–251
Zapfe M (2017) Deterrence from the Ground Up: Understanding NATO's Enhanced Forward Presence. Survival 59:147–160
Zapfe M, Haas M C (2016) Access for Allies? The RUSI Journal 161:34–41

Prof. Sten Rynning is Professor of War Studies and Vice Dean for Research at the faculty of business and social sciences, the University of Southern Denmark (SDU) in Odense, Denmark. Sten Rynning founded the Center for War Studies at SDU in 2011 and headed it until 2019.

Chapter 4
The Continuing Relevance of Conventional Deterrence

Karl Mueller

Contents

Abstract This chapter examines the theoretical principles that underpin conventional deterrence and its evolution in practice over the past century. It disaggregates conventional deterrence approaches into four strategic categories based on their geographic scope and the nature of the threats they employ, and focuses in particular on strategies of punishment through resistance to an invader on the battlefield. It concludes with an assessment of the strengths and limitations of conventional and nuclear deterrence, and a set of summary principles for conventional deterrence strategy makers.

Keywords airpower · Baltic States · coercion · credibility · defence · deterrence · misperception · nuclear weapons · strategy · Taiwan

The opinions expressed in this chapter are the author's and do not represent the views of the RAND Corporation or any element of the U.S. government.

K. Mueller (✉)
RAND Corporation, Washington, USA
e-mail: Karl_Mueller@rand.org

F. Osinga and T. Sweijs (eds.), *NL ARMS Netherlands Annual Review of Military Studies 2020*, NL ARMS, https://doi.org/10.1007/978-94-6265-419-8_4

4.1 The Nature of Deterrence

Deterrence comes in many forms. In the world of national security, the term tends to be most readily associated with nuclear threats, but even in the nuclear age most military deterrence revolves around conventional capabilities. This is often underappreciated since successful deterrence draws little attention. This chapter examines the subject of conventional deterrence, and the question of how it fits into the security landscape of the early 21st century. Defined at the brevity of a tweet, "deterrence is causing someone not to do something because they expect or fear that they will be worse off if they do it than if they do not".[1] We practice and study deterrence in a wide variety of contexts ranging from nuclear crises to crime prevention,[2] but here the focus is on deterring interstate and similar aggression: starting wars, launching other sorts of military attacks, and expanding or escalating armed conflicts.[3]

Other chapters in this volume discuss the nature and dynamics of deterrence in general, but four key points about it are worth reiterating before we delve into conventional deterrence in particular. First, deterrence (like other forms of coercion) involves making an opponent that has the ability to attack choose not to do so. Action that makes it impossible for an attack to take place, such as preventively disarming or destroying the opponent, is not deterrence, instead it is what Thomas Schelling dubbed "pure" or "brute" force.[4] Although brute force can be an effective way to deal with security threats, especially when the enemy is weak or vulnerable, coercion is usually more attractive if it can be achieved, particularly when successful deterrence means a war will not have to be fought.

Second, deterrence is not the same thing as simply making war look costly or risky but depends on making war look worse than the alternative. Deterrence tends to be relatively easy if the opponent considers the peacetime status quo to be reasonably acceptable, as most states do most of the time. However, a desperate actor may decide to attack even when starting a war appears dangerous if it expects that not doing so would be worse—Japan in 1941 is the evergreen example of a state deciding that going to war was the least bad of several unappealing options.

Third, there are a variety of ways to make aggression appear to be a bad idea compared to other options. Increasing the expected costs of aggression through threats of punishment (punitive deterrence) and making it appear unlikely that aggression will be successful in achieving its objectives (deterrence by denial), whether by military or other means, are the approaches most strongly associated

[1] Mueller 2018, p. 78.

[2] Freedman 2004, pp. 60–68; Kleiman 2009.

[3] The discussion below will give escalation short shrift. For more on the subject, see Morgan et al. 2008.

[4] Schelling 1966, Chap. 1. In Schelling's now-widely accepted terminology, coercion comprises deterrence and compellence, which is causing someone to change their behavior rather than causing them not to take an action not yet underway.

with deterrence. But the prospects for successful deterrence can also be improved by making not going to war look more attractive though reassurance measures or promises of rewards. Some have aptly referred to these types of promises as "positive deterrence" but that seemingly oxymoronic label has never been widely embraced.[5] However, whether or not one defines such measures as deterrence *per se*, they are fundamental to the deterrence calculus and must be taken into account by good strategists and analysts.[6]

Finally, and most importantly, deterrence occurs in the mind of the potential aggressor. The opponent's choice of action depends on what it *believes* about the future consequences of its options—the actual costs and benefits of war and probabilities of success and failure will only affect the deterrence calculus insofar as they shape these subjective expectations. (Of course, objective reality will become very important indeed if deterrence fails and the war begins.)[7] Decision makers can misperceive reality for many reasons, and future events are often inherently difficult to predict, so many wars are started by states that would have been better off if they had decided not to attack. The most robust deterrence strategies will be those that make a case that aggression would be a bad idea which is compelling enough to overcome any potential inclination toward war resulting from such misperception.

The concept of deterrence is agnostic regarding the tools that can be used to make deterrent threats.[8] Because modern deterrence theory was developed in response to the advent and proliferation of nuclear weapons, and for several decades deterrence scholarship focused on them as both the principal tool of then-contemporary deterrence and the principal threat in need of being deterred, "deterrence" became strongly associated with nuclear strategy. Theorists today rarely suggest, as some once did, that use of the term "deterrence" should be limited exclusively to nuclear deterrence, but it is still common, for example, for "deterrent" to be U.S. doctrinal shorthand for matters involving strategic nuclear forces. But deterrence long predated the nuclear revolution, and of course non-nuclear deterrence is the only sort that many states have the ability to practice. Moreover, the long and lengthening tradition of non-use has made nuclear weapons recede into the background of many of the deterrent relationships is which they do play a role.[9]

[5]Milburn 1959; Baldwin 1971.

[6]Huth and Russett 1990, p. 471.

[7]This is the point at which deterrence gives way to defense: the former involves making the expected results of war look unattractive to the opponent, the latter involves making the actual consequences of war better for yourself. See Snyder 1961, Chap. 1.

[8]Posen 1984, p. 15.

[9]Paul 2009.

4.2 Unpacking Conventional Deterrence

The term "conventional deterrence" came into wide use in the 1980s, particularly associated with the work of John Mearsheimer, including his book of the same name.[10] It implies on one hand that deterrence using conventional threats is meaningfully different from nuclear deterrence, but also that they are much alike. One could define conventional deterrence as all deterrence that doesn't involve threats to use nuclear (or other unconventional) weapons, but the non-nuclear deterrence category includes too many dissimilar elements to provide much analytical utility. Instead for this discussion we will bound it more narrowly to encompass deterrent threats to resist or to inflict costs against an aggressor using conventional military force during the resulting conflict. This is still fairly expansive, taking in measures ranging from fighting an invader on the battlefield to launching punitive military attacks against targets far removed from the scene of the aggression to irregular partisan warfare against the enemy in territory it has occupied. However, it excludes non-military threats of economic sanctions or diplomatic shaming, and any measures to inflict costs, deny benefits of conquest, or reverse the outcome of the war after hostilities end.

Within this scope exist several differentiable sub-categories of conventional deterrence, though in practice the boundaries separating them are often less than distinct. Table 4.1 portrays four ideal types in terms of the type of deterrent threat they involve and the extent to which they focus on the specific theatre of the potential enemy attack. Much of the ensuing discussion will apply to all of them, but because some are more familiar than others, we will not give each one equal attention.

Battlefield Defeat. Proceeding anti-clockwise from the upper left quadrant of the diagram, we start with the approach that is least novel in historical terms. Threatening to defeat an enemy that attacks you has been a basic element of military strategy since before strategy, let alone deterrence, had a name.[11] The deterrent message is "if you attack me, your forces will be defeated so you will not reap the rewards you hope to achieve by your action," or in more microeconomic terms, the probability of success is too low for attacking to be worthwhile. How convincing such a threat will be depends on the opponent's expectations about the offensive and defensive capabilities of the respective parties, taking into account factors such as whether the attacker believes that it can employ a strategy against which the defender is unlikely to be able to defend effectively. If so, it may be hard to deter even a significantly weaker opponent—James Wirtz labels this problem of an aggressor doubting that the defender will be able to fight effectively "contestability".[12] In general, the greater the relative capabilities of the attacker are, the harder it will tend to be for threats of battlefield defeat to carry deterrent weight.

[10]Mearsheimer 1983; Mearsheimer 1981–1982.

[11]Freedman 2013, pp. xii–xiii.

[12]Wirtz 2018.

Table 4.1 Conventional Deterrence Categories (*Source* The author)

		Scope	
		Operational	*Strategic*
Threat	*Denial*	**Battlefield Defeat**	**Strategic Defeat**
	Punishment	**Punitive Resistance**	**Strategic Retaliation**

Because such threats are very familiar, we will not pay them much further attention here.

Punitive Resistance. The basic idea that a potential aggressor may be deterred by the prospect of suffering heavy losses if it goes to war is also commonsensical, but such threats lie at the heart of conventional deterrence. Here the threat is "if you attack us we cannot guarantee that you will lose, but we will inflict such heavy losses on your forces that even if they ultimately win, the cost of doing so will outweigh any benefits you may gain". This is a natural approach to military deterrence for a weak state facing a powerful enemy that it has little hope of defeating, classically illustrated by the defensive military strategies of states such as Switzerland. The core of Mearsheimer's argument was that it can also be a powerful enough threat among major powers to make war appear too costly to be worth fighting, citing as evidence a consistent pattern in modern history of industrialized states attacking each other only when they believed that the ensuing war would be short and relatively inexpensive, and not being willing to embark on conflicts that they expected to result in costly wars of attrition whether ultimately successful or not.[13] Punitive resistance is a more purely deterrent approach than threatening battlefield defeat in the sense that carrying out the strategy if deterrence fails may not benefit the defender very much even though it punishes the attacker, and surrendering early in a conflict will typically be less costly to the defender than fighting on only to surrender later.

Strategic Retaliation. Deterrence can also involve threats to punish an aggressor by using conventional forces to attack targets less directly related to resisting the enemy attack, a deterrent approach most famously associated with nuclear retaliation but one that was also prominent in the decades before Hiroshima once airpower evolved to the point that it could range enemy territory far beyond the

[13]Mearsheimer 1983.

vicinity of the battlefield.[14] The better part of a century ago, such threats tended to be directed against targets such as enemy cities—counter-value targets in nuclear strategy parlance—but increasingly accurate munitions including long-range missiles give strategists a wider range of targeting options today. This might be particularly promising in cases where the enemy considers heavy losses on the battlefield to be a price worth paying to achieve its objectives, but depends on being able to hold targets at risk that the adversary values more. This category also includes many threats of horizontal escalation: threatening to respond to an attack by the enemy at a time and place of its choosing by striking back somewhere else where the defender enjoys a military advantage.[15]

Strategic Defeat. Finally, a deterrer can threaten "we may not be able to prevent your attack from succeeding, but that will be merely the first phase of a longer war, which we will ultimately win". Credibly threatening to defeat the enemy in the long run depends, of course, on being able to survive the initial onslaught, so it does not lend itself to deterrence by weaker states without allies. However, it may be well-suited for extended deterrence by major powers in places that are difficult to defend—provided that the prospective aggressor believes that the deterrer will not only be able to prevail in a longer conflict, but also will be sufficiently determined to see it through.

These strategy types tend to overlap considerably in practice, of course. Fighting to defeat an attacker will also impose costs on it, retaliatory attacks against an enemy's homeland may also weaken its military capabilities at the front, and so on. But the distinctions are worth drawing because of the differences among their characteristics, advantages, and limitations. As an illustration we can consider military strategies in each category that might be employed in the often recently-discussed case of NATO seeking to deter a potential Russian invasion of the Baltic States.[16] A battlefield defeat threat would be simple in theory though challenging in practice: preparing a defence of the Baltics potent enough to appear capable of stopping an invasion force before it reached its objectives; this would appear to require a considerably large Alliance military presence than currently exists there.[17] A threat of punitive resistance would be less ambitious and more programmatically feasible: preparing to exact sufficiently heavy costs from an invading force to make an invasion look unattractive. Strategic retaliation would focus not on the difficult problem of defending the Baltic allies, but instead threaten to impose heavy costs on the Russians elsewhere, such as by striking high-value targets in metropolitan Russia or responding with attacks against more vulnerable Russian territory or forces in other theatres. A strategic defeat approach would not

[14]Quester 1966; Overy 1992.

[15]Epstein 1983/84; Morgan et al. 2008, Chap. 2.

[16]Shlapak 2018. Each military approach would presumably be combined with threats of economic and diplomatic punishment against the Russians. For the moment, we will set aside the question of whether this is a sufficiently plausible threat to be worth trying to deter.

[17]Colby and Solomon 2015–16.

devote large resources to what might be a doomed defence in the Baltics, but instead threaten to respond to an attack by mobilizing NATO's greater military resources to mount a counteroffensive to liberate the lost territory and ultimately prevail in a prolonged war.

4.3 Conventional Deterrence in the 20th Century

Once, all deterrence was conventional, of course.[18] People didn't often talk about deterrence as a distinct strategic concept because the idea that a country would defend itself if attacked, and that in general nations would not attack enemies they did not expect to be able to defeat, seemed self-evident. Several developments made conventional deterrence more interesting over the course of the 20th century. One was that the airpower revolution greatly expanded the potential to threaten retaliatory attacks against enemy nations, not just their armies and navies, without first achieving victory on the battlefield. Expectations that this would make future wars cataclysmic emerged quickly, and by the 1930s Britain and to a lesser degree other European powers turned to strategic retaliation as a core element of their grand strategies—and as a deterrent and compellent tool in colonial policing. Great Britain would also be the first great power conspicuously deterred by the same prospect, when exaggerated fears of German strategic bombing loomed large is persuading it to abandon Czechoslovakia to its fate at Munich. Harold Macmillan would later recount "We thought of [conventional] air warfare in 1938 rather as people think of nuclear warfare today."[19]

This occurred in parallel with the transformative effects that the experience of the First World War had on perceptions of how bad the costs of war on conventional battlefields could be.[20] It became much more difficult to imagine winning victories over other major powers at a cost sufficiently low to make the exercise worthwhile —and by this point the deaths of tens or hundreds or thousands of thousands of troops had itself become more significant to governments as democratization and national mobilization meant that soldiers were less easily expendable than they once were. The Second World War would see this deterrent effect undermined by new doctrines for employing mechanization and telecommunications that revived the possibility of winning fast and decisive victories against well-armed opponents —making conventional deterrence more contestable in 1940 than it had appeared to

[18]To a first approximation. Of course, aggression in the premodern era could also be deterred by non-military factors, but many of those that loom large in the modern international system tended to be weaker or absent in eras of lower dependence on international trade and fewer concerns about starting wars being viewed as illegal or illegitimate.

[19]Macmillan 1966, p. 522; Bialer 1980.

[20]Mueller 1989.

be in 1920—but only under favourable conditions and against enemies unprepared to counter them.[21]

Nuclear weapons pushed conventional deterrence into the background, at least for the superpowers, for a while after 1945. Atomic and especially thermonuclear weapons' destructive power made the severity of retaliatory deterrent threats difficult to dismiss, and the threat of tactical nuclear weapons, used in quantity, did the same for punitive resistance, for anyone not suitably impressed by the costliness of conventional warfare after the experience of World War II. The United States would briefly embrace the "New Look" strategy of relying on nuclear retaliation to deal with a wide range of conventional military threats as well as nuclear ones in the 1950s, but the loss of its nuclear monopoly soon appeared to undermine the credibility of such responses. In less than a decade conventional deterrence (though not described as such) became a matter of considerable concern and investment in U.S. and Allied planning to deal with the Soviet threat, though always backed up by nuclear capabilities.[22] Some smaller states not protected by allies' nuclear umbrellas explicitly developed strategies for conventional deterrence against invasion through punitive resistance.[23]

As the Cold War ended and the 20th century wound down, a new set of emerging military capabilities further increased the deterrent potential of conventional military force. The development and proliferation of reliable precision-guided munitions (PGMs) enabled states with advanced air forces to inflict high levels of damage against enemy military and infrastructure targets without placing their own armies at risk, while stealth aircraft and modern long-range missiles limited the ability of air defences to protect against such attacks.[24] These technologies also fostered interest in strategies to deter or compel adversary leaders by personally threatening them, although such decapitation strategies mostly failed when they were attempted.[25] PGMs could be used against civilian targets, too, but it was their ability to efficiently cripple military forces not previously vulnerable to conventional bombing that turned out to be most significant for coercion, creating new and powerful options for deterrence by denial.[26] A series of air-centric wars in the Middle East and the Balkans during and after the 1990s demonstrated the growing power of these capabilities to punish weaker adversaries and, in concert with even limited ground forces, to defeat their armed forces and depose their regimes.[27]

[21]Mearsheimer 1983.

[22]Gaddis 2005, Chaps. 5–6.

[23]Roberts 1986.

[24]Lambeth 2000.

[25]Warden 1994; Pape 1996, pp. 79–86; Hosmer 2001b.

[26]Mueller 1998; Pape 2004.

[27]Hosmer 2001a; Mueller 2015.

4.4 Conventional Deterrence in the 21st Century

Does conventional deterrence still matter as much as it once did? The idea that conventional military threats can deter never went away, and it is clear that the concept is still meaningful. But this is not the same as saying that conventional military capabilities are worth maintaining for deterrent purposes, particularly for the United States and its Western allies. For policymakers, the question is whether they should invest resources—money, personnel, political capital, diplomatic effort—in developing or strengthening conventional deterrent capabilities. These things are limited in supply so expending them entails opportunity costs. So does choosing a strategy: focusing a state's national security efforts against a particular adversary or type of contingency using a particular strategy also tends to mean sacrificing some measure of opportunity to prepare to deal with other threats, or the same threats in a different way.

4.4.1 Making the Case for Deterrence

When making costly choices in the arena of security policy, investing in deterrence can be a hard sell. Successful deterrence is usually invisible—an adversary may back down conspicuously during a confrontation in response to a deterrent threat, but the causes of crisis outcomes are often ambiguous. More significant still are the many crises that never happen in the first place, which may be due to deterrence or may not. After the 1962 Cuban Missile Crisis, the superpowers never again knowingly pushed each other to the brink of major war between them, and each side continued to invest quite heavily in both conventional and nuclear military capabilities intended to deter the other. To what extent the former was attributable to the latter is something that we still understand only imperfectly, and had little insight into at the time.

Paying for a costly defence establishment that never fights often seems problematic, even for many people well versed in national security affairs. In his 2014 critique of the U.S. Air Force, Robert Farley holds up the fact that strategic bombers such as the B-47 Stratojet and B-58 Hustler—whose sole operational role was delivering nuclear weapons against the Soviet Union—never went to war as a "disturbing" sign of institutional failure and wasted money.[28] As U.S. Ambassador to the United Nations in 1992, seasoned diplomat Madeline Albright famously queried "What's the point of having this superb military if you can't use it?"[29] Americans typically characterize many NATO allies' anaemic defence spending as free riding on the U.S. military machine, far less often do they consider the role that is played by European leaders and voters who see little value in paying more for

[28]Farley 2014, p. 1.

[29]Powell 1995, pp. 576–77.

armed forces to deal with a distant power that appears to pose no more than a hypothetical threat to them.

In contrast, deterrence failures are quite visible, even though they tend to be rare. When they do occur, it can undermine faith in deterrence—conventional or otherwise—as a policy or a theory, but as with marriages, the existence of failures in execution does not imply that the principle or our theories about it are unsound, only that success is not always easy to achieve. The Russian invasion of Crimea was not the failure of NATO conventional deterrence it is often said to be (indeed it was barely a failure of Ukrainian deterrence given how little of it there was), nor does a terrorist attack prove that terrorists are in general undeterrable. Deterrence failures can occur because the aggressor does not believe that the deterrer will be able to carry out its threats (or promises) effectively, or doubts that it will actually try to do so when the time comes, or because the threatened costs or risks are insufficient to outweigh the factors that appear to argue in favour of war.[30] Good deterrence strategies will seek to avoid these pitfalls. However, any or all of these problems can become much worse if a prospective aggressor's decision making is affected by psychological, bureaucratic, or other factors that contribute to unwarranted optimism about how easy, inexpensive, or beneficial going to war is likely to be,[31] as was illustrated by the most consequential interstate deterrence failure of the past two decades, the 2003 U.S. decision to invade Iraq.[32]

4.4.2 Has Conventional Deterrence Become Irrelevant?

There are at least three general arguments that can be proffered in support of the idea that conventional deterrence is a relatively poor investment in the current era. One is the classic Cold War proposition that nuclear deterrence is so powerful that there is little need for nuclear-armed states or their friends to maintain substantial conventional military capabilities to deter aggression. This is logically sound, at least in contexts where the stakes are high enough to make the use of nuclear weapons plausible. Yet oddly, we see no clear examples of newer nuclear powers embracing this belief as the United States did in the 1950s. Having worked hard to acquire nuclear arsenals, we might expect Israel, India, Pakistan, or North Korea to exhibit greater confidence in the ability of nuclear weapons to protect them from attack. It is also arguably surprising that there is so little apparent sentiment within NATO in favour of trying to solve the perplexing Baltic defence problem simply by threatening nuclear strikes against Russia in the event of an invasion too substantial to fend off, as the Alliance did with respect to West Germany fifty years ago. Do

[30]Rhodes 2000.

[31]Van Evera 1999.

[32]Mazarr 2019.

nations apparently lacking faith in the deterrent power of their own nuclear arms imply that nuclear threats are not reliable deterrents?

A second, related reason for minimizing conventional deterrence investments might be that military aggression has become inherently less attractive for reasons other than conventional deterrent threats—territorial conquest appears less profitable than it once did, and international norms against aggression are stronger so attacking a neighbour entails a high political and moral price and may bring economic punishment by offended countries or frightened investors. More broadly, empire-building through conquest is rather anachronistic in the 21st century, so there simply aren't many potential attackers for most states to worry about. Russia does not want to own the Baltic states although it might find other reasons to attack them, China does not seek ownership of any important territory other than Taiwan (which it would prefer to reclaim by means other than force), the United States has run out of seemingly weak countries it is interested in attacking. This is an argument to take seriously, for interstate aggression has indeed become increasingly rare. However, we should be wary of presuming that the popularity of aggression would have declined similarly without warfare imposing costs on invaders: the strongest case for the "obsolescence of war" thesis is more an argument for the power of conventional deterrence than for its irrelevance.[33] It is also worth noting that most conventional military capabilities take time to develop or, once demobilized, to rebuild, so if an absence of threats might be temporary, disarming in response to it carries corresponding risks.

Finally, conventional deterrence, at least as a response to traditional military aggression, might be out of step with the times in an era of novel threats. If new modes of attack such as cyber warfare, non-state terrorism, or political subversion enabled by social media represent the principal security threats to a state, it will want to recalibrate its deterrence priorities. On the other hand, if the more old-fashioned threats of territorial aggression or coercive punishment have receded because of effective conventional deterrence, maintaining that effect may still be worth the candle. Moreover, while the capabilities that are well suited to deterring conventional wars may provide little defence against cyberattacks or terrorists,[34] punitive conventional threats may be quite useful for deterring enemies from launching, sponsoring, or facilitating such attacks.[35]

4.4.3 Conventional Military Threats in the 2020s

It is important not to exaggerate the security threats we face. In spite of frequently alarmist declarations from U.S. leaders, such as a Chairman of the Joint Chiefs of

[33]Mueller 1989.

[34]Libicki 2009.

[35]Wilner 2011.

Staff declaring in 2013 that the world was then "more dangerous than it has ever been,"[36] by virtually any historically-informed measure the contemporary security environment is relatively benign for the United States and its allies. But this does not mean that deterring aggression is irrelevant—the scarcity of imminent interstate threats against key Western interests is not unrelated to the effectiveness of conventional deterrence.

To focus on the United States, in a period featuring a rapidly rising China and a relatively belligerent Russia it is noteworthy that the scenarios for potential aggression that concern Washington the most—a Russian attack somewhere on NATO's eastern flank, a Chinese invasion of Taiwan, North Korea bombarding one of its neighbours on a major scale for some perplexing reason—do not appear to be imminent threats. However, for policymakers the problem is that if conflicts did occur in these places (and the United States were involved) the costs would likely be enormous. A war in the Baltics or over Taiwan would likely be hard to win,[37] but these are conflicts that would be much better not to fight at all. Winning a war against China or Russia would constitute a huge failure of U.S. national security policy—second only to losing one. And this is true even assuming that a conventional war did not escalate to include the use of nuclear weapons.

Among other states, some still face potential threats of attack from neighbours that well-crafted and well-resourced conventional deterrence strategies can make significantly less likely. Taiwan is arguably the most obvious example of a state with good reason to invest in being a poisonous shrimp or a porcupine, as Singaporean strategists once characterized their country;[38] it has not traditionally optimized its armed forces for conventional deterrence against China, continuing to invest resources in systems that would now have little chance of surviving very long in a conflict with the People's Republic.[39] If Taipei embraced conventional deterrence as a priority it would also be a boon for the United States, and the same is true of other states whose vulnerability to attack by powerful neighbours creates potential flashpoints for major power war. Finally, while some states are not as safe as America, others are not safe from it. For them, conventional deterrence is something to take very seriously indeed—and in some cases this would benefit the United States as well, given that it is still suffering the aftereffects of Iraq's failure to deter it in 2003.

[36]Preble and Mueller 2014.

[37]Ochmanek 2017.

[38]Ng 2005.

[39]Krejsa 2016.

4.4.4 The Merits and Limits of Conventional Deterrence

For states that have unresolved deterrence problems, conventional deterrence strategies often have much to offer, though their comparative advantages inevitably vary depending on the specific case. First, for many states conventional deterrence is more or less the only realistic military option, given the material and political costs of seeking security through nuclear or other unconventional means. Second, even states that possess nuclear arsenals face deterrence challenges that nuclear threats are ill-suited to address because employing such weapons would be incredible, unpalatable, or simply inconceivable. Finally, many of the tools of conventional deterrence have significant flexibility, with value for non-deterrent missions ranging from defence to security cooperation to disaster relief, something that tends to be less true for forces optimized for nuclear deterrence.

Among conventional deterrence strategies, punitive resistance is a straightforward threat that takes relatively little imagination to appreciate, though it is not as hard to dismiss as a good-sized nuclear threat. It also has the great virtue, relative to indirect conventional retaliation strategies as well as nuclear ones, of tending to be credible even when the issue at stake is not a vital interest for the deterrer that would clearly merit escalation to protect—not every army fights staunchly when attacked, but doing so is a natural response to invasion. When deterrence and defence overlap, deterrence is strengthened, and forces meant to deter can still defend if deterrence fails.

Perhaps most important, punishing an enemy on the battlefield during an invasion imposes immediate costs that are difficult for a prospective attacker to discount (except to the extent that it considers its armed forces to be expendable, which Russia, for example, does not appear to do). This relative incontestability represents an important advantage over deterrence approaches that rely on the enemy being frightened by the prospect of punishment or defeat that would occur only with considerable delay. Whether in the form of gradually cumulative economic sanctions, diplomatic shaming and isolation, sustained insurgency against an occupier, or an eventual military counterattack, a prospective aggressor has ample opportunity to imagine that it will be able to find a way to avert much or all of the eventual response. This is particularly true if the response will be costly to carry out, or will depend on maintaining the unity of an international coalition, or requires the deterrer to remain politically committed to protecting an interest that it does not hold dear.

That being said, conventional deterrence in general, and punitive resistance in particular, is not a panacea for every deterrence problem. Capable conventional military forces are expensive to build and maintain—this was the principal appeal of the New Look after all. When facing a threat from a far more powerful adversary, almost all deterrence is more difficult and punitive resistance is no exception. For powerful deterrers, security dilemma dynamics can result in defensively-motivated deterrent armament provoking attack instead of discouraging it if neighbours feel severely threatened. Finally, some non-traditional security threats simply aren't

amenable to conventional responses, an issue that is addressed elsewhere in this volume.

Looking forward, there appears to be little reason to expect conventional deterrence to wane in importance relative to other elements of national security policy in the near future. Technological changes such as expanding capabilities and applications for remotely-operated and autonomous weapons systems are likely to alter specific security threats and options for punitive resistance and retaliation, although it remains to be seen whether this will tend to narrow or expand the capability gap between large and small states, or rich and poor ones. Continuing expectations in the West that wars can and should involve few casualties, especially but not only for our own forces, may enhance the potential of punitive resistance strategies. If we are in the early days of a new era of great power strategic competition, as prophesied by recent U.S. strategy statements,[40] conventional deterrence certainly stands to be a growth industry, as does its nuclear counterpart, and the importance of making sound conventional deterrence strategy will be all the greater given the potentially enormous costs of escalation in conflicts among states with vast resources and large nuclear arsenals. There is no *prima facie* reason to assume that any of these factors will make wars more frequent given their declining incidence in the recent past, but as with nuclear weapons, a scarcity of conventional conflict does not imply the absence of conventional deterrence, and is often a sign of its potency. The fact that people don't see you using your "superb military" does not necessarily mean that there is no point in having it.

4.5 Principles for Conventional Deterrence

Every deterrence situation is different, so offering generalizations is often perilous, but there are some prescriptions that tend to apply in most cases, and make a good starting point for deterrence strategy:

Plan against a range of specific threats. We are often told that the world is unpredictable and threats are difficult to anticipate. Nevertheless, deterrence strategy should take case-specific considerations into account because the differences among adversaries matter. One size does not fit all. However, it is also important not to design deterrence strategy so narrowly that it becomes brittle when reality fails to match one's planning scenarios, as it almost always will.

Design forces to deter. One of the selling points of conventional deterrence is that the forces involved usually have a variety of uses. However, if deterrence is their most important function even if it is often invisible, maximizing their

[40]U.S. Department of Defense 2018.

deterrent value—in terms of capabilities, readiness, basing, interoperability, and other factors—should be prioritized accordingly.

Expect misperception and try to minimize it. The effects of deterrent threats depend on how they are perceived, and perceptions will be affected by cognitive and motivated biases, intelligence errors, and communications failures. When a threat needs to be understood, take pains to make it hard to misunderstand. This may involve trade-offs with military secrecy and maintaining freedom of action.

Threaten to tear an arm off the enemy, as de Gaulle described the purpose of the *Force de frappe.* This principle applies to threats of conventional punishment as well as nuclear ones, and arguably even more so: to carry deterrent weight, a punitive threat should target something the enemy values. In many cases, heavy losses to armed forces fit this bill, but this is not universally the case. What the enemy values most may not be physical, but that need not preclude threatening it.

Make threats that are hard to discount. As discussed in the main text, the effects of threats that depend upon favourable conditions or on sustained commitment, action, or unity of effort over a prolonged period are easier for adversary decision makers to imagine being able to avoid than threats that have immediate and relatively automatic consequences.

Make optimism about aggression impossible, or at least as difficult as possible. Because deterrence occurs in the mind of the adversary, its goals are best served not simply by making war a bad idea, but by making it impossible for enemy leaders to imagine or convince themselves that war is a good idea. The latter is almost always more difficult. Conventional deterrence failures are most likely when a Guderian or a Yamamoto or someone less clever but with the ear of the leader can present a convincing theory of how aggression will be successful at an enticingly affordable cost. The challenge the conventional deterrence strategist faces is to prevent this narrative from being created and believed.

References

Baldwin D A (1971) The Power of Positive Sanctions. World Politics 24.1:19–38

Bialer U (1980) In the Shadow of the Bomber. Royal Historical Society, London

Colby E, Solomon J (2015) Facing Russia: Conventional Defence and Deterrence in Europe. Survival 57.6:21–50

Epstein J (1983/84) Horizontal Escalation: Sour Notes on a Recurrent Theme. International Security 8.3:19–31

Farley R M (2014) Grounded: The Case for Abolishing the United States Air Force. University Press of Kentucky, Lexington, KY
Freedman L (2004) Deterrence. Polity, Cambridge
Freedman L (2013) Strategy: A History. Oxford University Press, Oxford
Gaddis J L (2005) Strategies of Containment. Oxford University Press, Oxford
Hosmer S T (2001a) The Conflict over Kosovo: Why Milosevic Decided to Settle When He Did. RAND Corporation, Santa Monica, CA
Hosmer S T(2001b) Operations Against Enemy Leaders. RAND Corporation, Santa Monica, CA
Huth P, Russett B (1990) Testing Deterrence Theory: Rigor Makes a Difference. World Politics 42.4:466–501
Kleiman M A R (2009) When Brute Force Fails: How to Have Less Crime and Less Punishment. Princeton University Press, Princeton
Krejsa H (2016) Seeing Strait: The Future of the U.S.-Taiwan Strategic Relationship. Center for a New American Security, Washington
Lambeth B S (2000) The Transformation of American Air Power. Cornell University Press, Ithaca, NY
Libicki M C (2009) Cyberdeterrence and Cyberwar. RAND Corporation, Santa Monica, CA
Macmillan H (1966) Winds of Change 1914–1939. Harper and Row, New York
Mazarr M J (2019) Leap of Faith: Hubris, Negligence, and America's Greatest Foreign Policy Tragedy. Public Affairs, New York
Mearsheimer J J (1983) Conventional Deterrence. Cornell University Press, Ithaca, NY
Mearsheimer J J (1981–82) Maneuver, Mobile Defense, and the NATO Central Front. International Security 6.3:104–22
Milburn T W (1959) What Constitutes Effective Deterrence? Journal of Conflict Resolution 3.2:138–45
Morgan F E et al (2008) Dangerous Thresholds: Managing Escalation in the 21st Century. RAND Corporation, Santa Monica, CA
Mueller J (1989) Retreat from Doomsday: The Obsolescence of Major War. Basic Books, New York
Mueller K P (1998) Strategies of Coercion: Denial, Punishment, and the Future of Air Power. Security Studies 7.3:182–228
Mueller K P (ed) (2015) Precision and Purpose: Airpower in the Libyan Civil War. RAND Corporation, Santa Monica, CA
Mueller K P (2018) Conventional Deterrence Redux: Avoiding Great Power Conflict in the 21st Century. Strategic Studies Quarterly, Winter:76–93
Ng P S (2005) From Poisonous Shrimp to Porcupine: An Analysis of Singapore's Defense Posture Change in the Early 1980s. Australian National University Strategic and Defense Studies Centre, Canberra
Ochmanek D (2017) Restoring the Power Projection Capabilities of the U.S. Armed Forces. RAND Corporation, Santa Monica, CA
Overy R J (1992) Air Power and the Origins of Deterrence Theory before 1939. Journal of Strategic Studies 15:68–81
Pape R A (1996) Bombing to Win: Air Power and Coercion in War. Cornell University Press, Ithaca, NY
Pape R A (2004) The True Worth of Air Power. Foreign Affairs 83.2:116–130
Paul T V (2009) The Tradition of Non-Use of Nuclear Weapons. Stanford University Press, Stanford, CA
Posen B R (1984) The Sources of Military Doctrine. Cornell University Press, Ithaca, NY
Powell C (1995) My American Journey. Random House, New York
Preble C J, Mueller J (eds) (2014) A Dangerous World? Threat Perceptions and U.S. National Security. CATO Institute, Washington
Quester G (1966) Deterrence Before Hiroshima. Wiley, New York
Rhodes E (2000) Conventional Deterrence. Comparative Strategy 19.3:221–253

Roberts A (1986) Nations in Arms: The Theory and Practice of Territorial Defence. St. Martin's, London
Schelling T E (1966) Arms and Influence. Yale University Press, New Haven, CT
Shlapak D A (2018) The Russian Challenge. RAND Corporation, Santa Monica, CA
Snyder G H (1961) Deterrence and Defense. Princeton University Press, Princeton, NY
U.S. Department of Defense (2018) Summary of the 2018 National Defense Strategy of the United States of America. Department of Defense, Washington
Van Evera S (1999) Causes of War. Cornell University Press, Ithaca, NY
Warden J A (1994) Air Theory for the Twenty-first Century. In: Magyar K P et al (eds) Challenge and Response. Air University Press, Maxwell AFB, AL, pp 311–32
Wilner A S (2011) Deterring the Undeterrable: Coercion, Denial, and Delegitimization in Counterterrorism. Journal of Strategic Studies 34.1:3–37
Wirtz J J (2018) How Does Nuclear Deterrence Differ from Conventional Deterrence? Strategic Studies Quarterly, Winter: 58–75

Karl Mueller (Ph.D.) is a senior political scientist at the RAND Corporation and adjunct professor at Johns Hopkins University and in the Security Studies Program at Georgetown University. Prior to his current position, he was professor of comparative military studies at the USAF School of Advanced Air and Space Studies. He specializes in research related to military and national security strategy, particularly coercion and deterrence.

Chapter 5
Nuclear Deterrence: A Guarantee for or Threat to Strategic Stability?

Alexey Arbatov

Contents

Abstract In recent literature, much attention has been paid to factors that affect nuclear deterrence and stability from the outside: new missile defence systems, non-nuclear (conventional) high-precision long-range weapons, the influence of third and threshold nuclear states, space weapons, and—more recently—cyber threats. These new factors have pushed the core of nuclear deterrence—strategic relations between Russia and the United States—to the background in the public consciousness. Yet dangerous changes are taking place. This chapter examines the real and imaginary causes of the current situation and suggests potential ways to reduce tensions that could benefit international security. It concludes that nuclear deterrence can serve as a pillar of international security with one crucial reservation: namely, that it can only work in conjunction with negotiations and agreements on

This chapter is a slightly revised version of Alexey Arbatov, Nuclear Deterrence: A Guarantee or Threat to Strategic Stability?, Carnegie Foundation, Moscow, 22 March 2019. Reprinted with permission.

A. Arbatov (✉)
Center for International Security, Primakov National Research Institute of World Economy and International Relations (IMEMO), Moscow, Russia
e-mail: info@carnegie.ru

F. Osinga and T. Sweijs (eds.), *NL ARMS Netherlands Annual Review of Military Studies 2020*, NL ARMS, https://doi.org/10.1007/978-94-6265-419-8_5

the limitation, reduction, and non-proliferation of nuclear weapons. Without such checks, nuclear deterrence goes berserk. It endlessly fuels the arms race, brings the great powers to the brink of nuclear war in any serious crisis, and sometimes the very dynamics of nuclear deterrence can instigate a confrontation.

Keywords Arms control · Strategic stability · Arms race · Nuclear doctrines · START

5.1 Introduction

The United States' withdrawal from the 1987 Intermediate-Range Nuclear Forces (INF) Treaty and the growing likelihood of the termination of the 2010 New Strategic Arms Reduction Treaty (New START) are returning U.S.-Russia nuclear issues to the forefront of discussions on international security and geopolitics. In these discussions, it is difficult to find concepts that are more commonly used—and abused—than strategic stability and nuclear deterrence. Both concepts have a long history. The former has been in official use for nearly thirty years, while the latter has been around for almost seventy. They appear in many state documents and international agreements. Entire libraries of academic literature and propaganda have been written about them, not to mention the reams devoted to both concepts on the Internet, along with oceans of words at countless conferences and symposiums.

Nevertheless, these concepts, their dynamics, and their dialectical interrelationship create new problems time and again. They give rise to paradoxes that, were it not a life-and-death matter for modern civilization, could be considered intellectually fascinating. But, unfortunately, these concepts concern actual matters of life and death. In the current military and political environment, it is no longer inconceivable that war between the United States and Russia could break out in just a few days in the event of a crisis. Such a conflict might culminate with an exchange of nuclear strikes taking as long as just a few hours.

During those hours, hundreds of millions of people in the northern hemisphere would be killed, and everything created by human civilization in the last thousand years would be destroyed. The direct effects would be irreversible, and the secondary effects would likely kill the rest of the world's population within a number of years, or at least send the remaining population back into a prehistoric existence. The prevention of nuclear war is an indispensable condition for the survival of human civilization, and it is inextricably linked to the concepts of nuclear deterrence, strategic stability, nuclear disarmament, and non-proliferation. It might seem that all of the above goes without saying, and that all of this has long been accepted both in theory and practice by politicians, military leaders, civilian experts, and the enlightened public of the world's advanced nations. Over the past three decades, the nuclear arsenals of Russia and the United States have been reduced substantially—both in terms of the number of warheads and in terms of total destructive power.

Yet despite all of this, the danger of nuclear war is today much greater than it was in the late 1980s.

After thirty years of major reductions in nuclear arsenals to strengthen strategic stability, why are Russia and the United States further diverging in their understandings of the principles of stability? For what reasons, after so many years of joint efforts by the two powers to eliminate incentives for a nuclear first strike against the other, is such a scenario more likely today than at any point over the past thirty years? How is it that, after three decades of successful negotiations on the reduction and non-proliferation of nuclear weapons, the world is entering a period of disintegration when it comes to the entire system of control over these weapons? And, finally, why is the world entering a new cycle of nuclear and related arms races that is both multifaceted and multilateral?

In recent literature, much attention has been paid to factors that affect nuclear deterrence and stability from the outside: new missile defence systems, non-nuclear (conventional) high-precision long-range weapons, the influence of third and threshold nuclear states, space weapons, and—more recently—cyber threats.[1] These new factors have pushed the core of nuclear deterrence—strategic relations between Russia and the United States—to the background in the public consciousness. Yet dangerous changes are taking place. This article examines the real and imaginary causes of the current situation and suggests potential ways to reduce tensions that could benefit international security.

5.2 The Genesis of Nuclear Deterrence

The philosophy of nuclear deterrence was born out of the symbiosis of the principle of military deterrence and the emergence of nuclear weapons. The first has thousands of years of history behind it. The latter appeared only in 1945. Intimidating an enemy with the threat of military force—to keep it from pursuing unacceptable actions or to force it into desired behaviour—has long been considered a political and psychological function of armies and fleets before they enter into combat actions. Two and a half millennia ago, the Chinese founder of strategic military thinking, Sun Tzu, wrote: "To fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting. . . . Therefore the skilful leader subdues the enemy's troops without any fighting. . . . With his forces intact he will dispute the mastery of the Empire, and thus, without losing a man, his triumph will be complete."[2]

The creation and use of the atomic bomb in 1945 did not immediately give rise to the idea of nuclear deterrence. At first, nuclear weapons were seen only as a new means of warfare, albeit one with unprecedented destructive power. According to

[1] As a recent example, see: Dvorkin 2018.

[2] Tzu 2019.

official U.S. doctrine of "Massive retaliation" in the 1950s, the actual plan for the use of nuclear weapons—set out in the Pentagon's first Single Integrated Operational Plan, or SIOP-62—called for quickly following any armed conflict with the Soviet Union by launching massive air strikes, conducted by 1,850 heavy and medium bombers that would drop 4,700 atomic and hydrogen bombs on cities and military installations across the Soviet Union, China, and their allies.[3] According to the Pentagon, this attack would have resulted in 800 million casualties across the targeted and adjacent neutral countries.[4] That figure was no less than one-third of the global population at the time.

The creation of Soviet nuclear weapons and intercontinental bombers—and later missiles, as delivery means—deprived the United States of its traditional territorial immunity behind two oceans, and forced the two sides to seriously reconsider their views on the relationship between the political and military roles of nuclear weapons. The idea of nuclear deterrence came to the forefront of U.S. military policy. Of course, it was based on real nuclear forces and operational plans for their use. This qualitative shift laid the foundation for formulating the philosophy that nuclear weapons play a predominantly political role, rather than a military one. At the same time, both roles demonstrate the classic law of Hegel's dialectics on the unity and struggle of opposites (more on this below).

5.3 The Birth of the Concept of Strategic Stability

The origins of this concept lie in analytical developments of the late 1950s at the RAND Corporation. Its first author at the official level was Robert McNamara, who served as U.S. secretary of defense from 1961 to 1968. In 1967, in a sensational speech in San Francisco, he said: "We do not want a nuclear arms race with the Soviet Union, primarily because the action-reaction phenomenon makes it foolish and futile. . . . Both of our nations would benefit from a properly safeguarded agreement first to limit, and later to reduce, both our offensive and defensive strategic nuclear forces."[5] This logic was implemented a few years later in the 1972 Anti-Ballistic Missile (ABM) Treaty and the Strategic Arms Limitations Treaty (SALT I). These agreements did not stop the arms race, however. It was only constrained, but gained momentum in other areas of the nuclear balance and types of nuclear weapons.

The number of U.S. nuclear weapons peaked in the early 1960s at 32,000, before being reduced to 22,200 weapons with a total 20,000 megatons of destructive power by 1989. In the Soviet Union, by the end of the 1980s, the number of weapons reached a maximum of 30,000 with a total destructive potential of 35,000

[3]Kaplan 1983.

[4]Ellsberg 2017.

[5]McNamara 1968, pp. 61–62.

megatons. Together, the two superpowers—which accounted for approximately 98% of the global nuclear arsenal—had accumulated a destructive power equivalent to about 3 million Hiroshima-class bombs. But by the end of the 1980s, the Cold War was winding down, major changes were beginning to take place within the Soviet Union, and the absurd redundancies of accumulated nuclear capabilities became obvious to the ruling elite on both sides. That created a powerful impetus for negotiations on the deep reduction of nuclear weapons, culminating in radical treaties, such as the INF Treaty in 1987 and the first Strategic Arms Reduction Treaty (START 1) in 1991. Against this favourable backdrop, the concept of strategic stability became a legal norm.

That concept was formally invoked for the first and, unfortunately, last time in June 1990 in the Soviet-United States Joint Statement on Future Negotiations on Nuclear and Space Arms and Further Enhancing Strategic Stability.[6] The concept was defined as a strategic relationship that eliminates the "incentives for a first nuclear strike". To create this kind of relationship, future agreements on strategic arms limitations were to include a number of agreed-upon elements:

- "the relationship between strategic offensive and defensive arms" (so that defences cannot undermine the other side's ability to retaliate);
- "measures that reduce the concentration of warheads on strategic delivery vehicles" (so one missile armed with several warheads could not hit several enemy missiles at their bases carrying a much larger number of warheads); and
- "giving priority to highly survivable systems" (so that they cannot be destroyed before launching a retaliatory strike).

This concept radically revised conventional wisdom. During the Cold War, each side ideologically perceived the enemy as an imminent aggressor, regardless of the specific content of its military doctrine or composition of its weapons arsenals. Now, both sides subscribed to the premise that a first nuclear strike is an act of aggression, no matter which state committed it. The basic assumption was that the goal of a first strike was to prevent or substantially weaken the retaliatory potential of the enemy by defeating its strategic forces at their starting positions, and to mitigate the impact of surviving weapons with ballistic missile defences (BMD). Strategic nuclear forces were therefore excluded,[7] by default, from the military theorist Carl von Clausewitz's immortal formulation, "War is the continuation of politics by other means."[8] According to the logic of the 1990 Joint Statement, if neither party is able to significantly reduce the damage of the other's retaliatory strike by launching a first strike, then the outbreak of war (the first strike) will not

[6]Soviet-United States Joint Statement on Future Negotiations on Nuclear and Space Arms and Further Enhancing Strategic Stability 1990.

[7]For the purposes of this work, the term "strategic nuclear forces" is used almost as a synonym of the term "strategic arms", although in the future there may be a discrepancy due to the development of strategic arms with non-nuclear warheads.

[8]Von Clausewitz n.d..

be a continuation of politics by other means, even in the event of an acute conflict of interest between the two states.

It is important to emphasize that the content of strategic stability was agreed upon during the negotiations for START I, signed in 1991, the complex provisions of which embodied all the principles of this concept. These were subsequently reflected in the 1993 START II, the 1997 START III Framework Agreement, the 2002 Strategic Offensive Reductions Treaty (SORT), and New START. As major parallel measures, deep parallel reductions were conducted regarding tactical nuclear arms, negotiations to conclude a treaty banning the production of fissile materials for military purposes (Fissile Material Cut-off Treaty) began in 1993, and the Comprehensive Nuclear-Test-Ban Treaty (CTBT) was signed in 1996. As a result of the implementation of these agreements, today's strategic balance looks much more stable (according to the criteria agreed upon in 1990) than on the eve of the 1990s, that is, before the signing of START I. The permitted levels of strategic weapons have been reduced about six-fold for warheads, almost threefold for deployed delivery systems, and by about thirtyfold for total mega tonnage.[9] The ratio of warheads to delivery systems has decreased from 5:1 to 2:1. The share of arms with increased survivability,[10] which once stood at 30–40%, now amounts to 60–70% of the Russian and U.S. strategic nuclear arsenals.

Even more importantly, the strategic balance has become much more stable in substance—in terms of its 1990 definition, that is, the elimination of incentives for a nuclear first strike. Models of a hypothetical nuclear exchange show that, under realistic conditions, an attack by either party is not capable of destroying more than 50% of the other side's forces while employing 20% more weapons than are hit.[11] In other words, an aggressor would disarm himself in a first strike, and the party under attack would have more surviving nuclear forces than the aggressor has in reserve after the strike, and could strike back, depriving the initiator of the desired advantage of the first strike. Nevertheless, strategic stability as one of the models of mutual nuclear deterrence is now deteriorating due to the evolution of strategic concepts and operational plans on both sides, as well as the beginning of a large-scale cycle of nuclear and advanced conventional arms races. These processes are naturally exacerbated by what is essentially a new Cold War between Russia and the West, which has accelerated the collapse of nuclear arms control.

[9]SIPRI 1991, 2017, pp. 3–51.

[10]Highly survivable capabilities refer to missile forces at sea and land-based mobile launchers. Heavy bombers in this case are not taken into account, since they are not kept in a state of high combat readiness, have a long flight time, and are not guaranteed to break through enemy air defenses.

[11]Dvorkin 2017, pp. 54–74.

5.4 Modern Nuclear Doctrines

The role of nuclear weapons in Russia's foreign and military policy has increased markedly since 2011, following the ratification of New START and the failure of dialogue between the United States and Russia on the joint development of missile defence systems. Ahead of his victory in Russia's 2012 presidential election, Vladimir Putin stressed: "Under no circumstances will we give up the potential of strategic deterrence, and we will strengthen it. . . . So long as the 'powder' of our strategic nuclear forces, created by the great effort of our fathers and grandfathers, remains 'dry', no one will dare unleash large-scale aggression against us."[12] This policy implied the large program of modernizing strategic nuclear forces, including the deployment of 400 new intercontinental ballistic missiles and the construction of eight nuclear-powered ballistic missile submarines.[13]

Meanwhile, U.S. President Donald Trump said in 2017: "Let it be an arms race. . . . We will outmatch them at every pass and outlast them all."[14] The position of the current U.S. political and military leadership on all aspects of nuclear deterrence is laid out quite clearly in the Nuclear Posture Review, published in January 2018. It is immediately apparent that in its basic assumptions, this policy is in tune with the Russian approach: "A safe, secure, and effective nuclear deterrent is there to ensure that a war can never be won and it will never occur."[15] But the analogies do not end there. Both powers embrace not only retaliatory strikes in the event of an attack using nuclear weapons, but also their first use in response to an attack using conventional forces, as well as in some other situations.

The 2018 Nuclear Posture Review emphasizes: "Given the diverse threats and profound uncertainties of the current and future threat environment, U.S. nuclear forces play the following critical roles in U.S. national security strategy. They contribute to the deterrence of nuclear and non-nuclear attack; assurance of allies and partners; achievement of U.S. objectives if deterrence fails; and capacity to hedge against an uncertain future."[16] The Russian military doctrine, published in 2014, also calls for "permanent readiness of the Armed Forces, other troops, and bodies for deterring and preventing military conflicts and for armed defence of the Russian Federation and its allies in accordance with the norms of international law and international treaties of the Russian Federation."[17] Nuclear forces should "maintain global and regional stability and the nuclear deterrence potential at a sufficient level."

In the event of war, the doctrine provides not only for a retaliatory nuclear strike, but also for a first strike: "The Russian Federation shall reserve the right to use

[12]Putin 2012.
[13]Ibid.
[14]Pilkington and Pengelly 2016.
[15]Office of the Secretary of Defense 2018.
[16]Ibid.
[17]Military Doctrine of the Russian Federation n.d..

nuclear weapons in response to the use of nuclear and other types of weapons of mass destruction against it and/or its allies, as well as in the event of aggression against the Russian Federation with the use of conventional weapons when the very existence of the state is in jeopardy" (emphasis added). The purpose of a nuclear strike is defined as "the infliction of the assigned level of damage on an aggressor under any conditions."[18] It turns out, however, that the Russian military doctrine is highly flexible. Answering a journalist's question in Sochi in October 2018, Putin unexpectedly formulated the nuclear aspect of the Russian doctrine as follows:

> Our nuclear weapons doctrine does not provide for a preventive strike. I would like to ask all of you and those who will later analyze and in one way or another interpret my every word here, to keep in mind that there is no provision for a preventive strike in our nuclear weapons doctrine. Our concept is based on a launch-on-warning strike. . . . This means that we are prepared and will use nuclear weapons only when we know for certain that some potential aggressor is attacking Russia, our territory. I am not revealing a secret if I say that we have created a system which is being upgraded all the time as needed—a missile attack early warning system. This system monitors the globe, warning about the launch of any strategic missile… and identifying the area from which it was launched. Second, the system tracks the trajectory of a missile flight. Third, it locates a nuclear warhead impact zone.
>
> Only when we know for certain—and this takes a few seconds to understand—that Russia is being attacked will we deliver a counterstrike. . . . Of course, this amounts to a global catastrophe, but I would like to repeat that we cannot be the initiators of such a catastrophe because we have no provision for a preventive strike. . . . Any aggressor should know that retaliation is inevitable, and they will be annihilated. And we as the victims of an aggression, we as martyrs, would go to paradise while they would simply perish because they wouldn't even have time to repent their sins."[19]

Public attention focused mostly on that last, emotional phrase. The remaining, unnoticed part of Putin's statement, however, seems to have made a fundamental amendment to Russia's military doctrine: essentially, the declaration of no first use of nuclear weapons. This is something the Soviet Union declared in 1982 (though no one in the world took it seriously then) and that Russia abolished in 1993 (which everyone believed). Of the nine states that currently possess nuclear weapons, the only countries to have undertaken such a commitment are China (though few believe it) and India (though it has provided some reservations). It is not clear what happened to the provision of Russia's official military doctrine that claimed the right to the first use of nuclear weapons "in the event of aggression against the Russian Federation with the use of conventional weapons when the very existence of the state is in jeopardy."[20] Moreover, the described launch-on-warning concept clearly does not apply to the use of tactical nuclear weapons—which Russia probably has more of than all the other countries in the world combined—by ground forces, the navy, air defence, and the air force.[21]

---

[18]Ibid.

[19]Kremlin 2018.

[20]Military Doctrine of the Russian Federation n.d..

[21]According to independent estimates, Russia has about 1,850 units of such nuclear weapons. See more: SIPRI 2017.

Furthermore, although Putin referred to nuclear weapons in general, it is possible that the concept he outlined relates only to the use of strategic nuclear forces, and above all the silo-based strategic rocket forces. Otherwise, it is not clear why large investments have been made for many years in expensive, high-value systems such as ballistic missile submarines and land-based mobile ICBMs, which are primarily designed for the "deep second strike" (that is, a launch when there is no doubt about an attack and its initiator after nuclear weapons have been detonated on Russian territory). In any case, Putin said what he said, and all possible interpretations are the personal opinion of experts, not the official position of the supreme commander, especially since he called on "all of you and those who will later analyse and in one way or another interpret my every word here" to keep this statement in mind. Besides, Putin implicitly reaffirmed the conviction shared by the Soviet Union and the United States in the 1970s and 1980s that a nuclear war would be a catastrophe for humanity, and therefore it cannot be fought and won. In any case, the historic importance of the above statement depends on whether or not the next edition of the Russian military doctrine is amended accordingly.

In all other respects, compared to the period of former U.S. president Barack Obama's time in the White House, the views of the two leading powers on the significance of nuclear weapons have become noticeably more symmetrical. In the Obama years, Moscow had not expressed alarm over U.S. nuclear forces, but had consistently shown concern about U.S. non-nuclear missile defence programs and high-precision long-range conventional offensive systems. For its part, Washington had worried about Russian sub-strategic (tactical) nuclear weapons and general-purpose forces. Now the United States sees Russia's (as well as China's) growing strategic nuclear potential over the past decade as a major threat, and intends to respond to this with an extensive program of modernization and expansion. In turn, Russia has clearly shifted emphasis in recent years to its long-range high-precision conventional offensive weapons, which finally aroused U.S. concern in the 2018 Nuclear Posture Review.[22]

Historical analysis shows that strategic asymmetries have periodically created considerable difficulties for nuclear arms control negotiations.[23] Conversely, nuclear symmetry—which began with the Soviet Union achieving parity with the United States in the 1970s and 1980s—has usually contributed to the progress of negotiations. However, the current symmetry of strategic capabilities and views on their importance does not guarantee a resumption of dialogue and reduction of the nuclear threat. This apparent paradox is explained by nuclear deterrence's nature as a special kind of military and political relationship between states.

[22]U.S. Nuclear Posture Review n.d..

[23]These asymmetries included forward-deployed U.S. nuclear forces in Eurasia; the predominant share of ground-based missiles, especially heavy types, in the Soviet strategic forces, and the sea- and air-based components of the U.S. triad; and U.S. advances in long-range cruise missiles in the late 1970s, an attempt to create space-based missile defense in the early 1980s, and, recently, leadership in the development of defensive and offensive high-precision conventional long-range systems.

5.5 The Dichotomy of Nuclear Deterrence

The dual nature of nuclear deterrence arises from the blurred distinction between the use of nuclear deterrence as a political tool to prevent war and the practical use of nuclear weapons as a means of warfare. After all, any deterrence is only feasible if it relies on the material basis of nuclear weapons and the willingness to use them in accordance with military doctrine, strategy, and operational plans. In today's world, all states openly (or, like Israel, by default) maintain and improve their nuclear weapons for deterrence purposes. At the same time, no weapons system is actually created for deterrence, because it is too general and amorphous a concept for the military planners and arms designers. The development of all nuclear weapons systems integrates the latest technical achievements to perform specific military tasks: the destruction of certain military and civilian targets in the specified conditions of conflict. At the same time, certain technical aspects of weapons and related operational plans may increase the likelihood of a military conflict or its escalation. Today, all of this is happening under the influence of technological and military developments and new strategic concepts among the leading nuclear powers, and is being exacerbated by the growing political tensions between Russia and the United States.

The enormous destructive power and technical complexity of existing nuclear forces have effectively left critical political decisions hostage to strategic concepts and operational plans developed in military offices long before an outbreak of armed conflict. And these plans are dictated by the technical specifications of the weapons and their command-and-control information systems. With regards to the present day, the classic Von Clausewitz postulate can be reformulated as follows: war (at least global nuclear war) is no longer the continuation of policy by other means. It is the continuation of military doctrine and the technical specifications of weapons systems that determine the plans and methods of their employment. An illustration of this is the concept of launch-on-warning as outlined by the Russian leadership. It is mainly driven by the vulnerability of strategic forces to a massive nuclear missile strike. However, this only relates to ICBMs in hardened silo launchers, underground command posts, missile submarines in bases, and bombers at airfields. Land-based mobile missiles on deployment routes, submarines at sea, and aircraft in the air are all able to survive nuclear attack and deliver a "deep second strike", but this potential seems to be considered insufficiently destructive.

The "assigned level of damage" mentioned in the Russian military doctrine therefore probably implies that a launch-on-warning of silo-based missiles must be carried out against the aggressor, in particular, launches of the most powerful heavy-class ICBMs (such as the current SS-18 Satan and its upcoming follow-on Sarmat).[24] And this means that the technical specifications of weapons (such as the inability to make mobile heavy-class liquid-fuelled ICBMs, the hardness of their silos, as well as the number, yield, and flight time of the attacking warheads) would

[24]Military Doctrine of the Russian Federation n.d..

dictate the decision of the state's leadership to end the world: to strike back before the arrival of nuclear attack, the consequences of which were so eloquently described in Putin's speech at Valdai. Meanwhile, the concept of launch-on-warning carries a fair risk of unintended nuclear war. This comes from the possibility of a technical failure of the missile attack warning system—which is composed of satellites and ground-based radars—or the unauthorized launch of missiles by the opponent, incorrect interpretations of the other side's actions, or an uncontrolled escalation of a crisis or local armed conflict.

In the short term, this risk may grow significantly along with the development of military hardware and changes to the strategic balance. For example, space weapons and cyber warfare are likely to have the ability to disable early warning systems or trigger false alarms. The proliferation of sea-based nuclear missiles poses the risk of provocative "anonymous" third-party attacks from underwater. The development of hypersonic systems will deprive ground-based radars of the ability to determine, in a timely manner, the trajectory of enemy missiles and their impact area, which means that a launch-on-warning response will have to be authorized immediately upon detection from satellites, which periodically signal false alarms.

Finally, the collapse of the INF Treaty and the possible deployment of new U.S. medium-range missiles in Europe and Asia will, due to their short flight time or low trajectory, neutralize the Russian concept of launch-on-warning, as there will simply be no time for its implementation during an attack. According to statements by authoritative military commanders, this might force Russia to accept the concept of a pre-emptive nuclear strike.[25] It is clear that such a strike would be more destructive than a purely retaliatory strike, but in any case, the subsequent nuclear retaliation by the enemy would be fatal for Russia. And if the United States accepts the concept of a pre-emptive strike, any possible crisis situation would force both sides to speed ahead of the other: not for any political reasons, but because of the vulnerability of Russian strategic forces and command-and-control system to the first strike by the other side.

Another example of the self-destructive tendencies of nuclear deterrence is the concept of a limited or selective nuclear war. The perennial question that strategic planners have fought over for decades is what to do if nuclear deterrence fails. These scenarios include if an attack by an enemy using conventional weapons threatens imminent defeat (including destruction of nuclear forces in bases using high-precision non-nuclear capabilities), if the other side uses nuclear weapons in any kind of limited way, or if it uses other weapons of mass destruction or cyber-attacks. From the early 1970s, the United States—starting with then secretary of defence James Schlesinger—promoted the concept of "retargeting": various options for selective and limited strikes against Soviet military targets.[26] But all of these plans were dashed by the likelihood of a massive nuclear response by the

[25]See more: interview with Colonel General Esin 2018.

[26]Schlesinger 1974.

Soviet Union, which categorically rejected such ideas and strengthened the potential for a "devastating retaliation".[27] Changes began many years later. In 2003, in an official Ministry of Defence document, Russia announced plans for the "de-escalation of aggression . . . [by] the threat to deliver or by the actual delivery of strikes of various intensity using conventional and (or) nuclear weapons." As such, the document assumed the possibility of "dosed combat employment of selected components of the Strategic Deterrence Force".[28]

It should be noted that, since then, subsequent editions of Russian military doctrine and other official strategic documents have made no mention of such concepts. At the same time, the adopted doctrinal formulations do not exclude such actions, since they do not specify how Russia can "use nuclear weapons . . . in the event of aggression against the Russian Federation with the use of conventional weapons when the very existence of the state is in jeopardy".[29] Neither is it clear when and how exactly the existence of the state can be considered in jeopardy, and what level of damage to the enemy is interpreted as sufficient.[30] The United States is not transparent about these points either, but officially allows for the possibility of a limited nuclear war.

Amid the current escalation of tensions, politicians and military experts in Russia and the West have renewed their focus on this concept. A number of publications by Russian military specialists (in active service) justify

> the limited nature of a first nuclear strike, which is designed not to harden, but rather to sober up an aggressor, to force it to halt its attack and move to negotiations. In the absence of the desired reaction, provision is made for increasing the mass of nuclear weapons brought to bear, both in quantitative terms as well as their energy emission (that is, destructive power). Therefore . . . a nuclear first strike by the Russian Federation could have a limited character.[31]

However, in his address to the Federation Council on 1 March 2018, Putin said: "Any use of nuclear weapons against Russia or its allies, weapons of small, medium, or any yield at all, will be considered as a nuclear attack on this country. Retaliation will be immediate, with all the attendant consequences.[32] Implicitly, this may mean that a limited nuclear war is not envisioned in Russian doctrine and planning either, but this important issue might benefit from an unequivocal official clarification.

The United States has included the concept of a limited nuclear war in its nuclear doctrine for many years in the form of "tailored nuclear options". But in the 2018 Nuclear Posture Review, this topic took on a central role and became the main innovation of Trump's nuclear strategy. The review states:

---

[27]Ogarkov 1982.

[28]Current Goals in the Development of the Armed Forces of the Russian Federation 2003.

[29]Military Doctrine of the Russian Federation n.d..

[30]Ibid.

[31]Akhmerov et al. 2016.

[32]Presidential Address to the Federal Assembly 2018.

> Recent Russian statements on this evolving nuclear weapons doctrine appear to lower the threshold for Moscow's first use of nuclear weapons. Russia demonstrates its perception of the advantage these systems provide through numerous exercises and statements. Correcting this mistaken Russian perception is a strategic imperative. . . . To address these types of challenges and preserve deterrence stability, the United States will enhance the flexibility and range of its tailored deterrence options.[33]

For limited nuclear strikes, the plan is to equip part of the Trident-2 submarine-launched ballistic missiles (SLBMs) with low-yield warheads, as well as to develop long-range standoff (LRSO) air-launched missiles, guided bombs with variable yields (such as the B-61-12) for tactical and strategic bombers, and new sea-launched cruise missiles with nuclear warheads.[34] No matter how much the deterrence doctrine is used to justify such capabilities and proposals, they actually reduce the nuclear threshold and increase the likelihood of any armed clash between the superpowers escalating into a nuclear conflict with a subsequent exchange of mass nuclear strikes.

Another controversial response to the question of what to do in the event that deterrence fails is the concept of damage limitation in a nuclear war. The recent U.S. Nuclear Posture Review says: "The goal of limiting damage if deterrence fails in a regional contingency calls for robust adaptive planning to defeat and defend against attacks, including missile defence and capabilities to locate, track, and target mobile systems of regional adversaries."[35] Although this passage refers to regional adversaries, Russia sees itself as a target of these plans (likewise, it feels threatened by U.S. missile defences and long-range high-precision conventional weapons). In a nuclear war, the desire to limit damage to one side by offensive operations looks like a threat of disarming strike to the opposite side, especially when it comes to destroying Russia's highly survivable forces, which in the form of mobile ICBMs are associated mainly with the concept of "deep second strike"—the basis of the philosophy of strategic stability.

Another dangerous area in which the degradation of nuclear deterrence is happening is the development of a variety of long-range (over 500 km) strike systems capable of delivering conventional warheads to targets that could previously only be destroyed with nuclear weapons. This has been made possible by new command-and-control information systems (including in space) and the miniaturization of electronics, which can significantly improve the accuracy of the guidance systems (allowing down to several meters of circular error probability).[36] Existing

[33]Nuclear Posture Review n.d..

[34]Ibid.

[35]Ibid.

[36]This applies to U.S. systems such as the Tomahawk sea-launched cruise missile (BGM-109), and air-launched cruise missiles (AGM-84, AGM-158B, JASSM-ER). Russia is also increasing its arsenal of non-nuclear cruise missiles: Kalibr 3M-54 and 3M-14 sea-launched cruise missiles and the Kh-55SM, Kh-555, and Kh-101-type air-launched cruise missiles. By 2018, the number of high-precision cruise missiles in the Russian arsenal had increased more than thirtyfold, according to the presidential address to the Federal Assembly on 1 March 2018.

non-nuclear cruise missiles have a relatively limited range (less than 2,000 km), subsonic speeds, and a long flight time to targets (about two hours). Yet the next generation of high-precision hypersonic or ballistic conventional weapons under development will make it possible to deliver these kinds of strikes at intercontinental ranges (over 5,500 km) with a relatively short flight time (up to 60 min).[37]

Non-nuclear long-range conventional systems are designed for and used by the superpowers primarily in regional wars (Iraq, the Balkans, Afghanistan, Libya, and Syria). However, they impinge on the strategic balance through the concept of "conventional deterrence", which has long been proclaimed in official U.S. documents,[38] and since 2014, in the Russian military doctrine, which states that: "The use of high-precision weapons is envisaged by the Russian Federation within the framework of performing strategic deterrence use-of-force measures."[39] Initially, this concept was conceived as the preferred alternative to a reliance on nuclear weapons and a way of raising the nuclear threshold. But, in fact, the opposite has turned out to be true: it results in lowering of the threshold. The issue of whether the accuracy of these capabilities will be sufficient to destroy hardened targets (ICBM silos and underground command posts) and whether they will be able to destroy ground-mobile missiles remains highly uncertain. However, there is no doubt that non-hardened strategic nuclear facilities are vulnerable even to existing subsonic non-nuclear cruise missiles. These include missile and air defence radars, light mobile ICBM shelters, submarines in port, bombers at base, forward nuclear warhead depots, and spacecraft control stations. These objects could be hit even in the event of a regional conflict between Russia and NATO.

In addition, many current and future weapons of this kind, as well as their launchers, are dual-purpose, and their character until the moment of detonation will be indistinguishable from a nuclear strike. This applies to heavy and medium bombers, tactical strike aircraft with missiles and bombs, ships, and attack submarines with missiles capable of carrying both nuclear and conventional warheads: the Kalibr and Tomahawk sea-based cruise missiles,[40] air-launched cruise missiles of the Kh101/102 type or the AGM-158, and Iskander-type ground-launched tactical ballistic and cruise missiles. Such systems and associated operational plans could also trigger the rapid, uncontrolled escalation of a conventional local conflict or even a military incident into nuclear war.

---

[37]In particular, such systems are being developed by the United States as part of the Prompt Global Strike program, for example, the Alternate Reentry System (ARS). In parallel, the Boeing X-51A Waverider hypersonic air-launched cruise missile is being tested for deployment on heavy bombers. Russia is ahead of the United States in flight tests of hypersonic gliders for launch by ICBMs (such as the SS-19 or the new Sarmat heavy ICBM by 2020). Putin spoke about the new Avangard system during his 1 March 2018 address.

[38]Einhorn and Pifer 2017.

[39]Military Doctrine of the Russian Federation n.d..

[40]In 2010, the U.S. decided to withdraw the Tomahawk from nuclear service by 2014, but the 2018 Nuclear Posture Review announced the decision to return the SLCM to nuclear service aboard submarines.

Neither Russia nor the United States—nor their allies—want war, and they have no real political motives to unleash it. But it should be remembered that in many wars, both sides believed that they were only defending themselves, fighting off real or probable aggression, even if it was they themselves that carried out offensive operations. That is how World War I began in 1914. That conflict shaped the follow-on terrible history of the twentieth century, and its consequences are still playing out across the world, including in Russia. The Cuban Missile Crisis of 1962 demonstrated clearly that a nuclear war could begin because of a loss of control over events, not as the result of planned aggression. Similar, though less dangerous, cases occurred during the Berlin crisis of 1961 and during three Middle East wars in 1956, 1967, and 1973, among a number of other similar situations. Since the events of 2014 in Ukraine, intense military confrontation between Russia and NATO has been renewed in Eastern Europe, the Baltic and Black Seas, and the Arctic. Regular large-scale military exercises (including with the participation of strategic systems and the imitation of nuclear weapon use) are frequent demonstrations of force.[41] Dangerous close encounters of combat ships and aircraft are a common occurrence. The possibility of a major war between Russia and NATO, which seemed irrevocably consigned to the past just a few years ago, hangs over Europe and the world.

5.6 The Collapse of Nuclear Arms Control

The military, technical, strategic, and political trends discussed above are destroying the systems and regimes of nuclear arms control built over a half-century through the great efforts of the Soviet Union/Russia, the United States, and others. Scholars have warned about this scenario for years,[42] and now the danger has become obvious to everyone. It is clear now that the weakest link in the nuclear arms control system is the INF Treaty. At the same time, the main claims of the parties against each other on compliance issues could be solved relatively quickly at the technical level if there was the political will and strategic interest in solving them. But instead, the Trump administration has officially announced its intention to denounce this historic treaty.

The crisis in nuclear arms control is also manifested in the fact that for eight years, Russia and the United States have not discussed how to progress to the next START agreement. This is the longest pause in fifty years for such negotiations. Although both parties fulfilled their reduction obligations under the current New START by the February 2018 deadline (though with certain misgivings from Russia), the treaty will expire in 2021, and this will create a vacuum in strategic arms control. There is little time for the conclusion of a new treaty, given the deep disagreement between the two parties on important issues. Meanwhile, the U.S. administration has been

[41]Unified Information Portal 2011.

[42]Arbatov 2015.

reluctant to extend New START to 2026 (which can be done once under the terms of the treaty) and faces resistance from Congress on such a step.

The United States and Russia are therefore on the threshold of a new large-scale arms race and, unlike the Cold War, this nuclear missile race will be augmented by competition in offensive and defensive non-nuclear strategic and medium-range weapons, as well as rivalry in the development of space weapons and cyber warfare. Beginning in the mid-2020s, the United States plans to modernize its strategic triad: new systems to replace the current heavy bombers, ICBMs, and SLBMs.[43] And Russia continues to modernize its triad, deploying and developing two new ICBM systems (Yars and Sarmat), one SLBM system (Borei-Bulava), and two heavy bomber systems (Tu-160M and PAK DA). In addition, the United States is developing the above-mentioned systems for limited nuclear strikes (Trident-2 SLBMs with low-yield warheads, LRSO, B-61-12, and nuclear sea-based cruise missiles). And Russia is developing the strategic systems unveiled in Putin's 1 March 2018 address (that is, Burevestnik nuclear-powered intercontinental cruise missiles, Avangard hypersonic gliders, and Poseidon long-range nuclear super-torpedoes).[44] The impact of these weapons on strategic stability requires special analysis, but is unlikely to be positive.

In addition, this arms race will be multilateral, involving states such as China, NATO members, India and Pakistan, North and South Korea, Japan, and others. The start of a nuclear arms race would undoubtedly undermine the norms and regimes for the non-proliferation of nuclear weapons. The review conference of the Non-Proliferation Treaty in 2015 ended in failure, and there is a high probability that the same will happen at the next conference in 2020, especially in light of the U.S. withdrawal from the 2015 multilateral Iran nuclear deal. This will likely be followed by the collapse of the CTBT, which for twenty-three years has not entered into force because of the refusal of the United States and a number of other states to ratify it. Nor is there much hope for progress in negotiating the Fissile Material Cutoff Treaty, which has been stalled for more than a quarter-century. Iran and Saudi Arabia will likely join the nuclear club, as may Egypt, Turkey, Japan, South Korea, Taiwan, Nigeria, Brazil, and other countries. Through them, nuclear weapons will sooner or later inevitably fall into the hands of international terrorists, with all the ensuing consequences.

5.7 Renewing Strategic Stability and Arms Control

At the Valdai forum in Sochi in 2016, Putin said "nuclear weapons are for deterrence and a factor of ensuring peace and security worldwide," and cannot be considered "a factor of any potential aggression."[45] As can be seen from the above

[43]U.S. Nuclear Posture Review n.d..

[44]Presidential Address to the Federal Assembly 2018.

[45]Valdai International Discussion Club 2016.

analysis, nuclear deterrence can serve as a pillar of international security with one crucial reservation: namely, that it can only work in conjunction with negotiations and agreements on the limitation, reduction, and non-proliferation of nuclear weapons. Without such checks, nuclear deterrence goes berserk. It endlessly fuels the arms race, brings the great powers to the brink of nuclear war in any serious crisis, and sometimes the very dynamics of nuclear deterrence can instigate confrontation.

By the early 1960s, the world had gone through a series of increasingly dangerous crises, edging closer to the brink of nuclear war. The culmination was the 1962 Cuban Missile Crisis, when sheer luck saved humanity from disaster. Only after that, with the conclusion of the Partial Test Ban Treaty in 1963, did the construction of a legal, treaty-based system of control over nuclear arms begin. A few years ago, the world once again embarked on the pernicious path of confrontation and military competition, as all areas of arms control stalled for technical, strategic, and political reasons. Only through the strengthening of strategic stability, rehabilitation, and improvement of the nuclear arms control system can we turn away from the path to the nuclear brink.

The Soviet-U.S. concept of strategic stability agreed upon in 1990 was perhaps even more revolutionary than the authors themselves understood.[46] It stipulated that the two sides recognized each other's right to a nuclear strike capability as a guarantor of their own security, but undertook not to develop offensive and defensive weapons that would deprive the other party of such an insurance. Moreover, the limitation of damage from a hypothetical nuclear war should not be carried out by developing disarming strike capabilities, large-scale anti-missile defences, and options for the selective use of nuclear weapons. Instead, it had to be achieved through minimizing the likelihood of such a war politically and reducing the destructive arsenals through treaties, transparency, and confidence-building measures, as well as improving mutual understanding of military doctrines and concepts.

Such a policy is not possible if the powers independently develop concepts, operational plans, and deterrence capabilities, since those are always aimed at defeating the alleged enemy "if deterrence fails". As stated in the Russian military doctrine, in an analogy to U.S. strategic documents and those published by other states, the purpose of the armed forces is "defeating the aggressor's troops (forces) and forcing the aggressor to cease hostilities on terms and conditions suiting the interests of the Russian Federation and its allies".[47] However, deterrence in a crisis may collapse simply under the weight of plans and capabilities intended to deter the enemy. Responsibility for the decision to launch a nuclear strike is laid by the military at the feet of politicians, but those politicians are hostage to the operational plans and technical characteristics of weapons developed by the military and engineers.

[46]At least, this pertains to the author as a participant of those negotiations.

[47]Military Doctrine of the Russian Federation n.d..

Only an understanding of strategic stability that is agreed upon by both sides and embodied in arms limitation and reduction agreements can put strict limits on destabilizing concepts, plans, and arms of nuclear deterrence. Elements of this philosophy were enshrined in the 1990 strategic stability document Now, as then, the conditions of strategic stability can only be imagined between Russia and the United States if this concept is to have clear meaning (elimination of incentives for a nuclear first strike) rather than stand as wishful thinking for international peace and harmony. However, after nearly thirty years, it would be crucial to update the agreed principles of strategic stability in light of the changes that have taken place.

Moreover, the very definition of stability in Russian-U.S. strategic relations should be expanded to include not only "eliminating incentives for a nuclear first strike" but also "incentives for any use of nuclear weapons". With regard to deterring a conventional attack, it should be based on sufficient general-purpose forces and capabilities and, better still, on agreements such as the Conventional Armed Forces in Europe (CFE) Treaty (1990). Further to that point, the meaning of the provision on "measures that reduce the concentration of warheads on strategic delivery vehicles" and "giving priority to highly survivable systems" should be expressed not indirectly but directly, and with mutual recognition that weapons systems threatening the survival of strategic forces and their command-and-control are destabilizing and should be limited and reduced as a matter of priority. If this condition is met, launch-on-warning concepts should be mutually cancelled in light of the possibility of initiating nuclear war due to false alarms, unauthorized use, or cyber sabotage.

In addition, weapons systems that blur the line between nuclear and conventional arms (that is, dual-purpose) should be recognized as destabilizing and should be subject to mutual restrictions and confidence-building measures. Missile defence systems intended to protect against third countries and non-state actors should once again be the subject of a mutually agreed "relationship between strategic offensive and defensive arms". Space weapons—above all, anti-satellite systems—should be acknowledged as destabilizing and be subject to a verifiable ban. Cyber warfare against each other's strategic command-and-control information systems is also destabilizing and should be subject to prohibitions and confidence-building measures. Both sides should recognize that their nuclear doctrines and weapons could create the risk of unintended war as the result of an escalating crisis, which should be the subject of serious and ongoing dialogue at the state level. Finally, the involvement of third states in the process of nuclear arms limitation should be based on an objective assessment of their forces and programs and on an agreement on the sequence, principles, and objects of multilateral arms limitation agreements.

It is extremely important to note that the abstract discussion of the modern meaning of strategic stability will remain fruitless, as demonstrated by years of dialogue on this topic between the United States and China,[48] as well as between

[48]It is true, however, that the United States and China have made some progress: they have begun to compile a dictionary of strategic words and concepts.

Russia and the United States. The proposals that have emerged in recent years for multilateral discussions on nuclear issues and strategic stability as an alternative to specific negotiations do not provide a clear answer to the direct questions of format, subject, and expected results of such intellectual exercises.[49] Such ideas are no doubt attractive to those military and political leaders who are prejudiced against nuclear arms control agreements, do not understand their importance, and do not know the history of the issue. In reality, however, the alternative to time-consuming and sometimes exhausting negotiations is not strategic discussion in the "clubs of interested parties", but an unrestricted arms race for all, at great cost and with the growing danger of war.

Another extreme was the approval of the Treaty on the Prohibition of Nuclear Weapons (TPNW) by the UN General Assembly on 6 July 2017.[50] Without calling into question the good intentions of supporters of this treaty, it must be admitted that the treaty is completely unrealistic, both in theory and in practice, if only because all nine of the nuclear powers that would have to ratify it, in a rare act of solidarity, did not support the UN initiative. But along with the many technical and economic shortcomings of this project, the main omission in the treaty is that it does not address the military and political roles that states associate with nuclear weapons, besides deterrence of nuclear attack: preventing conventional aggression or attacks with other types of WMDs and systems based on new physical principles; maintaining international prestige and status (especially if economic and political assets are lacking); providing security guarantees to allies living near strong opponents; obtaining a bargaining chip for negotiations on other issues; and so on. Over the past seventy years, nuclear weapons have become an integral part of international politics, military strategy, and security. Without changing this environment, it is impossible to simply excise the nuclear factor as a malicious entity from international relations: the system would turn into chaos and the existing security norms and institutions would collapse.

Only consistent and step-by-step treatment is applicable: disarmament measures, in parallel with positive changes in the international political and strategic environment. And it is only in the context of substantive negotiations on arms limitations, reduction, and prohibition that these updated principles of stability can be formulated. The first priority is to salvage the INF Treaty. Russia and the United States should work together to develop additional means of verification, using confidence-building measures and on-site inspections, in order to eliminate mutual suspicions. Technical solutions have been around for several years,[51] and only the ambiguous attitude of the parties toward this agreement—and the overall negative atmosphere in their relations—have prevented them from sorting out these disagreements. If the treaty is nevertheless abrogated, the two powers should as a

[49]For more, see: Karaganov 2017.

[50]UN 2017.

[51]Arbatov 2018.

minimum make a commitment not to deploy missiles prohibited by the agreement on the European continent, and agree on appropriate transparency measures.

Then, if New START cannot be extended beyond 2021, there is an urgent need to begin negotiations on a follow-on treaty. Ceilings on the maximum number of launchers and warheads are not so important; they can be lowered marginally, even by just 100–200 launchers and warheads. What is far more important is the scope of the next agreement. It is essential that any follow-on treaty should count air-launched nuclear cruise missiles and bombs according to the actual loading of the bombers, and include ground-based intercontinental cruise missiles under overall ceilings, as well as intercontinental hypersonic systems, regardless of the type of warheads—nuclear or conventional—that they carry.

Restrictions or bans on fractionally orbital ICBMs and long-range autonomous underwater drones could be exchanged for measures of transparency and delineation of missile defence systems. For example, the sides could limit (to mutually acceptable parameters) strategic defence from ICBMs and SLBMs but allow regional missile defence and air defence systems for protection against medium- and short-range ballistic and cruise missiles. In parallel, negotiations on space weapons should be initiated, beginning with the prohibition of testing any anti-satellite systems against real orbital targets. It is also essential to move on to discussing a mutual pact not to develop capabilities and methods of cyber-attack against strategic command-and-control information systems. Concurrent with intensified negotiations on the issues of nuclear disarmament and the limitation of non-nuclear weapons systems, it might be possible to gradually and selectively include other states in this process. All of these measures are necessary to provide a foundation for the real intensification of cooperation between leading powers in the fight against the threat of nuclear terrorism, which will otherwise inevitably increase.

Amid the current deplorable political and strategic situation, it may seem that the above proposals are utopian. However, experience shows that the situation can change very quickly—both for the better and for the worse. To avoid the latter, every effort must be made to achieve the former. The main prerequisite is the recognition by political leaders and elites of the leading powers that the task of saving and updating the system and regimes of nuclear arms control is the top priority, just as the preceding generation saw it after the Cuban Missile Crisis. The dynamic changes in the world order, military technology, and strategic thinking do not mean that nuclear arms control is no longer needed. On the contrary, these changes make arms control an even more essential condition for the survival of human civilization than it was during the past Cold War.

References

Akhmerov Y, Valeev M, Akhmerov D (2016) The Balloon Is a Friend of 'Sarmat'. Military-Industrial Courier (in Russian). https://vpk.name/news/165525_aerostat__drug_sarmata.html (12 October 2016) Accessed 2 February 2018

Arbatov A (2015) Nuclear Arms Control: The End of the Story. Global Economy and International Relations, 5:5–18

Arbatov A (2018) The Danger of Withdrawing from the INF Treaty. Carnegie Moscow Center. https://carnegie.ru/commentary/77589 (23 October 2018)

Current Goals in the Development of the Armed Forces of the Russian Federation (2003) Red Star (in Russian). http://old.redstar.ru/2003/10/11_10/3_01.html (11 October 2003). Accessed 2 February 2018

Dvorkin V (2017) Reduction of Offensive Weapons. In: Arbatov A, Dvorkin V (eds) A Polycentric Nuclear World: Challenges and New Opportunities (in Russian). Carnegie Moscow Center; ROSSPEN, Moscow, pp 54–74

Dvorkin V (2018) Strategic Stability: Preserve or Destroy? (in Russian) (28 November 2018). Carnegie Moscow Center. https://carnegie.ru/2018/11/28/ru-pub-77809

Einhorn R, Pifer S (2017) Meeting U.S. Deterrence Requirements. Foreign Policy at Brookings, p 20

Ellsberg D (2017) The Doomsday Machine: Confessions of a Nuclear War Planner. Bloomsbury, New York, pp 100–104

Kaplan F (1983) The Wizards of Armageddon. Simon and Schuster, New York, p 269

Karaganov S (2017) On the New Nuclear World: How to Strengthen Deterrence and Maintain Peace. Russia in Global Politics 2

Kremlin (2018) Transcript of the meeting of the Valdai International Discussion Club (18 October 2018). http://kremlin.ru/events/president/news/58848

McNamara R S (1968) The Essence of Security: Reflections in Office. Harper and Row, New York, 61–62

Military Doctrine of the Russian Federation (in Russian). http://news.kremlin.ru/media/events/files/41d527556bec8deb3530.pdf. Accessed 1 February 2018

Office of the Secretary of Defense (2018) U.S. Nuclear Posture Review (February 2018). Office of the Secretary of Defense, Washington, DC. https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-

Ogarkov N (1982) Always Ready to Defend the Fatherland (in Russian), p 49

Pilkington E, Pengelly M (2016) Let It Be an Arms Race: Donald Trump Appears to Double Down on Nuclear Expansion, Guardian (24 December 2016). https://www.theguardian.com/us-news/2016/dec/23/donald-trump-nuclear-weapons-arms-race. Accessed 21 February 2018

Presidential Address to the Federal Assembly (1 March 2018). http://en.kremlin.ru/events/president/news/56957

Putin V (2012) Be Strong: Guarantees of Russian National Security. Rossiiskaya Gazeta (in Russian) (20 February 2012). http://www.rg.ru/2012/02/20/putin-armiya.html. Accessed 2 February 2018

Schlesinger J R (1974) Annual Defense Department Report, FY 1975 (4 March 1974). U.S. Government Printing Office, Washington DC. http://history.defense.gov/Portals/70/Documents/annual_reports/1975_DoD_AR.pdf?ver=2014-06-24-150705-323. Accessed 2 February 2018

Soviet-United States Joint Statement on Future Negotiations on Nuclear and Space Arms and Further Enhancing Strategic Stability (1990). https://www.presidency.ucsb.edu/node/263949 (1 June 1990). Accessed 11 February 2019

Stockholm International Peace Research Institute (SIPRI) (1991) SIPRI Yearbook 1990: World Armaments and Disarmament. Oxford University Press, Oxford, pp 3–51

Stockholm International Peace Research Institute (SIPRI) (2017) SIPRI Yearbook 2017: Armaments, Disarmament, and International Security. Oxford University Press, Oxford
Tzu S (2019) The Art of War. http://classics.mit.edu/Tzu/artwar.html. Accessed 11 February 2019
UN (2017) Treaty on the Prohibition of Nuclear Weapons. http://undocs.org/en/A/CONF.229/2017/8. Accessed 11 February 2019
Unified Information Portal (2011) (in Russian) (17 December 2011) Russia Conducted Secret Military Exercises Near EU Borders—the Media. http://ua-ru.info/news/41846-rossiya-provela-taynye-voennye-ucheniya-u-granic-es-smi.html. Accessed 2 February 2018
Valdai International Discussion Club (2016) (27 October 2016). http://en.kremlin.ru/events/president/news/53151. Accessed 28 October 2018
U.S. Nuclear Posture Review (n.d.)
Von Clausewitz C (n.d.) On War, Part I, chapter 1, section 28

Alexey Arbatov is the head of the Center for International Security at the Primakov National Research Institute of World Economy and International Relations. Arbatov is a former scholar in residence and the chair of the Carnegie Moscow Center's Nonproliferation Program. A former member of the State Duma, vice chairman of the Russian United Democratic Party (Yabloko), and deputy chairman of the Duma Defence Committee, he is currently member of, i.a., the research council of the Russian Ministry of Foreign Affairs and of the governing board of the Stockholm International Peace Research Institute.

Chapter 6
The US and Extended Deterrence

Paul van Hooft

Contents

Abstract The U.S. provides extended nuclear deterrence to allies in Europe, Asia, and elsewhere. The 2018 NPR signals several potentially destabilizing policies, including lowering the threshold for use and adding low-yield capabilities, and it emphasizes the need for nuclear superiority. This chapter argues that the U.S. is changing its nuclear posture to address the growing challenge to U.S. conventional superiority. Extended nuclear deterrence is inherently dubious and the asymmetry between the U.S. on the one hand, and its allies and adversaries on the other, makes it doubly so. In the coming decades, this will continue to generate problems for the U.S. as long as it maintains its alliance commitments.

Keywords United States · Extended Deterrence · Nuclear Deterrence · Grand Strategy · Alliances · Nuclear Strategy · Autonomy

P. van Hooft (✉)
The Security Studies Program (SSP), Massachusetts Institute of Technology (MIT), Boston, USA
e-mail: paul.vanhooft@planet.nl

The Hague Centre for Strategic Studies (HCSS), The Hague, The Netherlands

F. Osinga and T. Sweijs (eds.), *NL ARMS Netherlands Annual Review of Military Studies 2020*, NL ARMS, https://doi.org/10.1007/978-94-6265-419-8_6

6.1 Introduction

The US nuclear posture serves a drastically different purpose than that of other nuclear weapon states; US nuclear weapons are not solely or mostly intended to directly deter attacks on the homeland or other vital interests. Rather, the U.S. nuclear posture must consider how its nuclear weapons can deter attacks on third parties, namely its allies and partners.[1] The U.S. is also physically present with conventional forces in the states it protects. it does so not only to defend its allies against conventional attack and make nuclear weapons superfluous, but by underlining U.S. credibility and providing it with "sunk costs" to prove it has real interests at stake. Consequently, the U.S. has a series of complex extended deterrence arrangements across the globe, to allies in Europe, Asia, and the Middle East. Yet, the U.S. seems to have succeeded in achieving in its ambitions, given the absence of major war with its allies, as well as the avoidance of nuclear annihilation for the past seven or so decades. However, should we expect the US to continue to successfully provide extended deterrence to into the 1st century? This chapter will argue that current political and technological trends will intersect with structural features of the U.S. extended deterrence arrangements and present these with distinct challenges. The most current statement of US nuclear doctrine, the 2018 Nuclear Posture Review (NPR) is illustrative of these developments. However, before delving into current U.S. policies and trends, the rest of this introduction lays out the enduring features of U.S. extended deterrence.

Nuclear weapons are inherently paradoxical: they considered too destructive as weapons to be considered useful in war, at least a war between two nuclear-armed states.[2] After all, the catastrophic consequences of nuclear war make it inherently dubious that most states would consider using nuclear weapons unless they themselves are under attack or unless the survival of their state was at risk in other ways, such as invasion and conquest. The U.S. has not been at risk of invasion since the American civil war and is protected by two oceans and weak neighbours. To deter existential threats to the American homeland would require a more limited number of nuclear weapons sufficient to survive a possible nuclear first strike—a counterforce strike—by an adversary.[3] Yet, the U.S. has 5,800 warheads, of which 1,750 are deployed. Its nuclear triad consists of 400 warheads on land based Intercontinental Ballistic Missiles (ICBMs), 900 on Ballistic Missile Submarines (SSBNs), 300 assigned to bombers based in the United States, and 150 to tactical bombs based in Europe (and 2,050 are held in reserve).[4] Moreover, this is only a fraction of the over 30,000 warheads the US possessed at the height of the Cold

[1] Mazarr et al. 2018, pp. 8–9.

[2] As Bernard Brodie famously noted, the goal was no longer to win wars, but to avert them. Brodie et al. 1946.

[3] For a discussion on how Admiral Arleigh Burke lost the debate in the early 1960s on a SSBN-based "finite deterrence" doctrine, see: Rosenberg 1983, pp. 3–71.

[4] Kristensen and Korda 2020, pp. 46–60.

War. What drives these numbers? Also, given the overwhelming potential for destruction inherent in such an arsenal, why has the U.S. deployed hundreds of thousands of members of its armed forces in Europe, Asia, and elsewhere?

Since the advent of the nuclear age, the U.S. nuclear posture has primarily been driven by the obligations of the U.S. to protect its allies in Europe and Asia.[5] As extended nuclear deterrence has been a permanent feature of the U.S. grand strategy since the late 1940s, it is easy to underestimate how counterintuitive it is. Moreover, arguably most of the scholarship tends to underline the difficulties of deterrence by focusing on basic or direct deterrence against direct threats to a state. Basic or direct deterrence depends on ensuring that the costs of actions an actor might undertake outweigh their benefits, in order that an actor does not engage in a specific behaviour.[6] Deterrence can be through denial—the costs while acquiring the benefits will be high—and through punishment—the costs imposed afterward will outweigh the benefits.[7] Deterrence exists as a function of both capabilities and signalling the perceived willingness or resolve to use these capabilities.[8] Rationalist approaches to deterrence have focused on four sets of variables: the balance of military forces, costly signalling and bargaining behaviour, reputations, and interests at stake.[9] Yet, the rationalist assumptions underlying deterrence have been challenged, as history is rife with errors in judgment by both attackers and defenders.[10] Signals of intent are often not understood. The interests the adversary has at stake are misjudged. How can we assess the chance of success of deterrence if we are not sure of the mechanics?

However, while direct deterrence is already complex, extending deterrence on the behalf of others drastically multiplies the complexity of assessing intentions.[11] In the case of deterrence failure, there is an obvious incentive to avoid conflict. Weaker allies fear being abandoned by their protectors, while those in turn fear being dragged into conflict.[12] Integrating nuclear weapons into the management of alliances in turn further amplifies the complexities: a guarantor of extended nuclear deterrence is in effect promising that it is willing to be annihilated on behalf of its allies when those allies are threatened by a state with a credible second strike capability. As Richard Betts notes, "once basic deterrence becomes mutual, it negates extended deterrence by definition, since the latter requires the willingness to initiate nuclear attack".[13]

[5]See, for example, Gavin 2015, pp. 9–46.

[6]Mazarr et al. 2018, pp. 2–6.

[7]Mazarr et al. 2018, pp. 6–8.

[8]Schelling and Schelling 1966, pp. 92–125.

[9]Huth 1999, pp. 25–48.

[10]Jervis et al. 1985.

[11]Danilovic 2001, pp. 341–369.

[12]Snyder 1997, pp. 187–88.

[13]Betts 2010, p. 10. See also Freedman 1981, p. 276.

If deterrence with nuclear weapons is most believable when the issues at stake are existential in nature, extended nuclear deterrence is thus inherently deeply dubious.[14] The problems of direct deterrence of the Soviet Union received more attention, yet, as Betts points out, the "most fundamental and vexing dilemmas" in U.S. nuclear doctrine remain driven by extended deterrence commitments.[15] The underlying question remained and remains whether the U.S. will follow through with its promises.[16] As these are not the intrinsic interests that would make nuclear use believable, the U.S. has had to go far beyond other states that pursued sufficient nuclear deterrence to prevent invasion or other large-scale threats to vital interests (such as France, the UK, and China). The physical presence of U.S. forces was fundamental to reassuring U.S. allies in Europe and Asia during the Cold War, with allied plans for the acquisition of nuclear weapons closely linked to rises and declines in U.S. troop numbers in the region.[17] The U.S. has persistently struggled to find options between backing down from threats by its adversaries and provoking nuclear disaster.[18]

As understated as the inherent difficulties of extended nuclear deterrence, is how the demands of U.S. extended deterrence during the Cold War shaped many of the institutions within the global order. NATO was not only designed to defend Western Europe against the threat of Soviet invasion, it was also designed to let the West German contribute armed forces without unsettling its neighbours but still accept their precarious position on the front line of the Cold War. In turn, by providing it with security, the US could discourage Germany's pursuit of nuclear weapons.[19] The presence of U.S. forces in West Germany thus served multiple goals beyond deterring Russian conventional forces, it reassured Germany's neighbours, and signalled a supposed U.S. willingness to perish on behalf of its

[14]Jervis et al. 1985, p. 185; Crawford 2009, p. 282.

[15]Betts 2010, p. 11.

[16]See: Freedman 1981, p. 276. Indeed, U.S. officials repeatedly expressed doubts that the U.S. would follow through on its guarantees. National Security Advisor for Richard Nixon, Henry Kissinger, at a private gathering of American and European strategies in Brussels in September 1979 said: "If my analysis is correct, we must face the fact that it is absurd to base the strategy of the West on the credibility of the threat of mutual suicide… and therefore I would say […] that our European allies should not keep asking us to multiply strategic assurances that we cannot possibly mean or if we do mean, we should not want to execute because if we do execute, we risk the destruction of civilization." Cited in Ravenal 1982, p. 37. Defense Secretary for John F. Kennedy and Lyndon B. Johnson, Robert McNamara, wrote that "in long private conversations with successive Presidents Kennedy and Johnson-I recommended, without qualification, that they never initiate, under any circumstances, the use of nuclear weapon." Cited in Garnham 1985, p. 97. See also Pauly's analysis of the reticence of U.S. officials to escalate to the use of nuclear weapons during wargames: Pauly 2018, pp. 151–192.

[17]See particularly: Lanoszka 2018; Crawford 2009, pp. 283–84.

[18]As President John F. Kennedy put it: "Above all, while defending our own vital interests, nuclear powers must avert those confrontations which bring an adversary to a choice of either a humiliating retreat or a nuclear war. To adopt that kind of course in the nuclear age would be evidence only of the bankruptcy of our policy–or of a collective death-wish for the world." Kennedy 1963.

[19]For a definitive take, see: Trachtenberg 1999. See also: Sayle 2019.

allies. The often-cited quote by Lord Hastings Ismay, NATO's first Secretary-General, remains appropriate: NATO was intended to "keep the Soviet Union out, the Americans in, and the Germans down". Unlike the multilateral model of NATO, in Asia the US relied on a "hub and spokes" model of bilateral relations. Though it supplied its main Asian allies with military presence, US assurance was arguably more difficult in Asia. Its allies looked at US behaviour elsewhere in the region. In Japan abandonment fears intensified towards the late 1960s when the U.S. sought to lessen its involvement in the Vietnam War.[20] US manpower cuts on the Korean Peninsula unsettled South Korea in the 1970s.[21] Its Asian allies looked to (re)initiating their independent nuclear programs as soon as the US commitment seemed to falter. In fact, inhibiting the proliferation of nuclear weapons was a key driver of U.S. grand strategy since 1945, as Frank Gavin argues, and this included extensive alliance commitments, perpetual troop commitments, and financial incentives and punishments.[22] Put differently, the number of US nuclear weapons is driven by its alliance commitments, but its alliance commitments are in turn partly driven by the need to diminish the number of nuclear weapons held by other states. The key point here is that many aspects of the current political order and relations between the U.S. and its European and Asian allies derive from the nuclear relationship. Due to changes in the distributions of conventional and nuclear capabilities, specifically in Asia, this order has become fragile in multiple ways. Specifically, the U.S. is no longer guaranteed of fighting a conventional conflict at low costs, which undermines its commitments to allies. As the rest of chapter shows, the most recent statement of the U.S. nuclear posture focuses primarily on the flexibility and superiority of U.S. nuclear capabilities to address the increasing difficulties to guarantee current US commitments. The risks of crisis instability have strongly increased, as have the risks that current U.S. allies will reconsider their non-nuclear stances. Simultaneously, the Trump administration is ambiguous in signalling its intentions. The chapter proceeds as follows. First, the chapter lays out the perceived challenges to the U.S. strategy that the adaptations that the 2018 Nuclear Posture Review (NP) addresses. Specifically, how the asymmetry of interests between the U.S. and its adversaries and allies ensures that the declining conventional superiority of the U.S. has real repercussions for the credibility of its commitments. The second and third section follows through and notes the perceived need for flexibility and superiority the NPR identifies, and how it seeks to address these partly with additional low-yield weapons. The fourth section discusses how the suggestion that U.S. is lowering the threshold for use increases the risk of crisis instability. The final section notes how the intersection of these policies with current trends makes the U.S. extended nuclear deterrence arrangements precarious.

[20]Lanoszka 2018, p. 79.

[21]Lanoszka 2018, p. 115; Jang 2016.

[22]Gavin 2015; Gerzhoy 2015.

6.2 Current U.S. Nuclear Posture and Challenges

In the 2018 United States Nuclear Posture Review (NPR), the most current statement on the U.S. nuclear posture, the Donald Trump administration seeks to ensure the American arsenal is unchallengeable. Three features are particularly noteworthy. First, the 2018 NPR proposes to modernize the nuclear triad, in line with the NPR of the previous administration, though it also seems to signal a great willingness to gain superiority over rivals. Second, the 2018 NPR expands the threshold to include "non-nuclear strategic attacks", and, third, stresses the need for more non-strategic options, particularly a low-yield nuclear warhead for the submarine-launched ballistic missile (SLBM). The second and third features have the potential to be escalatory.[23] While similarities exist with previous NPRs,[24] it is the emphasis in the 2018 NPR on the pursuit a "flexible, tailored nuclear deterrent strategy"[25] that seems far removed from the previous NPR drawn up during the Obama administration. Those made claims about the desirability of disarmament.[26] I argue that the changes to the U.S. nuclear posture are driven by the increased difficulties and precariousness of providing extended nuclear deterrence to U.S. allies.

United States is an extra-regional guarantor, insulated from all non-ICBM attacks by virtue of its insularity. The inherent asymmetry of interests between the U.S. and its adversaries there make extended nuclear deterrence even more difficult than it would already be. Competitors and adversaries such as China, Russia, and Iran are states with intrinsic security interests in their respective regions. The U.S. is operating in *their* backyard. Each of these is pursuing strategies aimed at raising the costs of U.S. actions, with the intention of forcing U.S. leaders and the American public to reconsider the extent of interests in these regions. North Korea is a more radical example of this logic, with its brinkmanship strategy underlining that the U.S. does not have existential interests at stake in the Korean Peninsula, unlike North Korea itself.[27] Adversaries know that pursuing asymmetric strategies that raise costs will in turn deter U.S. actions and thus undermine the credibility of its deterrent.

To deter its adversaries and reassure its allies, the United States is heavily reliant on its cutting-edge military technological advantages—exemplified in its precision strike complex—and its ability to command the global commons.[28] Given the fact

[23]Steinberg 2018.

[24]The 2018 NPR and the 2010 NPR both call for maintaining strategic stability together with Russia and China, continued NATO nuclear capabilities, addressing the threat of nuclear terrorism, as well as arms control. Both also calls for modernizing the nuclear arsenal. Mauroni 2018.

[25]Office of the Under-Secretary of Defense 2018.

[26]See: Gavin et al. 2018.

[27]As Austin Long notes, once an adversary can reliably strike the U.S., the credibility of its extended nuclear deterrence becomes more questionable. Long 2018.

[28]Posen 2003.

that the U.S. is an extra-regional guarantor, ensuring that the U.S. has access to the theatres of operations is crucial for projecting power against threats to its allies. The U.S. command of the global commons allows the U.S. to move forces, munitions, fuels, and dry goods to and within these theatres.[29] Adversaries are also investing in capabilities that test the U.S. command of the commons and its abilities to quickly reinsert or reinforce forces in local conflicts. U.S. conventional military superiority ensures that the costs of military actions are asymmetrical to its advantage to negate the asymmetry of interests between the U.S. and its (potential) adversaries.

Like the other key national security texts from the Trump administration, the 2017 National Security Strategy (NSS) and the 2018 National Defense Strategy,[30] the 2018 NPR identifies the return of great power competition as the key challenge driving American grand strategy. The NPR specifically signals advances in missile and targeting technology, has created the need for rethinking the nuclear posture.[31] This was primarily a response to the incredibly rapid and sustained growth of the economy of the People's Republic of China and its growing military capabilities, reinforced by the renewed Russian belligerence exemplified by its annexation of the Crimea and invasion of Ukraine.[32] The 2018 Nuclear Posture Review (NPR) followed suit, distancing itself from the previous NPRs—specifically the 2010 Barrack Obama administration NPR—that assumed the prospects for military confrontation between great power had declined and would continue to do so and that the U.S. could lead in nuclear arms reduction.[33] The NPR specifically notes the risks of Russia and China pursuing asymmetric ways and means to counter U.S. conventional capabilities, specifically the U.S. capabilities that make up its precision strike complex. Russia and China are developing counter-space military capabilities that undermine U.S. space-based intelligence, surveillance, and reconnaissance (ISR), nuclear command, control and communications (NC3), and positioning, navigation, and timing, as well as offensive cyberspace capabilities.[34]

Chinese and Russian investments in Anti-Access Area Denial (A2/AD are a particularly powerful driver of the change in U.S. nuclear posture.[35] The conventional advantages the U.S. has long enjoyed—certainly in the years that followed the end of the Cold War—have been steadily eroding, though not ending. That erosion of conventional military superiority impacts the options for deterrence. China is putting the conventional superiority upon which the U.S. military strategy

[29]Matthews and Holt 1992.

[30]Trump 2017.

[31]The nuclear posture can be defined as the capabilities of the nuclear force, with a doctrine for when and how to employ them, and specified control and command arrangements.

[32]In contrast to the Chinese challenge to U.S. power in Asia, U.S. officials consider Russia primarily a regional concern. Interviews of the author with current and former national security officials, D.C., December 2018, February and December 2019.

[33]Office of the Under-Secretary of Defense 2018, p. 6.

[34]Office of the Under-Secretary of Defense 2018, p. 7.

[35]Office of the Under-Secretary of Defense 2018, p. 7.

rests under pressure through the advances in quality and quantity of specifically its ballistic missiles but also other capabilities. The 2018 NPR signals how Chinese DF-26 intermediate-range ballistic missile capable of attacking land and naval targets, as well as new mid-course missile defence systems, sea-based mid-course ballistic missile defence, and developing theatre ballistic missile defence systems.[36] China has thus become increasingly capable of targeting fixed assets of the U.S. in Japan, South Korea, Guam, as well as elements of the U.S. navy.[37] The Chinese strategy centres on damaging or destroying on the airbases, shelters, fuel storage, and runways.[38] Their numbers are limited for the U.S. in the Asia-Pacific and their damage or destruction heavily constrains U.S. air power. Chinese capabilities are also targeting moving targets, specifically the aircraft carriers that extend U.S. power projection. The logic is straightforward: impede U.S. access to the region and deny the U.S. the ability to freely move around the region.

Russia has further developed its own A2/AD capabilities and trained these upon possible NATO reinforcements through the Baltics for any escalation in the Baltics. The Baltics are, after all, only connected to NATO territory through a narrow land bridge. The deployment by Russia of the 9M729 (SSC-8) land-based or submarine-launched cruise missile 3,000 km range missile violated the INF Treaty. This, in turn, has led to the suspension and then cancellation of the INF Treaty by the U.S. However, beyond the U.S. decision to reciprocate in kind to Russian actions, the suspension of the INF Treaty also freed up the U.S. to place its own missiles in the Asia-Pacific.[39]

While the primary driver of the overall U.S. posture might be its declining conventional military superiority, the nuclear capabilities of Russia and China offer their own distinct challenges. U.S. officials fear that the Russian nuclear posture may rely on threats of limited nuclear first use to terminate conflicts on terms favourable to Russia.[40] Whether Russia would choose to exploit ambiguity through hybrid warfare ("the little green men") or to exploit the geographically exposed nature of the Baltic NATO member states through sudden moves (fait accompli), it could then threaten the use of nuclear weapons should the U.S. and the other European NATO member seek to retake that territory. The NPR remarks that Russia has retained large numbers of non-strategic nuclear weapons and is modernizing these, in order to pursue military strategies and capabilities that rely on nuclear escalation.[41] This has been referred to as its "escalate to de-escalate" doctrine—controversially so, because it is far from clear whether this accurately describes Russian outlook. As Ven Bruusgard notes, the strategy bears no resemblance to the theoretical discussions on limited nuclear options within Russian

[36]Office of the Under-Secretary of Defense 2018, p. 11.
[37]Biddle and Oelrich 2016; Montgomery 2014.
[38]Heginbotham et al. 2015.
[39]Blumenthal and Dan 2011.
[40]Office of the Under-Secretary of Defense 2018, p. 7.
[41]Office of the Under-Secretary of Defense 2018, p. I.

military journals. If anything, when digging beneath apparent nuclear sabre rattling by the Russian regime,[42] Russians are actively seeking to increase the threshold of nuclear use. Russians are apprehensive about the perceived unwillingness of the U.S. to accept mutual vulnerability.[43] Austin Long concurs; while Vladimir Putin believes nuclear weapons are of central importance to Russian security, he has generally refrained from invoking their use over anything besides vital interests.[44] Russia is also developing new intercontinental range systems, such as a hypersonic glide vehicle, and a new intercontinental, nuclear-armed, nuclear-powered, undersea autonomous torpedo, the so-called Status-6 system.[45] Yet, it is unclear how the latter would be significantly more effective in threatening the U.S. second-strike capability than current Russian ICBM capabilities.

The U.S. appraisal of Chinese capabilities is more difficult to understand. The 2018 NPR notes that China is modernizing and expanding its "already considerable nuclear forces".[46] However, it seems to overstate Chinese innovations. China possess a nuclear arsenal of approximately the same order as that of the UK and France (250–300 warheads). Moreover, unlike the UK and France, it relies on ICBMs rather than SSBNs. The Chinese second-strike capability is far from secure, and, importantly, so far it does not seem a major priority for China to invest resources to ameliorate this discrepancy.[47] As James Steinberg notes, the 2018 NPR's assessment of the "China threat" is puzzling, as the document confirms that China's policy and doctrine have not changed, yet it highlights a supposed lack of transparency from China. The fear might be that China could strengthen its theatre nuclear forces to threaten forward deployed U.S. forces in the case of a Taiwan contingency.[48]

As the U.S. preoccupation is primarily with overcoming the improved Chinese A2/AD capabilities,[49] the real risk of the Chinese nuclear posture is the mixing of command and control systems of its nuclear capabilities and its A2/AD capabilities. In conflict, the U.S. could target Chinese command and control to ensure its naval and air assets survive, which Chinse military leaders could interpret as the first phase of a counterforce strike on Chinese nuclear capabilities.[50] There is thus a non-negligible risk of inadvertent nuclear escalation in the Sino-American competition.[51]

[42]Braw 2015.

[43]Ven Bruusgaard 2018.

[44]Long 2018.

[45]Office of the Under-Secretary of Defense 2018, pp. 8–9.

[46]Office of the Under-Secretary of Defense 2018, p. I.

[47]Kristensen and Korda 2019, p. 173.

[48]Steinberg 2018.

[49]Office of the Under-Secretary of Defense 2018, p. I.

[50]Cunningham and Fravel 2015.

[51]See also: Posen 1991; Acton 2020.

The scenarios in Europe and Asia are thus entirely distinct, creating vastly different challenges for U.S. deterrence. In Europe, the threat is primarily land-based, favouring the offensive. It would be exceedingly difficult for NATO to stop Russia from capturing one or more of the Baltic states through conventional means—though it would be difficult for Russia to retain these gains through military means should the U.S. and NATO seek to recapture these. In such a scenario, U.S. planners fear Russia will resort to threatening the limited use of tactical nuclear weapons against NATO reinforcements or infrastructure—the supposed "escalate to de-escalate" doctrine discussed above. It is an interesting reversal of the Cold War stand-off between NATO and the Warsaw Pact: then, the U.S. was the actor that considered pre-strategic, tactical nuclear weapons to compensate for conventional shortfalls vis-à-vis the Soviet Union.[52] Yet, during the Cold War, losses would have been cumulative, and degenerative for the balance of power. The capture of West Germany would have added significant industrial and military capabilities to the Soviet Union. Currently, the capture of the Baltics adds little to Russian capabilities, except potentially exposing the fissures within the alliance regarding the willingness to fight. Russian A2/AD capabilities would present problems for forces seeking to route Russian incursions into the Baltics. However, unlike in Asia, NATO airfields are too numerous for Russian missile attacks to present serious problems. Reinforcement of NATO Europe would be less vulnerable to Russian naval disruption.[53]

In Asia, scenarios are primarily maritime in nature, favouring the defensive. While China is increasingly capable of targeting the limited number of U.S. and allied fixed assets such as airfields and airport, the 'stopping power of water' ensures it would be exceedingly difficult to make actual territorial gains. Yet, current U.S. allies could resort to 'hiding' or 'bandwagoning' strategies when facing Chinese power and retract U.S. access to airfields and ports on their territory, quickly degenerating the access of the U.S. to the Western Pacific. Losses would be cumulative. The solution to the U.S. problems in the Asia-Pacific—if it exists—is likely to focus on maintaining enough conventional air power and maritime access in the region to dampen the pressure China can put on U.S. allies, while dispersing U.S. bases and facilities across the region.[54] However, the improvements of Russian and Chinese A2/AD capabilities create another problem.

To ensure the credibility of its commitments, the U.S. has relied on a physical presence in the regions where it extends nuclear deterrence to its allies. It does so for two reasons. The first is to enable the U.S. and its allies to engage in deterrence by denial, meaning that they can raise the costs of aggression by the adversary by mounting a conventional defence. One could argue that the long-range precision

[52]The reversal of the Cold War dynamics in Europe was noted by several former and current officials in interviews with the author.

[53]However, despite the more favorable circumstances in the European theater, the ability of the U.S. to reinforce NATO Europe is far from given. Colin and Townsend 2019.

[54]Heginbotham and Samuels 2018; Biddle and Oelrich.

strike capabilities of the U.S., plus its command of the commons, would allow the U.S. to remain out of region or retain only a minimal presence, with the option of reinforcing should deterrence fail.[55] This would, however, go against what constitutes the second reason for a U.S. presence in the regions it extends deterrence to, which is that the presence of American forces gives the U.S. 'skin in the game'.[56] As Lawrence Freedman puts it, during the Cold War, the most important thing about U.S. ground forces in Europe was "their nationality".[57] It compensates for the inherent asymmetry of interests between those of the U.S. as an extra-regional protector and those of its adversaries and allies in the region, and makes it more believable that the U.S. will risk the survival of its own society on behalf of its allies. Innovations in conventional weaponry by China and Russia in terms aim to raise the costs for the U.S. to maintain a physical presence.

What is different from previous eras—hence the emphasis on great power competition—is that the U.S. now faces two major powers that have significant conventional and nuclear capabilities. It is therefore significant that the U.S. has abandoned the planning assumptions of the 1997 Strategic Defense Review (SDR); the U.S. military is no longer planning the capability to fight and win two major regional wars.[58] The move to a one-war standard will limit the US ability to deter adversaries in multiple regions, as committing forces in Asia might undermine the ability to reinforce Europe and vice versa.[59] In combination with its declining conventional military superiority, the U.S. is increasingly pressured to rely on its nuclear arsenal.

6.3 Perceived Need for Flexibility

The current U.S. outlook is to increase flexibility in its nuclear posture in the face of perceived deterrence gaps. Yet, in doing so, the US is undermining stability in multiple ways, as the proposed solutions are likely to provoke potential adversaries. The NPR considers it a deterrence gap that the U.S. cannot respond in kind to a possible Russian limited use of low-yield tactical nuclear weapons. The existing U.S. non-strategic nuclear force consists exclusively of a relatively small number of B61 gravity bombs carried by F-15E and allied dual capable aircraft (DCA). The United States is incorporating nuclear capability onto the forward-deployable, nuclear-capable F-35 as a replacement for the current aging DCA.[60] The NPR believes Russia currently perceives it has a coercive advantage due its greater

[55]Posen 2014; Mearsheimer and Walt 2016, p. 70.
[56]Lanoszka 2018.
[57]Freedman 1981, p. 276.
[58]Mattis 2018.
[59]Brands and Montgomery 2020.
[60]Office of the Under-Secretary of Defense 2018, p. X.

number variety of non-strategic nuclear systems. While the NPR insists the U.S. is not pursuing "nuclear war-fighting" options, it still identifies a need to expand flexible U.S. nuclear options, including low-yield options. The DCA aircraft that allow nuclear sharing with NATO Europe allies, will be upgraded with the nuclear-capable F-35 aircraft.

However, the policy option that has most commentators up in arms, is the U.S. plan to modify existing Trident missiles on its SSBN force for a low-yield option (the W-76 or W-88 missile), and, in the longer term, a modern nuclear-armed sea-launched cruise missile (SLCM). The reason given is that, unlike DCA, a low-yield SLBM warhead or SLCM does not require or rely on host nation support.[61]

What to make of this reluctance to rely on allies? Is the concern that the European allies that currently base American nuclear weapons on their territory—Germany, the Netherlands, Belgium, Italy, Turkey—will stop doing so? Or is the concern that the DAC are too vulnerable to interception by Russian missile defence, while the SSBNs would be undetectable until it was too late? As James Steinberg notes, the choice suggests that administration officials think European governments might no longer support basing them on allied territory, a "rather curious turnabout" for an administration ostensibly preoccupied with 'burdensharing'. Steinberg postulates that the US might be looking for a bargaining chip to incentivize Russia to negotiate seriously over a reduction of its non-strategic nuclear weapons (similar to the logic underlying the 1979 NATO Doubletrack decision that was intended to force the Soviet Union back to the negotiating table).[62] In part, the move to SSBN based SLCMs and Tridents with low-yield options is supposed to be driven by Russian moves, it is as likely to be driven by the need to reassure South Korea and Japan vis-à-vis Chinese modernization.[63]

Notwithstanding the motives, problems abound with the renewed U.S. emphasis on low-yield non-strategic nuclear weapons, and specifically the plan to adapt the Tridents on board the SSBNs to launch low-yield nuclear weapons. The first problem is that it muddles the political signalling that the division between platforms allows, through which the U.S. can significantly reduce uncertainty. At present, a submarine-launched weapon would be understood as a strategic attack, while bombers taking off from European airfields would signal the use of tactical nuclear weapons. Combining the tasks on one platform discards this advantage and generates a clear discrimination problem, as it relies on Russian systems distinguishing between a single SLBM and a massive counterforce attack.[64] Second, it supposes that Russia (or another adversary) would wait and see what the impact of warhead was—was it a single military target or multiple cities—to assess whether this was a deliberate tactical attack, an accidental misfire of a strategic attack, or the

[61]Office of the Under-Secretary of Defense 2018, pp. XI–XII.

[62]Steinberg 2018.

[63]Mauroni 2018.

[64]Narang 2018; Nolan and Radzinsky 2018.

first phase of a strategic attack, before deciding whether to launch their own counterattack with strategic weapons. The third problem is a more general one to relying more on tactical nuclear weapons—what military asset would a low-yield non-strategic weapon target and where would it be located? During the Cold War, NATO's theatre nuclear weapons were intended to destroy staging areas and infrastructure that were part of the Soviet conventional assault envisioned as the most likely scenario. Importantly, these would likely be on the territory of Warsaw Pact states, but not Russia itself.[65] That would not be the case now and targeting Russian territory to stop a conventional move adds another step on the dangerous spiral path of escalation.[66]

6.4 Superiority and Triad Renewal

The U.S. nuclear posture is expansive to cover a wide range of contingencies. The NPR identifies the increasing need for diversifying and increasing flexibility, makes the sustainment and modernization of the nuclear triad—and its command and control—necessary.[67] The triad consists of three legs: (1) land-based Intercontinental ballistic missiles (ICBM); (2) sea-based nuclear ballistic missile submarines (SSBNs) with submarine-launched ballistic missiles (SLBM); and (3) strategic bombers carrying gravity bombs and air-launched cruise missiles (ALCMs). During the Cold War, the triad was intended to assure a survivable second-strike, as it was considered extremely unlikely that the Soviet Union could destroy all legs of the triad in a surprise attack. The triad illustrate three different solutions for the problem of an adversary's first strike: redundancy; hiding; and hardening.[68] Redundancy ensures that the number of warheads would likely exceed what the adversary could destroy in a first strike. With no certainty that he would be secure, the adversary would refrain from action. Hardening centres on solidifying the shelters in which ICBMs are kept. Without precision penetration strikes, too many weapons are likely to survive, again assuring a secure second strike. Hiding centres on mobile platforms. Bombers are one option, mobile land launchers another, but the most effective mode for concealing platforms for launching nuclear weapons is under the sea: SSBNs. To insure against innovative adversary strategies, all three legs of the triad were thus deemed necessary to assure a secure second strike.

[65]Long 2018.

[66]During the Cold War, theater nuclear weapons would target Soviet forces on the territory of Warsaw Pact members. At present, U.S. tactical nuclear weapons would target Russian forces on Russian territory. Narang 2018.

[67]Office of the Under-Secretary of Defense 2018, p. X.

[68]Lieber and Press 2017.

The renewal of all three legs of the triad has been planned, as well as associated nuclear command and control. The costs of the current nuclear arsenal are approximately 3% of DoD budget, modernization will add another 3–4%. High projections place the highpoint of future cost at approximately 6.4% of the current DoD budget. The cost of modernizing all three legs of the nuclear triad are indeed significant, with estimates from the Congressional Budget Office of $1.2 trillion between 2017 and 2046. In 2029, the Ground-Based Strategic Deterrent (GBSD) will replace Minuteman III and the 450 ICBM launch facilities will also be modernized. The air leg will see its own modernization, with a new development program for the next-generation bomber—the B-21 Raider. The Long-Range Stand-Off (LRSO) cruise missile replacement program will add onto the B-52H and B-2A 'stealth' strategic bombers. The 14 Ohio-class SSBNs will be replaced by 12 Columbia-class SSBNs.[69]

Is the U.S. second strike capability at risk, given the modernization efforts? The NPR claims the triad provides flexibility while guarding against technological surprise,[70] yet it provides no evidence that technological surprises are imminent. U.S. planners have consistently feared counterforce options. Keir Lieber and Daryll Press claim that various technological innovations—specifically advances in sensing and computing—have made a secure second strike more doubtful.[71] However, Russian and Chinese conventional capabilities are not close to achieving the capabilities needed to contemplate a first strike. Specifically, there is little justification for renewing the land-based leg of the triad, the ICBMs, beyond offering a target in sparsely populated areas of the U.S. to soak up the adversary's weapons in a first strike. If the purpose is a secure second-strike capability, then the SSBNs have already assured these. The 14 Ohio-class SSBNs the U.S. currently relies on are undetectable to Russian or Chinese ASW capabilities or sensing. The 12 new Columbia-class SSBNs will assure this capability remains for the foreseeable future. An argument used for maintaining the number of weapons, as well as all three legs of the triad, centres on the perceived benefits of nuclear superiority. Matt Kroenig suggests that historical evidence shows the side with the greater number of nuclear weapons has a clear advantage in coercion.[72] Yet, this is a highly controversial interpretation of the historical record, as Charles Glaser, Todd Sechser, and Matt Fuhrmann point out.[73] Arguably, the key driver of current decisions to maintain the triad is a preoccupation with vulnerability among U.S. officials.[74]

[69]Dorminey and Gomez 2019.

[70]Office of the Under-Secretary of Defense 2018, p. II.

[71]Lieber and Press 2017.

[72]Kroenig 2018.

[73]Glaser 2019. As Todd Sechser and Matthew Fuhrmann note, in their study of militarized compellent threats from 1918 to 2001, compellent threats from nuclear states are no more likely to succeed than those from non-nuclear states. Sechser and Fuhrmann 2013.

[74]Thompson 1992; Walt 2018.

6.5 Lowering the Threshold

Observers commented that the NPR is also remarkable in that it lowers the threshold for nuclear use by the U.S. by emphasizing cross-domain deterrence. The U.S. will invest in a range of flexible nuclear capabilities needed to ensure that nuclear or non-nuclear aggression against the vital interests of the U.S. itself or its allies and partners can lead to "intolerable consequences" for potential adversaries.[75] However, when operationalizing what this means, the NPR notes that this also applies to significant strategic attacks that are non-nuclear in nature. These could include attacks on the U.S., allied, or partner civilian population or infrastructure—which would include its information networks, i.e. a cyber-attack.[76] If the NPR's statements are taken at face value, the possible scenarios for the use of limited yield nuclear weapons, or of strategic weapons, have now clearly multiplied. The NPR claims this "does not lower nuclear threshold", but, by convincing adversaries that limited use of nuclear weapons will be too costly, "in fact raises the threshold".[77] Yet, if the threshold has not been significantly lowered, at the very least its location has been obfuscated.

The NPR seems incomplete where in comes to identifying many concrete credibility gaps that are not addressed by the existing posture that necessitate increasing flexibility and offering "tailored responses". If the text represents a change in nuclear doctrine, the only real change from the time of the 2010 review to now in terms of nuclear capabilities is in Russian posture. China has invested in conventional, and not nuclear capabilities. There has been no radical expansion of the Chinese program, and the doctrine is still a minimal one. In which scenario will U.S. lower-yield pre-strategic nuclear weapons aid the U.S. or its allies? With regards to North Korea, the newer, more flexible range of weapons foreseen in the NPR would not be relevant. If anything, the use of low-yield weapons by the U.S. would immediately trigger the maximum response from the weaker and more vulnerable nuclear forces of North Korea.[78] The 2018 NPR also includes North Korea and Iran as states to be deterred. The document notes that North Korea threatens "regional and global peace".[79] The Iranian program was still contained by the JCPOA at the time the NPR was written. The 2018 NPR stresses that Iran's ambitions remain an "unresolved concern".[80] Yet, it does not seem to offer much that is specific for either one.

The 2018 NPR also reiterates past policy: "The United States will not use or threaten to use nuclear weapons against non-nuclear states that are party to the NPT and in compliance with their nuclear non-proliferation obligations." So far, the U.S.

[75]Office of the Under-Secretary of Defense 2018, pp. VII, VIII.
[76]Office of the Under-Secretary of Defense 2018, pp. 21, 55.
[77]Office of the Under-Secretary of Defense 2018, p. II.
[78]Steinberg 2018.
[79]Office of the Under-Secretary of Defense 2018, p. I.
[80]Office of the Under-Secretary of Defense 2018, p. I.

has refused to disavow a first strike with nuclear weapons. Yet, during the 2019–2020 Democratic Party presidential primaries, candidates argued in favour of the U.S. adopting a "no first use" policy.[81] As the Center for Arms Control and Non-Proliferation argues, a "no first use policy" could increase crisis stability by formalizing that nuclear weapons are only for deterrence and not "nuclear war-fighting", thereby lowering the risk of nuclear-armed adversaries escalating to the nuclear level. A "no first use policy" would give Congress its rightful place in the decision to go to war.[82] However, "first use" exists as an option because of U.S. alliance commitments, in the scenario that adversaries threaten U.S. allies or partners with conventional attack.

6.6 Difficult Decades Ahead

The chapter has argued that the future of the U.S. extended deterrence guarantee is precarious. It is increasingly unclear whether the U.S. can be credible without being escalatory, and vice versa. From its inception the problem of extended nuclear deterrence is that it is inherently dubious. However, as the U.S. is less and less sure whether it can fight and win conventional conflicts at low costs, the asymmetry of interests between the U.S. on the one hand, and its allies and adversaries on the other, is likely to play a greater role. At its core, as long as the U.S. maintains its alliance commitments, this will continue to generate uncertainty that this and future U.S. nuclear posture must address. Four additional points will serve to conclude the chapters.

First, the NPR emphasizes the possibility of U.S. deterrence failure due to changing Russian and Chinese nuclear capabilities. Yet, arguably the political signalling from the Trump administration has contributed to undermining the credibility of U.S. commitments to its allies.[83] The Trump administration's policies have been rife with ambiguity. The commitment of resources to the European Reassurance Initiative has taken place at the same time as the President's rhetorical dismissal of the value of alliances,[84] and obvious preference for a more transactional approach to alliances.[85] President Trump has also unsubtly poked his finger at the sore spot of the inherently dubious nature of the U.S. guarantees; the U.S. takes on real risks on behalf of states that present at best peripheral interests to the

[81]Elizabeth Warren, Bernie Sanders, and Joe Biden favor no first use. Egelko 2019.

[82]Center for Arms Control and Non-Proliferation n.d.

[83]In 2018 and 2019, the author interviewed former (and even current) U.S. national security officials. A key question was what they perceived as the main current challenges to the U.S. system of extended deterrence: over half considered the real challenge to deterrence in Europe and Asia to be statements by President Trump.

[84]Reuters 2019; Barnes and Cooper 2019.

[85]Leonnig and Rucker 2020.

U.S.[86] There is thus a clear tension between the current U.S. administration's sceptical outlook towards alliances and its focus on greater renewed nuclear superiority and flexibility. U.S. allies must decide what they will make of this discrepancy, and how it compares to previous fractures in the alliance. In doing so, they should keep in mind that Trump's style of politics is unusual, but that calls for retrenchment were growing before he came to office.[87]

Second, the long-term U.S. commitment to European and Asian security is arguably more precarious for structural reasons that extend beyond the Trump presidency. The physical presence of U.S. forces has addressed the question of whether the U.S. has sufficient interests at stake in other regions. It is not clear whether it is still guaranteed, as the U.S. is increasingly challenged conventionally, especially in Asia, and has moved towards a one-war planning standard. Theoretically, there is a threshold "point X" below which the U.S. presence cannot go below without losing credibility with both its adversaries and allies. Point X would be a function of perceived U.S. interests at stake in the region (which includes the physical presence of U.S. forces as well as rhetorical commitments), the costs of U.S. commitments if it attempts to defend against aggression, and the costs of defeat in that region. Adversaries might still refrain from exploring where that threshold is located, because the costs of miscalculation will generally exceed the gains of aggression. One could argue that the simple creation of uncertainty in would-be adversaries' minds about the nature of the potential response—calling to mind Thomas Schelling's notion of a threat "that leaves something to chance"—is sufficient to deter threats to U.S. allies.[88] However, if that is not the case, and the U.S. is no longer to back up its alliance commitments through a physical presence, U.S. allies will find themselves in a precarious situation.

Third, the non-proliferation stance of U.S. allies will not be sustainable if the trends above continue. The 2018 NPR reiterates established U.S. policy by effectively assuring allies and partners depends on their confidence in the credibility of U.S. extended nuclear deterrence. In turn, this enables most allies and partners to eschew possession of nuclear weapons, and consequently contributes to U.S. non-proliferation goals.[89] Yet, even in Europe, a small but remarkable debate on alternative European nuclear arrangement emerged following the 2016 election of Donald Trump.[90] U.S. allies in Asia are also questioning their non-proliferation stances. An alternative to pursuing independent nuclear weapons, with all the instability and risk of escalation that might ensue, is to rely on other nuclear states for their protection. For European allies, such options, theoretically, exist as the UK and France are nuclear weapon states with significant interests in European security.

[86]President Trump claimed that adding Monte Negro could entangle the U.S. in a conflict. The Guardian 2018.

[87]Kinzer 2019.

[88]Schelling 1960, p. 169.

[89]Office of the Under-Secretary of Defense 2018, p. VIII.

[90]Thompson et al. 2018; Tertrais 2019.

Another alternative is the acquisition of significant advanced conventional weapon capabilities by allies who fear U.S. abandonment. In doing so, they can significantly improve their deterrence by denial capabilities to partially compensate for the absence of the U.S. nuclear arsenal. U.S. allies should ask themselves these questions and seek for satisfactory answers. The increasingly precarious commitment of the U.S. to its European and Asian alliances requires them to do so.

Finally, as noted at the beginning of the chapter, policy debates and scholarship on nuclear deterrence have often been explicitly or implicitly informed by the demands the U.S. placed on itself to provide extended nuclear deterrence and the difficulties it faced due to its extra-regional status. This holds even if most authors frame the problems of U.S. nuclear deterrence as those following from direct deterrence. However, if the U.S. would no longer play the role of extended nuclear deterrence guarantor to the same extent, the notion of what is sufficient to deterrence is likely to change. The nuclear arsenals of states that are not the U.S. and Russia are significantly smaller and less sophisticated. Should the U.S. stop playing its role, a reinvention of the grammar of nuclear deterrence that is specified by separate regions will be in order.

References

Acton J (2020) Is It a Nuke? Pre-Launch Ambiguity and Inadvertent Escalation. Carnegie Endowment for International Peace, Washington DC

Barnes JE, Cooper H (2019) Trump Discussed Pulling U.S. From NATO, Aides Say Amid New Concerns Over Russia. The New York Times, 14 January 2019

Betts R K (2010) Nuclear Blackmail and Nuclear Balance. Brookings Institution Press, Washington DC

Biddle S, Oelrich I (2016) Future Warfare in the Western Pacific: Chinese Antiaccess/Area Denial, US AirSea Battle, and Command of the Commons in East Asia. International Security

Blumenthal M S, Dan (2011) Can a Treaty Contain China's Missiles? http://www.washingtonpost.com/wp-dyn/content/article/2010/12/31/AR2010123104108.html. Accessed 18 January 2020

Brands H, Montgomery E B (2020) One War Is Not Enough: Strategy and Force Planning for Great Power Competition. Texas National Security Review 2.3

Braw E (2015) Behind Putin's Nuclear Threats. Politico EU 18 https://www.politico.eu/article/nato-putin-russia-nuclear-weapons-ukraine-war/. Accessed 11 May 2020

Brodie B, Dunn F S, Wolfers A, Corbett P E, Fox W T R (1946) The Absolute Weapon: Atomic Power and World Order. Harcourt, New York

Center for Arms Control and Non-Proliferation (n.d.) No First Use. https://armscontrolcenter.org/issues/no-first-use/. Accessed 17 January 2020

Colin S, Townsend J (2019) Not Enough Maritime Capability: The Challenge of Reinforcing Europe. Centre for New American Security, Washington DC

Crawford T W (2009) The Endurance of Extended Deterrence: Continuity, Change, and Complexity in Theory and Policy. Complex Deterrence: Strategy in the Global Age 277–303

Cunningham F S, Fravel M T (2015) Assuring Assured Retaliation: China's Nuclear Posture and US-China Strategic Stability. International Security 40.2:7–50

Danilovic V (2001) The Sources of Threat Credibility in Extended Deterrence. Journal of Conflict Resolution 45.3:341–369

Dorminey C, Gomez E (2019) America's Nuclear Crossroads: A Forward-Looking Anthology. Cato Institute
Egelko B (2019) Nuclear Weapons - They're Still out There. Presidential Candidates Have Ideas on Them. San Francisco Chronicle https://www.sfchronicle.com/nation/article/Nuclear-weapons-they-re-still-out-there-14873992.php. Accessed: 17 January 2020
Freedman L (1981) The Evolution of Nuclear Strategy. Palgrave Macmillan, New York NY
Garnham D (1985) Extending Deterrence with German Nuclear Weapons. International Security 10.1:96–110
Gavin F J (2015) Strategies of Inhibition: US Grand Strategy, the Nuclear Revolution, and Nonproliferation. International Security 40.1:9–46
Gavin F J et al (2018) Policy Roundtable: The Trump Administration's Nuclear Posture Review. https://tnsr.org/roundtable/policy-roundtable-trump-administrations-nuclear-posture-review/. Accessed 19 January 2020
Gerzhoy G (2015) Alliance Coercion and Nuclear Restraint: How the United States Thwarted West Germany's Nuclear Ambitions. International Security 394:91–129
Glaser C L (2019) Review of Matthew Kroenig. The Logic of American Nuclear Strategy: Why Strategic Superiority Matters. H-Diplo | ISSF Roundtable X.25
Guardian Staff (2018) 'Very Aggressive': Trump Suggests Montenegro Could Cause World War Three. The Guardian 19 July 2018
Heginbotham E et al (2015) The US-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power, 1996–2017. Rand Corporation
Heginbotham E, Samuels R J (2018) Active Denial: Redesigning Japan's Response to China's Military Challenge. International Security 42.4:128–169
Huth P K (1999) Deterrence and International Conflict: Empirical Findings and Theoretical Debates. Annual Review of Political Science 2.1:25–48
Jang S Y (2016) The Evolution of US Extended Deterrence and South Korea's Nuclear Ambitions. Journal of Strategic Studies 394:502–520
Jervis R, Lebow R N, Stein J G (1985) Psychology and Deterrence. JHU Press, Baltimore
Kennedy J F (1963) Commencement Address at American University https://www.jfklibrary.org/archives/other-resources/john-f-kennedy-speeches/american-university-19630610. Accessed 11 May 2020
Kinzer S (2019) In an Astonishing Turn, George Soros and Charles Koch Team up to End US 'Forever War' Policy, The Boston Globe 30 June 2019
Kristensen H M, Korda M (2019) Chinese Nuclear Forces, 2019. Bulletin of the Atomic Scientists 75.4:171–178
Kristensen H M, Korda M (2020) United States Nuclear Forces, 2020. Bulletin of the Atomic Scientists 76.1:46–60
Kroenig M (2018) The Logic of American Nuclear Strategy: Why Strategic Superiority Matters. Oxford University Press, Oxford
Lanoszka A (2018) Atomic Assurance: The Alliance Politics of Nuclear Proliferation. Cornell University Press, Ithaca NY
Leonnig C D, Rucker P (2020) A Very Stable Genius' Book Excerpt: Inside Trump's Stunning Tirade against Generals. Washington Post 17 January 2020 https://www.washingtonpost.com/politics/youre-a-bunch-of-dopes-and-babies-inside-trumps-stunning-tirade-against-generals/2020/01/16/d6dbb8a6-387e-11ea-bb7b-265f4554af6d_story.html. Accessed 17 January 2020
Lieber K A, Press D G (2017) The New Era of Counterforce: Technological Change and the Future of Nuclear Deterrence. International Security 41.4:9–49
Long A (2018) Nuclear Strategy in an Era of Great Power Competition. Texas National Security Review, Policy Roundtable: The Trump Administration's Nuclear Posture Review (13 February 2018)
Matthews J K, Holt C J (1992) So Many, So Much, So Far, So Fast. United States Transportation Command and Strategic Deployment for Operation Desert Shield/Desert Storm, Joint Chiefs of Staff Washington DC Joint History Office, Washington DC

Mattis J (2018) National Defense Strategy of the United States of America. Department of Defense, Washington DC
Mauroni A (2018) Maintaining the Course - for the Most Part. Texas National Security Review, Policy Roundtable: The Trump Administration's Nuclear Posture Review (13 February 2018)
Mazarr M J et al (2018) What Deters and Why: Exploring Requirements for Effective Deterrence of Interstate Aggression. Rand Corporation, Santa Monica CA
Mearsheimer J J, Walt S M (2016) The Case for Offshore Balancing: A Superior US Grand Stategy, Foreign Affairs 95:70
Montgomery E B (2014) Contested Primacy in the Western Pacific: China's Rise and the Future of US Power Projection. International Security 38.4:115–149
Narang V (2018) The Discrimination Problem: Why Putting Low-Yield Nuclear Weapons on Submarines Is So Dangerous. Texas National Security Review, Policy Roundtable: The Trump Administration's Nuclear Posture Review (13 February 2018)
Nolan J, Radzinsky B (2018) Policy or Party Platform? Making Sense of the Trump Nuclear Posture Review, Texas National Security Review, Policy Roundtable: The Trump Administration's Nuclear Posture Review (13 February 2018)
Office of the Under-Secretary of Defense (2018) 2018 Nuclear Posture Review, Office of the Secretary of Defense, Department of Defense, Washington DC
Pauly R B C (2018) Would US Leaders Push the Button? Wargames and the Sources of Nuclear Restraint. International Security 43.2:151–192
Posen B R (2003) Command of the Commons: The Military Foundation of US Hegemony. International Security 28.1:5–46
Posen B R (1991) Inadvertent Escalation: Conventional War and Nuclear Risks (2014 edn). Cornell University Press, Ithaca NY
Posen B R (2014) Restraint: A New Foundation for US Grand Strategy. Cornell University Press, Ithaca NY
Ravenal E C (1982) Counterforce and Alliance: The Ultimate Connection. International Security 6.4:26–43
Rosenberg D A (1983) The Origins of Overkill: Nuclear Weapons and American Strategy, 1945-1960. International Security 7.4:3–71
Reuters (2019) Trump Renews Criticism of Japan-US Alliance before G20 Summit. Reuters 27 June 2019 https://www.reuters.com/article/us-g20-summit-trump-japan-idUSKCN1TS057. Accessed 31 October 2019
Sayle T A (2019) Enduring Alliance: A History of NATO and the Postwar Global Order. Cornell University Press, Ithaca NY
Schelling T C (1960) The Strategy of Conflict (1980 edn). Harvard University Press, Cambridge
Schelling T, Schelling T C (1966) Arms and Influence. Yale University Press, London
Sechser T S, Fuhrmann M (2013) Crisis Bargaining and Nuclear Blackmail. International Organization 67.1:173–195
Snyder G H (1997) Alliance Politics. Cornell University Press, Ithaca NY
Steinberg J B (2018) Expanding the Options and Lowering the Threshold for Nuclear Weapons, Texas National Security Review, Policy Roundtable: The Trump Administration's Nuclear Posture Review (13 February 2018)
Tertrais B (2019) Will Europe Get Its Own Bomb? The Washington Quarterly 42.2:47–66
Thompson B, Kühn U, Volpe T (2018) Tracking the German Nuclear Debate. Carnegie Endowment for International Peace https://carnegieendowment.org/2018/08/15/tracking-german-nuclear-debate-pub-72884. Accessed 6 May 2019
Thompson J A (1992) The Exaggeration of American Vulnerability: The Anatomy of a Tradition. Diplomatic History 16.1:23–43
Trachtenberg M (1999) A Constructed Peace: The Making of the European Settlement, 1945–1963. Princeton University Press, Princeton
Trump D J (2017) National Security Strategy of the United States of America (December 2017), White House, Washington DC https://www.whitehouse.gov/articles/new-national-security-strategy-new-era/.

Ven Bruusgaard K (2018) The Russian Rogue in the New Nuclear Posture Review, Texas National Security Review, Policy Roundtable: The Trump Administration's Nuclear Posture Review (13 February 2018)
Walt S M (2018) The Hell of Good Intentions: America's Foreign Policy Elite and the Decline of US Primacy. Farrar, Straus and Giroux, New York NY

Paul van Hooft (Ph.D.) is a strategy fellow at the Security Studies Program (SSP) at the Massachusetts Institute of Technology (MIT) and a senior policy analyst at the Hague Centre for Strategic Studies (HCSS). He is a former SSP Stanton Nuclear Security Fellow, and a former Max Weber Fellow at the European University Institute (EUI). Paul Van Hooft received his Ph.D. in political science from the University of Amsterdam (UVA).

Chapter 7
Deterrence by Punishment or Denial? The eFP Case

Jörg Noll, Osman Bojang and Sebastiaan Rietjens

Contents

Abstract In 2017 NATO initiated Enhanced Forward Presence (eFP) in the Baltics to deter Russia. While most studies analyse eFP from the perspective of NATO or the troop contributing countries, this chapter addresses the question how the host nations, i.e. in this contribution Estonia, Latvia and Lithuania, perceive the deterrence strategy underlying eFP as well as their own strategies. In doing this, the chapter emphasizes how strategic culture influences the Baltic countries' behaviour towards deterrence. We found that in Estonia perspectives on eFP were ambiguous. While official documents reflect the official NATO narrative based on deterrence by punishment other sources stress the illusion, expectation or aspiration of deterrence

J. Noll (✉) · O. Bojang · S. Rietjens
Netherlands Defence Academy, Breda, The Netherlands
e-mail: je.noll@mindef.nl

O. Bojang
e-mail: oe.bojang@mindef.nl

S. Rietjens
e-mail: sjh.rietjens.01@mindef.nl

F. Osinga and T. Sweijs (eds.), *NL ARMS Netherlands Annual Review of Military Studies 2020*, NL ARMS, https://doi.org/10.1007/978-94-6265-419-8_7

by denial. In Lithuania, documents, officials and experts emphasize deterrence by denial as opposed to deterrence by punishment. Latvia considers the strategy behind eFP as deterrence by punishment. The strategic cultures, the history and threat perceptions of the Baltic states explain these differences to a large extent. In particular the presence of Russophone minorities in Estonia and Latvia, lead to some reluctance in fully embracing NATO's strategy, while at the same time both countries prepare to counter Russia's threat with their allies.

Keywords Strategic Culture · eFP · NATO · Estonia · Latvia · Lithuania

7.1 Introduction

The security and defence policies of the Baltic states are strongly influenced by the Russian aggression of 2014.[1] This also holds true for NATO. The alliance has deployed around 4,500 troops to Poland and the Baltic States since 2017. There is a large consensus amongst academics and practitioners that this mission, labelled Enhanced Forward Presence (eFP), should deter Russian aggression. However, the strategy to do so remains highly ambiguous and unclear (see also Rynning's chapter in this volume). While many official NATO documents as well as observers simply refer to the strategy as deterrence, others, either explicitly or implicitly, distinguish between *deterrence by denial*[2] or *deterrence by punishment.*[3] The exact nature of the strategy can have far reaching consequences in terms of allocation of resources, strategic communication, (perceived) effectiveness as well as the very foundation of the alliance itself: the trust of every ally that it is protected by NATO in case of aggression.

Traditional deterrence theory presumes a rational actor perspective. Over time the role of psychology and actor specific perceptions has become more appreciated, in particular in the third wave in the deterrence literature. Most of these studies have focused on the history of the deterrent relationship and the nature of signaling behaviour.[4] However, although strategic culture has been widely acknowledged as an important shaping factor of strategic behaviour,[5] the role of strategic culture has been largely ignored in deterrence studies. This contribution aims to address this gap. Specifically, this chapter focuses on how strategic culture influences the Baltic countries' behaviour towards deterrence.

While most of the literature analyses eFP from the perspective of NATO or the troop contributing countries, this chapter addresses the question how the host

[1]Rostoks and Vanaga 2016, p. 71.
[2]E.g. Daalder 2017.
[3]E.g. Zapfe 2017.
[4]Lebow 1991, p. viii; Jervis 1991.
[5]Booth 2005, p. 25.

nations, i.e. in this contribution Estonia, Latvia and Lithuania, perceive the strategy underlying eFP and their own strategies. Given the fact that NATO's responses in the Baltics post-2014 were also intended to be 'assurance measures', such a perspective is important because similar or diverging perspectives can have far reaching consequences for NATO's strategy and its credibility. We found that in Latvia official documents reflect the official NATO narrative based on deterrence by punishment. In Estonia and Lithuania, documents, officials and experts emphasize deterrence by denial as opposed or sometimes even parallel to deterrence by punishment. To understand these tendencies, this contribution contends that the respective strategic cultures of the host nations influence their perspectives on the NATO's strategy. To that end, Sect. 7.2 briefly addresses the debate on deterrence and the different perspectives observers take on the eFP mission. Section 7.3 subsequently introduces strategic culture theory as a lens to explain the perspectives of the host nations. Section 7.4 outlines the methods we used. We discuss the results in Sect. 7.5 and provide a discussion and conclusions in Sect. 7.6.

7.2 The Academic Divide: eFP, Deterrence by Punishment or by Denial?

Like the other chapters in this volume, we share the definition that deterrence refers to the practice, the process or the situation in which one state relies on the prospect of harm to persuade an opponent not to engage in certain specified behaviour. Deterrence-by-denial relies on convincing the opponent that it is unlikely to attain its immediate objectives at a reasonable cost, whereas deterrence-by-punishment consists of the threat of great harm which will be imposed after the opponent has engaged in unwanted behaviour. The success of deterrence is highly dependent on the credibility of the threat, which is in turn strongly linked to the level of commitment to the deterrence strategy (preferences), the costs and risks associated with the fulfilment of the threat and the credibility of the promise for rewarding compliance.[6]

Turning to eFP, while not indicating the exact strategy explicitly, most NATO documents as well as its officials point towards a strategy deterrence by punishment.[7] They strongly emphasize NATO's respect for international agreements, commitments and obligations and declare that the aim of eFP is to "unambiguously demonstrate Allied solidarity".[8] Moreover, they signal to the world that any aggression towards the Baltic States and Poland will be met with a collective response, thereby leaving little doubt that deterrence by punishment is the main strategy behind eFP according to NATO. Meanwhile, indicators of deterrence by

[6]Schelling 1966, p. 6.

[7]NATO 2016a, b, 2017, 2018a, b, c, d.

[8]Ibid.

denial, such as improved capabilities or logistics, were not emphasized as much. When discussing deterrence within NATO context, it is important to keep in mind that it is ultimately a form of extended deterrence based on the solidarity between member states, most crucially the US. Greater effort is therefore required to signal readiness and determination as there is always doubt whether a pledge to defend a third party will be upheld.[9]

Amongst experts and academia there is, however, no clear consensus on which deterrence strategy eFP is based. There is a large group of pundits that explicitly[10] or implicitly[11] argue that the strategy behind eFP is, or should be, deterrence by denial. They emphasize a number of military factors such as the role of the Kaliningrad exclave. Kaliningrad is heavily defended with so-called anti-access and area denial (A2/AD) systems and precision strike capabilities, which can supposedly disrupt, neutralize or even destroy NATO forces in the Baltic region before reinforcements could arrive.[12] Moreover, these capabilities deny NATO air and maritime superiority in the Baltic area as well as large parts of Poland and Germany, which in turn, according to these authors, will deny access to reinforcements to the Baltics or at least make such a NATO effort very costly. This raises doubts about NATO's ability to deliver on its declared deterrence strategy presuming it is based on deterrence by denial. Their concern with the Kaliningrad exclave shows that those experts assume that eFP is meant to hold out against a large-scale Russian invasion. NATO's forward presences have supposedly never been mere 'tripwire forces'.[13] With the aim of balancing against Russia, this group of observers generally also recommends sending additional reinforcements to the Baltic region[14] next to investing in conventional capabilities and improving military logistics.[15] All of these measures are meant to strengthen eFP to the point that it can withstand a Russian invasion, thereby revealing that the authors assume that the strategy behind eFP is deterrence by denial, or argue that NATO should aspire to evolve into such a strategy. Most of these denial measures were also strongly recommended to the Dutch government by the Advisory Council on International Affairs (AIV) as they believe the greatest risk facing NATO is a Russian invasion with the aim of a fait accompli due to strategic miscalculation by Moscow.[16]

A second group of academics and experts argues that eFP is based on the strategy of deterrence by punishment. In their views eFP should symbolise NATO

[9]Mazarr 2018, p. 3; Shifrinson 2017, p. 111.

[10]Lanoszka and Hunzeker 2016, p. 14.

[11]Frühling and Lasconjarias 2016; Daalder 2017; Pothier 2017.

[12]Lanoszka and Hunzeker 2016, p. 12.

[13]Ibid., p. 14.

[14]Daalder 2017, p. 37; Frühling and Lasconjarias 2016, p. 108; Lanoszka and Hunzeker 2016, p. 17; Pothier 2017, p. 77.

[15]Daalder 2017, p. 37; Frühling and Lasconjarias 2016, p. 110.

[16]Advisory Council on International Affairs 2017, p. 21.

unity and solidarity, but is no more than a so-called 'tripwire force'.[17] Fear of an arms race due to the Russian security dilemma makes these pundits skeptical of further reinforcing the Baltic region.[18] It is this same logic that makes European member states reluctant to send follow-on forces to the Baltic region instead preferring deterrence by ambiguity, but this is in effect deterrence by punishment.[19] Moreover, this group of experts argues that the divergent interests within NATO simply make deterrence by denial unrealistic.[20] In general, those who conceive NATO's strategy pointing towards deterrence by punishment show a much greater appreciation for the nuances of deterrence theory as they actually make specific mention of deterrence by punishment,[21] while deterrence by denial proponents write about eFP without distinguishing the exact form of deterrence, Lanoszka and Hunzeker (2016) being a notable exception. Moreover, they do not consider the possibility of deterrence of denial leading to an arms race with Russia or they claim an arms race is already ongoing without providing any clear evidence.

Ultimately, however, deterrence theory is a formal theory for determining rational moves. It cannot be used to explain why certain states are motivated towards certain goals or why a group of states might perceive an ambiguous deterrence strategy as either deterrence by denial or deterrence by punishment. Nor does it explain why states in a similar geopolitical position facing the same geopolitical threat hold different views on a commonly devised deterrence strategy. To gain insight into the perceptions and expectations of states, this chapter turns to strategic culture.

7.3 Strategic Culture

When reacting to Robert Kagan's provocative view of Europe's pacifistic strategic culture, Adrian Hyde-Price emphasized that "European attitudes to the use of force are characterized by considerable heterogeneity. These differences cannot simply be attributed to relative power differentials", but have to be seen in the light of diverse historical and cultural experiences.[22] Theories based on rationality, like realism and most deterrence approaches, fall short of explaining differences between supposedly functional similar countries with comparable capabilities, facing a supposed similar threat in their vicinity. And even with similar historical experiences, like the Baltic states have had over the last century, nature and value of a strategic choice, like NATO's deterrence by punishment, face different interpretations and choices by

[17]Zapfe 2017, p. 152.
[18]Kroenig 2015, p. 65; Zapfe 2017, p. 158; Veebel 2018, p. 232.
[19]Ringmose and Rynning 2017, p. 134.
[20]Ibid., p. 135; Veebel 2018, p. 239.
[21]Ringmose and Rynning 2017, p. 129; Veebel 2018, p. 230; Zapfe 2017, p. 157.
[22]Hyde-Price 2004, p. 325.

those countries hosting NATO members' armed forces to deter Russia. This contribution uses the concept of strategic culture to show why Estonia and Latvia at first sight appear to be content with NATO's recent strategy, but "secretly" tending towards deterrence by denial and why Lithuania perceives NATO's and its own strategy much more as deterrence by denial.

There are broadly three traditions of strategic culture. The first sees strategic culture as the context "within which states form their security policies".[23] Associated with Snyder and Gray this includes also history and political culture.[24] The second tradition looks for the difference between state's official security and defence policy and what their actual motivations are.[25] The third considers strategic culture as an independent variable influencing the strategic choices of a state.[26] All three have methodological challenges. As far as the second tradition is concerned, it is difficult to find reliable evidence. Also, it is not the purpose of this contribution to find a hidden agenda of the countries under scrutiny. The third tradition is looking for a silver bullet, a single variable explaining a state's behaviour, which is "a rather ridged approach, implying the option to derive falsifiable hypotheses".[27]

We situate our contribution within the first tradition of studies, seeing strategic culture as the context within which national security and defence policy takes place. It influences but does not determine behaviour of actors within a security community.[28] Following Biehl et al. (2013) we therefore define strategic culture as "a number of shared beliefs, norms and ideas within a given society that generate specific expectations about the respective community's preferences and actions in security and defence policy".[29] To understand the origins of a particular strategic culture, it is necessary to consider the geography of a country, its (political) culture and history.[30] Elites are seen as the carriers of strategic culture[31] and many of the strategic documents express elite consensus on security strategy. These documents are subsequently used for planning and serve as "an instrument of public policy, communicating with and shaping domestic and external audiences".[32] In addition to the elites there are many subgroups that may have different interpretations on the security strategy. These interpretations "compete with each other to offer the 'most

[23]Biehl et al. 2013, p. 10.

[24]Becker and Malesky 2017, p. 165.

[25]Biehl et al. 2013, p. 10; Becker and Malesky 2017, p. 165.

[26]Cf. Johnston 1998, p. 10.

[27]Biehl et al. 2013, p. 10.

[28]Ibid., p. 11.

[29]Ibid., p. 12. See also Miklóssy and Smith 2019 for a debate about the (dis)advantages and methodological challenges of each tradition.

[30]Hyde-Price 2004, p. 325.

[31]Biehl et al. 2013, p. 12.

[32]Becker and Malesky 2017, p. 165.

accurate' interpretation of the state's international context".[33] Hence the importance of official documents, public statements and pundit contributions that fuel the public debate. They reflect the views of the elites, of different subgroups and with that the dominant and subordinate narratives about a state's strategic culture.

7.4 Method and Data

Given the explorative nature of this research, and the complexity and richness of the context, a case study approach is the most appropriate research strategy.[34] We are focusing on this strategy since it provides clarity and direction in method and operationalization. Following Yin's case study approach, the theoretical concepts of deterrence and strategic cultures outlined in the previous sections were applied to eFP.[35]

Based on the recommendations by proponents of deterrence by denial and deterrence by punishment, it is possible to identify specific indicators that primarily pertain to one of these two deterrence strategies in the context of NATO eFP. We will now provide an oversight of the main factors that are deemed important by both proponents of deterrence by denial and deterrence by punishment. These factors will be used as indicators for determining which specific form of deterrence is meant in the analysis of official texts and interviews.

Starting with deterrence by denial, proponents of this strategy place a very high value on the direct defence of the Baltic region. They therefore argue that eFP should be reinforced even before a conflict arises with the experts at RAND even going as far as to recommend that seven brigades be placed in the Baltic states and Poland.[36] Other proponents of the same strategy recommend improving the military capabilities of eFP and other NATO forces in the region.[37] Proponents of deterrence by denial are also strong advocates of improved logistics to ensure the timely arrival of follow-on forces in case of a conflict.[38] They often view the Russian A2/AD capabilities in Kaliningrad as a serious concern in this context as Russia could use its exclave to block follow-on forces from reaching the Baltic states.[39] This concern ties into another factor of importance to deterrence by denial proponents, which is the fear of a fait accompli. The fear is that Russia could use its time-distance

[33]Miklóssy and Smith 2019, p. xiv.

[34]George and Bennet 2005.

[35]Yin 2009.

[36]Lanoszka and Hunzeker 2016, p. 13; Shlapak and Johnson 2016, p. 8; Boston et al. 2018, p. 11.

[37]Daalder 2017, p. 38; Lanoszka and Hunzeker 2016, p. 16; Pothier 2017, p. 77; Mazarr et al. 2018, p. 83.

[38]Daalder 2017, p. 37; Frühling and Lasconjarias 2016, p. 110; Lanoszka and Hunzeker 2016, p. 14; Mazarr et al. 2018, p. 86.

[39]Frühling and Lasconjarias 2016, p. 107; Lanoszka and Hunzeker 2016, p. 12; Pothier 2017, p. 78; Mazarr et al. 2018, p. 71.

advantage and superior troop numbers to overwhelm the Baltic states (as predicted in the RAND wargames), thereby making deterrence by denial the only viable strategy for NATO to protect the Baltic region.[40] In summary, the most important factors to deterrence by denial proponents in the context of eFP are: (1) the immediate reinforcement of eFP, (2) enhancement of eFP capabilities, (3) improved logistics for the sake of eFP follow-on forces, and (4) the fear of a fait accompli.

As for deterrence by punishment, the proponents of this strategy mainly view eFP as a way to guarantee retaliation against Russia in the case of a conventional attack i.e. a tripwire.[41] The primary strength of eFP is therefore symbolic as it is supposed to remind Russia that Article 5 of the North Atlantic Treaty is alive and well and that there is unity and solidarity between the member states of NATO.[42] With the aim of strengthening this message to Russia, proponents of deterrence by punishment often argue that NATO should improve its strategic preparedness.[43] However, the fear of (intensifying) an arms race is also one of the concerns held by proponents of deterrence by punishment, because an unnecessary conflict with Russia is to be avoided.[44] In short, the most important factors for proponents of the strategy of deterrence by punishment are: (1) the tripwire function of eFP, (2) the symbolism of NATO unity and solidarity, (3) signalling through strategic preparedness, and (4) the fear of (intensifying) an arms race. As mentioned earlier, these two groups of indicators are used to identify the specific deterrence strategy in our analysis of official texts and interviews.

Regarding strategic culture, and following Biehl et al. (2013) we consider four dimensions:[45]

(1) Level of Ambition, on a continuum between passive indifference and active international leadership. Data relating to that dimension are among others the country's main objectives in the security realm and the country's tendency to promote proactive intervention, including troops deployed.
(2) Scope of Action for the Executive, which is expressed on a continuum between a low level and a high level of executive flexibility. Here, it is important to look for example at the key players in security and defence policy.
(3) Foreign Policy Orientation, which is situated on a continuum between a European and a transatlantic focus as the country's preferred forum of security and defence cooperation.
(4) Willingness to Use Military Force, in other words, it is placed on a continuum between reluctance and unconstrained acceptance to use military force as an instrument of security policy. Here, we are looking for the role of the armed forces and how the core tasks for the armed forces are defined. It is also

[40]Lanoszka and Hunzeker 2016, p. 16; Shlapak and Johnson 2016, p. 4.
[41]Veebel 2018, p. 247; Zapfe 2017, p. 152.
[42]Ringmose and Rynning 2017, p. 141; Zapfe 2017, p. 150.
[43]Kroenig 2015, p. 61; Veebel 2018, p. 248; Zapfe 2017, p. 157.
[44]Kroenig 2015, p. 65; Veebel 2018, p. 245.
[45]Biehl et al. 2013, pp. 13–16.

important how different tasks are being prioritized (e.g. territorial defence is more important than international crisis management).

The advantage of using the framework by Biehl et al. (2013), is that it gives clear guidance for operationalising the concept of strategic culture. The different questions relating to the four dimensions offer a transparent operationalisation, justifying which variables and indicators have been selected to provide valid conclusions.[46] Additionally, the framework proved its merits when it was well applied to 28 European nations, including the three countries under scrutiny. To fully comprehend and grasp the strategic cultures, the framework is extended with historical experiences and an analysis of possible subcultures.

To that aim, the data collection involved several distinct sources. A thorough desk research was carried out. This included the national security concepts of the Baltic states and retrieving data on relevant indicators of deterrence and dimensions of strategic culture. Second, 20 semi-structured interviews were held with high level officials and experts in the different countries. Most of the stakeholders were active at ministerial level, the armed forces or think thanks.[47] The interviews were used mainly for triangulation purposes, since the number was too low to draw valid inferences solely on their own merits. As a third input the second author made two visits to the Baltic States and Poland in December 2018 and June 2019. These visits lasted 6 weeks in total. During these visits he was able to acquire many relevant documents and held numerous (informal) conversations.[48]

7.5 Deterrence and Strategic Cultures of the Baltic eFP Hosting Countries

7.5.1 Estonia

Estonia sees NATO's strategy as deterrence by denial. Prior to the Russian aggression in Ukraine and Crimea in 2014, Estonia, as Salu and Männik convincingly show, was "a small state deeply worried about its (hard) security".[49] The country strived to prevent marginalization within the alliance, punching above its weight when participating in Alliance missions. However, since the incidents in 2014 much has changed. Estonia's renewed military strategy foresees a great increase in terms of operational capacity. The country is planning to have an

[46]For the entire operationalization, see Biehl et al. 2013, pp. 13–16.

[47]The interviews were conducted in confidentiality, however, a list of questions can be obtained by the authors.

[48]The first author of this contribution travelled several times through the countries either in preparation of visits with different student groups or with those groups, and talked extensively to experts, diplomats and officials in all three countries. This also holds true for the third author.

[49]Salu and Männik 2013, p. 109.

operational wartime structure of 60,000 personnel, approximately 4.5% of the entire population.[50]

While the goals are broader, including interoperability with NATO and EU and participation in Alliance and international missions, like Mali, it is fair to say that the main aim of the Estonian Defence Forces is "the preservation of the independence and sovereignty of the state, the integrity of its land area, territorial waters and airspace and its constitutional order".[51] By 2026, the 1st Infantry Brigade will be fully mechanised and the 2nd will be equipped with two more battalions, one infantry and one artillery.[52] In 2018 the defence budget of the country rose to 524 million euro, or 2.14% of the GDP. The strategy of the country has clearly changed from the post-Cold War internationalism towards the development of the "capabilities for ensuring the initial self-defence capability of Estonia".[53] At the same time the country invests in improving the conditions for hosting NATO forces, including necessary infrastructure. In particular, the relation to the US and its "presence in Europe, including in the Baltic Sea region, serves Estonia's interests".[54] The tasks of air force and navy are rather limited. While the first focuses on air surveillance and the hosting of aircraft and personnel of allied forces, the latter concentrates on mine countermeasure capabilities.[55] In case of a direct attack against Estonia or an ally, the Estonian President has the authority to declare the state of war or order mobilization, without authorization from the parliament, Riigikogu. In all other cases the President and the government have to ask Riigikogu for authorizing the use of the armed forces. In other words, only in case of a direct attack, the government is flexible. Parliament must approve missions abroad.[56]

The country clearly prioritizes collective defence, yet relies at the same time on its ability to defend itself: "Estonia's consistent commitment to development of military defence and Allies' readiness to spend noteworthy resources for strengthening NATO's deterrence and defence posture in the region give assurance that in the changing world, Estonia's military security rests strongly on two pillars: a well-designed independent defence capability and trustworthy collective defence."[57] To that end the country adapted a comprehensive security approach based on resilience and deterrence, following with that the early examples of Norway, Sweden and Finland.[58] Yet, as Veebel and Ploom (2018) show, a civilian-military divide exists when it comes to resilience, in which the former

[50] https://mil.ee/en/defence-forces/ as of 16 March 2020.
[51] https://mil.ee/en/defence-forces/ as of 16 March 2020.
[52] Estonian Ministry of Defence 2016.
[53] Estonian Ministry of Defence 2016.
[54] Estonian Ministry of Defence 2011, p. 9.
[55] Estonian Ministry of Defence 2016.
[56] Salu and Männik 2013, p. 107.
[57] Estonian Ministry of Defence 2016.
[58] Veebel and Ploom 2018.

interprets the security approach more in societal and economical terms while the latter focuses on the military or hard aspects.[59] In other words, the civilian interpretation of resilience forms a subgroup with its own security strategy.

This also holds true for the Russian or Russophone minority. Estonia has a large Russophone minority of approximately 25%.[60] This subgroup can influence the strategic culture of a country. It can do so either by influencing elite discourse, or by influencing beliefs, norms and ideas. There is a Russian tendency to influence the ethnic and cultural minority in the country, but there is little evidence this is successful. Nielsen and Paabo (2015) found that "although Russia does indeed have a number of soft power resources, their potential for being translated into actual power and influence is too often exaggerated, not least because Europe provides a much more attractive focus point for the disgruntled".[61] Most Russophone citizens, which also include Belarussians and Ukrainians, are satisfied with the status quo as the European Union offers a more prosperous existence than Putin's Russia.[62] However, when it comes to NATO, the divide between the different ethnic groups becomes much more obvious. Only 33% of the Russophone minority supports membership in NATO, compared to 92% of ethnic Estonians.[63] There is, in other words, a divide between the perception of NATO and Russia along ethnic and lingual divides.

Estonian respondents generally agreed that eFP's main goal is to demonstrate alliance solidarity and to signal a strong message to Russia, as is the official line. The respondents do not think that an increase in troop numbers or a more permanent presence is necessary as long as the threat level remains stable. Yet, at the same time, the respondents emphasize an interest in improved military capabilities. This is also in line with the official policy to invest heavily in the armed forces by 2026. In case of a large-scale scenario, according to the Estonian constitution, the country "will continue to resist any foreign invader no matter how large" for as long as possible and wait for NATO reinforcements to arrive. Additionally, while the respondents agree that eFP is militarily more than a tripwire, which points towards a denial strategy, one of the Estonian respondents stresses that "[i]n a political sense, eFP might be considered a tripwire."

In 2013 Biehl et al. concluded that Estonia's strategic culture reflected a security policy as international bargaining, due to a low to medium international level of ambition, strong legislative rights in sending armed forces abroad, functional view of NATO for collective defence and a high willingness to use military force for

[59]Ibid., p. 9.

[60]328,299 on a total population of 1,324,820 (as of 1 January 2019), see https://andmed.stat.ee/en/stat/rahvastik__rahvastikunaitajad-ja-koosseis__rahvaarv-ja-rahvastiku-koosseis/RV0222, retrieved 16 March 2020.

[61]Nielsen and Paabo 2015, p. 125.

[62]Noll et al. 2017.

[63]Atmante et al. 2019, p. 64. See also Veebel and Ploom 2016, pp. 46, 48.

defence purpose and less for crisis management.[64] This has changed. In particular the defence of the own country became much more important. With that the flexibility of the executive changed, since Estonia's parliament has less authority in response to an attack as compared to deciding on sending troops abroad. Hence, it is fair to say that the country's strategic culture is more focused on protecting and projecting state power than 10 years ago, perceiving threat for the vulnerable national territory and thereby striving for deterrence by denial. The influence of the Russophone minority and the military-civilian divide on resilience and with that the whole of government approach to defence might be countervailing forces for a new strategy.

7.5.2 Latvia

Like Estonia, Latvia underscores NATO's strategy. At the same time, the country is looking for deterrence by denial, not so much by the alliance but with its own capabilities. The reasons for that can be found in its history, its comprehensive defence and the Russophone minority. In 2013 Rikveilis wrote "that a parallel strategic culture might be emerging in Latvia" favouring closer ties with Russia both economically and politically.[65] He continues that "it is possible that in the near future the current strategic elite will be forced to justify its principles of unequivocal orientation towards the West in more sophisticated ways than simply alluding to Latvia's natural place in the 'European family'". This elite is confronted with a dilemma, the more it strongly favours US involvement in European security affairs. The developments since 2014 again show the ethnic divide.

Yet, like in Estonia, several studies show that the Russophone minority has a different view of Russia and NATO than ethnic Latvians do. Being an important minority of 26%, Russophones tend more towards Eastern and post-Soviet countries than to Western countries. In 2015, 64% of the ethnic Latvians considered Russia a threat, compared to 23% of the Russophones.[66] When it comes to NATO 65% of the ethnic Latvians are confident while 27% are not. Meanwhile, 69% of the Russophones distrust NATO and 21% does not. Even more important is their view about stationing allied troops in the country: the majority (58%) of the ethnic Latvians has a positive attitude, while the majority (54%) of the Russophones has a negative attitude.[67] The size of the Russophones and their views are a non-neglectable factor for Latvians strategic culture and with that strategic choices. When talking to officials and experts, some emphasized the sensitivity of having a

[64]Biehl et al. 2013, p. 394.

[65]Rikveilis 2013, p. 215.

[66]Rostoks and Vanaga 2016, pp. 90–91 (Latvia's Security and Defence Post-2014).

[67]Rostoks and Vanaga 2016, p. 99.

greater US presence in Latvia, due to public opinion, while others could imagine more US engagement.

Central to Latvian security and defence policy is the concept of Comprehensive Defence, announced in August 2018: "The aim is to strengthen the cooperation among state institutions, provide effective mechanisms for public—private partnership, increase the skills and capabilities of the society to protect themselves, their families and Latvia in case of crisis".[68] It comprises seven pillars, ranging from military capabilities to psychological resilience.[69] In its nature and scope, this concept is comparable to Finnish Comprehensive Security.[70] The minority issue influences also Latvia's resilience, closely associated with the country's comprehensive defence. Like in Estonia the chance that Russia might use the minorities as a pretext to seize the country are rather slim. Yet the linguistic divide and the domination of Russian information channels undermine the government's striving for an effective comprehensive approach.

While in 2016 Reire contended that resilience is about coping with threats "that are not related to defensive security and the concept of deterrence",[71] the government interprets "comprehensive defence means that people are organized to defend the country against all forms of attack, both military and non-military".[72] It shows that the country focuses on territorial defence with almost all means available. This is also reflected in the main aim of the armed forces, defending the sovereignty and territorial integrity of the country. Like in many other NATO and EU member states, international missions and (civil) emergency rank second and third as main task. Over the years, the country participated in a broad variety of international (military) operations led by NATO and EU, including ISAF and follow-up missions.[73]

With a relatively small-sized country and a population of less than 2 million people, the armed forces consist of 6000 military personnel and 8300 national guards. Atmante et al. (2019) point to the importance of these national guards, the more they mitigate the debate about reinstating conscription.[74] Compared to 2018, the 2019 defence budget rose with almost 8% to 636 million Euro, 2% of its GDP.[75] The president of Latvia is formally the commander-in-chief of the armed forces, yet

[68]https://www.mod.gov.lv/en/nozares-politika/comprehensive-defence as of 18 March 2020. Compare also to https://www.mod.gov.lv/sites/mod/files/document/Comprehensive%20National%20Defence%20in%20Latvia.docx.

[69]Military capabilities, Public-private cooperation, Education of society, Civil defence, Strategic communication, Economic resilience, Psychological resilience.

[70]Cf. Seppo and Forsberg 2013; https://www.defmin.fi/files/3827/Valtonen_2017_06_14_FI_Concept_for_Comprehensive_Security_Valtonen.pdf as of 18 March 2020.

[71]Reire 2016, p. 179.

[72]https://www.mod.gov.lv/en/nozares-politika/comprehensive-defence as of 16 April 2020.

[73]Anāžans and Veebel 2017, pp. 37–38.

[74]Atmante et al. 2019, p. 65.

[75]https://www.mod.gov.lv/sites/mod/files/document/NBS%20faktu%20lapa%20-%20ENG.pdf as of 18 March 2020.

the prime minister is politically responsible.[76] Their authority with regard to territorial defence is, however, heavily influenced due to a special provision in Latvia's security law from 2015. This law, of which the roots can be traced back to Soviet aggression in 1940, states that it is "a duty of every member of the LNAF to respond to military aggression—even in the absence of any direct orders to that effect (in case command and control ceases to function)".[77]

At first sight it seems that Latvian respondents and official documents mostly emphasize the strategy of deterrence by punishment. On closer look, the perception of eFP and the future planning is slightly mixed. Respondents perceive eFP as deterrence by punishment, yet at the same time most respondents support improved military capabilities. The National Security Concept 2016 points to the strengthening of self-defence capabilities of the country and the need for a long-term presence of allied forces.[78] This, however, is typical for deterrence by denial. This part shows that the strategic culture of Latvia changed towards more protecting and projecting power, indeed with its rather limited capabilities, compared to the eFP partners in the region. The new provision of the security law in 2015 states that the country always has to be defended, the switch towards comprehensive defence and the rise of the defence budget establish a straightforward line towards deterrence by denial. This is also supported by the need for a long-term presence of the allied armed forces. At this moment, however, the country's interpretation of eFP and its own initiatives with regard to its defence are also dependent on Latvia's ability to incorporate its minorities in the efforts. Additionally, the acceptance rate of NATO, its troops stationed in Latvia and the own government has to be higher across the population to have a strategy of deterrence by denial.

7.5.3 Lithuania

"Total and unconditional defence is the main principle of Lithuanian defence meaning that all national resources will be used to defend the State and that every citizen and the entire nation will resist in every way defined as legitimate by international law. Defence of Lithuania is not a subject to any conditions, and no one can inhibit the right of the nation and every citizen to resist an aggressor. Lithuania will defend its sovereignty and resist all aggression independently and without waiting until Allied support is provided".[79] This clearly reflects a strategy of deterrence by denial and, at first sight independence, from eFP and any NATO strategy.

[76]https://likumi.lv/ta/en/id/57980-the-constitution-of-the-republic-of-latvia as of 18 March 2020.
[77]Atmante et al. 2019, p. 65.
[78]Latvian Ministry of Defence 2016.
[79]Lithuanian Ministry of Defence 2017, p. 11.

When looking at Lithuania's strategic culture, Šešelgytė concluded in 2013 forcefully "that it is a country shaped by transatlantic and even militaristic tendencies, albeit with limited resources and opportunities".[80] According to her, the military activism is a strategic choice "to ensure national security via collective defence and a strong bond with the USA". Militaristic here means the prioritization of the military tool in security and defence and a main focal point within the whole of government approach.

It does not take much imagination to see that this has not changed since 2014. On the contrary, the country invested even more in its military capacity and its relation to the U.S. Most Lithuanian respondents would welcome a more permanent US presence, which has been a longstanding policy goal of the Lithuanian Ministry of National Defence. This is confirmed in the 2017 National Security Strategy of the Republic of Lithuania, which mentions the military presence of the US as an important source of strength for the national security of the country.[81]

In 2019, the country had a defence budget of 948 million euro, or 1.99% of its GDP. The breakdown of the expenditures is 42% Personnel, 29% Equipment and 21% Operations and Maintenance. The number of military personnel grew substantively over the past years to more than 20,000 in 2019, including conscripts. Conscription was reintroduced in Lithuania in 2015. While the country participates in several international missions, the defence of the country is top priority. To that end, the country established among others a national rapid reaction force, consisting of up to two battalion-sized battlegroups that can be used against hybrid threats.[82] The greatest security challenge that Lithuania faces is Russia[83] and "its ambition to regain its status as a major power".[84] To counter that threat, Lithuania also has—besides the traditional branches—a state-supported paramilitary organization, the Lithuanian Riflemen's Union (LRU) with approximately 10,000 members. More than 6,000 youngsters (11–18 years) joined the young riflemen, whether or not during summer camps.[85] The country is very clear about the allocation of funds and efforts: "Land Force development is a priority for Lithuania".[86] Even in recent publications, the country focuses on the army, enhancing society resilience and cyber.[87]

It is not surprising that, given the priority for the military in the whole of government approach and the strong will to defend the country, Lithuanian respondents as well as official documents place great emphasis on deterrence by

[80]Šešelgytė 2013, p. 226.

[81]Seimas of the Republic of Lithuania 2017, p. 3.

[82]Lithuanian Ministry of Defence 2018.

[83]Seimas of the Republic of Lithuania 2017, p. 2.

[84]Lithuanian Ministry of Defence 2017, White Paper, p. 7. The Lithuanian White Paper dedicates two pages to Russia and less than one page to the other two perceived threats.

[85]Lithuanian Ministry of Defence 2017, White Paper, pp. 52–53.

[86]Lithuanian Ministry of Defence 2018, p. 5.

[87]Lithuanian Ministry of Defence 2018.

denial. Although they consider eFP as a form of political deterrence, the Lithuanian respondents are quick to point out that eFP is supposed to be underpinned by a viable reinforcement strategy. An increase in eFP troop numbers is not seen as necessary for now, but Lithuanian respondents place a heavy emphasis on improving NATO logistics for the sake of enabling reinforcement, another important denial factor. In a similar way, these respondents were also keen on more advanced and more diverse military capabilities for eFP as this would greatly enhance Lithuania's ability to resist a limited incursion. In practice, however, all Lithuanian respondents perceive eFP as a NATO tripwire, albeit with certain added military functions.

7.6 Conclusion

We concur with Veebel and Ploom's view that "some signs of "self-deterrence" are also visible, referring to unsubstantiated, if not somewhat naïve, views of the political and military elite of the Baltic countries, as well as relying on so-called deterrence by imagination".[88] Yet, contrary to these authors, we were able to link the respective strategic culture of the Baltic states to their perception of eFP and their own strategies. Table 7.1 summarizes our findings.

Estonia is, within its limits, prepared to fight an enemy, relying on a comprehensive or whole of government and society approach. This points towards deterrence by denial. This is supported by the government's will to improve the infrastructure for eFP forces in the country. The country considers eFP to be a force multiplier. Based on the documents and the views held by the respondents we believe the most likely explanation for this perception is that Estonia, having the smallest potential manpower, benefits most from eFP compared to the other host nations and is therefore more convinced of its military value. At the same time, the country has to take into account its Russophone minority in leaning towards NATO.

With eFP, a rising defence budget and a new concept for defending Latvia—whole of society approach—the fear of an ethnic divide within the country seemingly disappeared. Yet non-native Latvian speakers still consider NATO more aggressive than the Latvian-speaking majority. Latvia values the added military strength that eFP offers, but Latvian respondents were slightly skeptical about the timely reinforcement and combat effectiveness of eFP.[89] This resulted in a perceived strategy that is based on deterrence by punishment while striving for more deterrence by denial on its own. The newly introduced concept of comprehensive defence might also foster a strategy that is oriented at deterrence by denial. The important caveat for success of this strategy is the effectiveness of an important

[88]Veebel and Plooms 2018, p. 195.

[89]Veebel and Plooms 2016, pp. 46, 48.

Table 7.1 Overview of deterrence strategy and strategic culture (*Source* The authors)

	Estonia	Latvia	Lithuania
View on NATO's deterrence strategy	Denial	Punishment	Denial and punishment
View on own strategy	Tendency towards denial	Tendency towards denial	Denial
Key characteristics of strategic culture	• Whole of government approach towards security; • Conscription; • Change from security policy as international bargain towards protecting and projecting state power	• Comprehensive defence; • Change from security policy as international bargain towards protecting and projecting state power; • Provision to defend the country at almost any price by law	• Whole of government, yet with a central role of military; • Conscription; • Change from security policy as international bargaining towards projecting and protecting power; • Focus on US, afraid that eFP is not enough
Countervailing forces to strategic culture	• Russophone minority • Military-civilian divide on resilience	• Russophone minority possible threat to resilience	

concept like resilience within heterogenic societies. While Latvia, like Estonia, slightly softened its harsh tune against minorities since the early independent phase, the divide between the ethnic groups is probably still too big to develop effective whole of society strategies against Russian threat.

Although having larger armed forces than the other host nations, Lithuania also appreciates the additional military strength provided by the eFP battlegroups. However, the country puts greater emphasis on striving for deterrence by denial as it expects higher engagement and readiness from NATO in the Baltic region.

What does all this mean for deterrence theory and NATO's deterrence strategy? While most theoretical chapters focus on the effect of deterrence on the adversary, we show that for an effective strategy within an alliance the perceptions of the host nations must be taken into account. NATO deterrence is primarily based on extended deterrence, which means for NATO that it needs to define its strategy more clearly. Different perceptions, not only in the host countries, point to a divide within NATO. It jeopardizes the alliance's solidarity and commitment. Without a common definition and perception any deterrence strategy is prone to the adversaries' moves, even below an Article 5 threshold. Our contribution shows how serious the threat is in the eyes of the Baltic States, the most vulnerable allies when it comes to Russian aggression.

References

Advisory Council on International Affairs (2017) Annual Report 2017. AIV, The Hague
Andžāns M, Veebel V (2017) Deterrence Dilemma in Latvia and Estonia: Finding the Balance between External Military Solidarity and Territorial Defence. Journal on Baltic Security, 3:29–41
Atmante K, Kaljurand R, Jermalavičius T (2019) Strategic Cultures of the Baltic States: The Impact of Russia's New Wars. In: Miklóssy K, Smith H (eds) Strategic Culture in Russia's Neighbourhood: Change and Continuity in an In-Between Space. Lexington Books, Lanham, 53–82
Becker J, Malesky E (2017) The Continent or the "Grand Large"? Strategic Culture and Operational Burden-Sharing in NATO. International Studies Quarterly 61:163–180
Biehl H, Giegerich B, Jonas A (2013) Introduction. In: Biehl H, Giegerich B, Jonas A (eds) Strategic Cultures in Europe: Security and Defence Policies Across the Continent. Wiesbaden, Springer US, 7–17
Booth K (2005) Strategic Culture: Validity and Validation. Oxford Journal on Good Governance, 2:25–28
Boston S, Johnson M, Beauchamp-Mustafaga N, Crane Y (2018) Assessing the conventional force imbalance in Europe: Implications for Countering Russian Local Superiority. Rand Corporation, Santa Monica, CA
Daalder I (2017) Responding to Russia's Resurgence. Foreign Affairs, 96(6):30–38
Estonian Ministry of Defence (2011) National Defence Strategy Estonia. Estonian Ministry of Defence, Tallinn
Estonian Ministry of Defence (2016) Estonian Military Defence 2026. Estonian Ministry of Defence, Tallinn
Frühling S, Lasconjarias G (2016) NATO A2 AD and the Kaliningrad Challenge. Survival, 58:95–116.
George A, Bennet A (2005) Case Studies and Theory Development in the Social Sciences. MIT Press, Cambridge MA
Hyde-Price A (2004) European Security, Strategic Culture, and the Use of Force. European Security, 13: 323–343
Jervis R (1991) Introduction: Approach and Assumptions. In: Jervis R, Lebow R N, Stein JG (eds) Psychology and Deterrence. The Johns Hopkins University Press, Baltimore, pp 1–12
Johnston A (1998) Cultural Realism: Strategic Culture and Grand Strategy in Chinese History. Princeton University Press, Princeton
Kroenig M (2015) Facing Reality: Getting NATO Ready for a New Cold War. Survival, 57: 49–70
Lanoszka A, Hunzeker M (2016) Confronting the Anti Access Area Denial and Precision Strike Challenge in the Baltic Region. The RUSI Journal, 161: 12–18
Latvian Ministry of Defence (2016) National Security Concept of the Republic of Latvia (2016 -). Ministry of Defence Latvia, Riga
Lebow N (1991) Preface and Acknowledgements. In: Jervis R, Lebow R N, Stein JG (eds) Psychology and Deterrence. The Johns Hopkins University Press, Baltimore, pp vii–x
Lithuanian Ministry of Defence (2017) White Paper: Lithuanian Defence Policy. Ministry of National Defence of the Republic of Lithuania, Vilnius
Lithuanian Ministry of Defence (2018) Lithuanian Defence System: Facts and Trends. Ministry of National Defence of the Republic of Lithuania, Vilnius
Mazarr M (2018) Understanding Deterrence. RAND Corporation, Santa Monica, CA
Mazarr M, Chan A, Demus A, Frederick B, Nader A, Pezard S, Thompson J, Treyger E (2018) What Deters and Why: Exploring Requirements for Effective Deterrence of Interstate Aggression. RAND Corporation, Santa Monica, CA

Miklóssy K, Smith H (2019) Introduction: Reviewing Strategic Culture in the Russian Neighbourhood. In: Miklóssy K, Smith H (eds) Strategic Culture in Russia's Neighbourhood: Change and Continuity in an In-Between Space. Lexington Books, Lanham, pp ix–xxiii

NATO (2016a) Warsaw Summit Communique: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8–9 July 2016. NATO, Brussels

NATO (2016b) NATO Summit Guide: Warsaw, 8–9 July 2016. NATO, Brussels

NATO (2017) The Secretary General's Annual Report 2017. NATO, Brussels

NATO (2018a) Brussels Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11–12 July 2018. NATO, Brussels

NATO (2018b) NATO Summit Guide: Brussels, 11–12 July 2018. NATO, Brussels

NATO (2018c) Deterrence and defence. https://www.nato.int/cps/en/natohq/topics_133127.htm

NATO (2018d) Boosting NATO's presence in the East and Southeast. https://www.nato.int/cps/em/natohq/topics_136388.htm

Nielsen K, Paabo H (2015) How Russian Soft Power Fails in Estonia: Or, Why the Russophone Minorities Remain Quiescent. Journal on Baltic Security, 1:125–157

Noll J E et al (2017) De Baltische staten, de Russische minderheid en de verdediging van de NAVO. Militaire Spectator, 186:169–182

Pothier F (2017) An Area Access Strategy for NATO. Survival, 59:73–80

Reire G (2016) Resilience Challenges in the Baltic Countries. In: Andžāns M, Bruģe I (eds) The Baltic Sea Region: Hard and Soft Security Reconsidered. Latvian Institute of International Affairs, Riga, pp 179–200

Rikveilis A (2013) Latvia. In: Biehl H, Giegerich B, Jonas A (eds) Strategic Cultures in Europe: Security and Defence Policies Across the Continent. Wiesbaden, Springer US, pp 207–216

Ringmose J, Rynning S (2017) Now for the Hard Part: NATO's Strategic Adaptation to Russia. Survival, 59:129–146

Rostoks T, Vanaga N (2016) Latvia's security defence post-2014. Journal on Baltic Security, 2:71–108

Salu K, Männik E (2013) Estonia. In: Biehl H, Giegerich B, Jonas A (eds) Strategic Cultures in Europe: Security and Defence Policies Across the Continent. Wiesbaden, Springer US, pp 99–111

Schelling T (1966) The Strategy of Conflict. Harvard University Press, Cambridge

Seimas of the Republic of Lithuania (2017) National Security Strategy of the Republic of Lithuania. Seimas of the Republic of Lithuania, Vilnius

Seppo A, Forsberg T (2013) Finland. In: Biehl H, Giegerich B, Jonas A (eds) Strategic Cultures in Europe: Security and Defence Policies Across the Continent. Wiesbaden, Springer US, pp 113–124

Šešelgytė M (2013) Lithuania. In: Biehl H, Giegerich B, Jonas A (eds) Strategic Cultures in Europe: Security and Defence Policies Across the Continent. Wiesbaden, Springer US, pp 217–218

Shifrinson J (2017) Time to Consolidate NATO? The Washington Quarterly, 40:109–123

Shlapak D, Johnson M (2016) Reinforcing Deterrence on NATO's Eastern Flank: Wargaming the Defence of the Baltics. RAND Corporation, Santa Monica, CA

Veebel V (2018) NATO options and dilemmas for deterring Russia in the Baltic States. Defence Studies, 18:229–251

Veebel V, Ploom I (2016) Estonian Perceptions of Security. Not only about Russia and the Refugees. Journal on Baltic Security, 2 :71–108

Veebel V, Ploom I (2018) Estonia's comprehensive approach to national defence: Origins and dilemmas. Journal on Baltic Security, 4:1–13

Yin R K (2009) Case Study Research: Design and Methods. Sage Publications, Thousand Oaks, CA

Zapfe M (2017) Deterrence from the Ground Up Understanding NATO s Enhanced Forward Presence. Survival, 59:147–160

Dr. Jörg Noll is associate professor Conflict Studies at the Department of War Studies of the Netherlands Defence Academy. He is also a reserve officer in the German Bundeswehr.

Osman Bojang (M.Sc., M.A.) is a media specialist at the Netherlands Ministry of Defence. He conducted research for this project as an air force reserve officer at the Department of War Studies at the Netherlands Defence Academy.

Prof.dr.ir. Sebastiaan Rietjens an engineer by training, is a professor of Intelligence & Security at the Department of War Studies at Netherlands Defence Academy. He has published widely in international books and journals including the International Journal of Intelligence & Counterintelligence (IJIC), Armed Forces & Society (AF&S), Disasters, and the International Journal of Public Administration. His main research focus is on intelligence during military operations, peacekeeping intelligence, information warfare and the implementation of data science.

Chapter 8
The Essence of Cross-Domain Deterrence

Tim Sweijs and Samuel Zilincik

Contents

Tempora mutantur nos et mutamur in illis.

Abstract Both deterrence theory and deterrence practice are evolving to address contemporary strategic challenges. In the military domain, states progressively integrate and synchronise military operations. Outside of it, they exploit grey zone

T. Sweijs (✉)
The Hague Centre for Strategic Studies, The Hague, The Netherlands
e-mail: Timsweijs@hcss.nl

S. Zilincik
Masaryk University, Brno, Czech Republic
e-mail: zilinciks@gmail.com

F. Osinga and T. Sweijs (eds.), *NL ARMS Netherlands Annual Review of Military Studies 2020*, NL ARMS, https://doi.org/10.1007/978-94-6265-419-8_8

strategies that combine different instruments of influence across multiple domains. These developments are now giving birth to a new wave of thinking about cross domain deterrence (CDD), what it precisely entails, and what favouring conditions are necessary for it to be effective. This chapter situates CDD in the context of today's challenges, and identifies the prerequisites for these favouring conditions based on a review of a rather diverse body of literature. It finds that one strand of that literature predominantly focuses on practical and technical prerequisites in order for CDD to be effective, leaving the framework of traditional deterrence theory intact. It also finds a second strand that holds that the nature of today's challenges requires more than mere innovation in application. The ideas about deterrence proposed by this second strand are expanding on common understandings of deterrence to the extent that deterrence is no longer only about fear nor about convincing opponents to refrain from certain behaviour. The conclusion summarises the findings and elaborates their implications for theory and practice.

Keywords deterrence · dissuasion · cross domain · cyberspace · space · grey zone · hybrid threats

8.1 Introduction

Deterrence is about convincing adversaries to refrain from certain behaviour through the prospect of costs that outweigh the benefits.[1] As related in the preface to this volume by Osinga and Sweijs, deterrence has been a central tenet of strategic practice throughout history,[2] even if its logic was only clearly articulated in the aftermath of the Second World War. Deterrence scholarship has since then evolved in four consecutive waves. The first, second and third wave of the deterrence literature, which emerged during the Cold War, tended to almost exclusively focus on deterrence of high-intensity aggression including most importantly the possible use of nuclear weapons alongside large scale conventional invasion.[3] Lower-intensity threats which were considered mere nuisances were largely left outside of the scope of investigation.[4] However, these became more important in the 1990s with the demise of the Soviet Union and the emergence of non-traditional threats such as terrorism.[5] This gave birth to the fourth wave of deterrence literature that focused on the question whether deterrence would work against such threats that emerged in the 1990s and 2000s.[6] Over the past decade, a new body of ideas has been emerging concerning the application of deterrence in today's strategic

[1]Long 2008, pp. 7–8. See also the preface by Osinga and Sweijs in the present volume.
[2]Cioffi-Revilla 1999; Naroll 1974.
[3]Knopf 2010.
[4]Kennan 1948.
[5]Wilner 2011.
[6]Knopf 2010.

environment. An important characteristic of our age is the proliferation of ways and means by which hostile activities can be perpetrated. Accordingly, strategists have started to pay more attention to the application of deterrence in new domains and to cross domain deterrence (CDD), across both traditional and new domains. This chapter appraises the contribution of the emerging body of cross domain deterrence literature to deterrence theory and deterrence practice. It explains the context in which theories of cross domain deterrence have emerged and elaborates different conceptualisations of cross domain deterrence distinguishing between two different approaches. The conclusion summarises the findings and elaborates their implications for theory and practice.[7]

8.2 The Origins of Cross-Domain Deterrence

The shift in attention to CDD can be explained by two principal challenges. The first challenge relates to the progressive integration and synchronization of military operations across different domains (land, air, sea, cyber, and space) and the inherent disharmony between different levels of war (strategic, operational and tactical).[8] This is because military organizations aspire to better integrate physical, social and communication technologies in their ability to apply violence in the pursuit of political objectives, leading to strategic compression and cross domain warfare. Multi-domain operations concepts are being developed to guide efforts to synchronise actions both horizontally across domains and vertically across levels of war.[9] In light of the cross-domain nature of the challenge, strategists are envisaging analogous responses, including CDD.

The second challenge relates to the increased salience of "hybrid" or "grey zone" strategies that feature the simultaneous employment of military and non-military instruments, typically below the conventional military threshold, in an ambiguous fashion in order to evade attribution, with the goal to exploit adversary's vulnerabilities, in the pursuit of political objectives.[10] While the analytical value of the labels as such have caused considerable debate,[11] the real-world impact of these strategies poses a serious strategic challenge. Their increased salience stems from the enormous costs associated with interstate wars, which makes major military powers disinclined from waging actual hot wars against each other. These powers therefore try and find alternative ways to achieve their political objectives—in line

[7]This chapter builds on and further develops ideas that we first discussed in Sweijs and Zilincik 2019.

[8]Luttwak 2002.

[9]This is an evolutionary change, which has been long time in coming, and builds on earlier historical military strategic concepts such as Combined Arms Warfare, Joint Warfare, and Network Centric Warfare. See Black 2018; Johnson 2018; Hayes and Alberts 2003.

[10]Fridman 2018, p. 154; Morris et al. 2019, pp. 7–12; Hoffman 2018.

[11]See for example Stoker and Whiteside 2020.

with the original tenets of the coercive diplomacy literature. Furthermore, the increased salience of grey zone strategies also derives from the opportunities offered by new avenues to hurt opponents due to technological and societal developments because of the global wiring of societies over the past quarter century. Strategically innovative actors have been making frequent use of these avenues over the past decade to considerable effect. These developments have led scholars and strategists to start thinking about the use and utility of cross domain deterrence in dealing with adversaries employing cross domain strategies also outside the traditional military domains.

Authors from both sides of the Atlantic generally concur that cross-domain deterrence involves the use of threats in one domain to deter activities in (an)other domain(s). Some authors define cross domain deterrence exclusively in the military domains land, sea, air, cyber and space albeit at different levels of abstraction. James Scouras, Edward Smyth and Thomas Mahnken assert for example that it is the prospect of retaliation from one domain to another which constitutes the essence of CDD.[12] It is worth noting that the authors seem to focus exclusively on deterrence by punishment rather than denial. James Dawkins emphasizes that CDD involves the use of specific weapons rather than mere threats or retaliation in general. His conceptualization includes both punishment and denial strategies and draws attention to the actual instruments by which deterrent effects are to be achieved.[13] Despite the differences in abstraction, these authors understand CDD to operate specifically within the military domains.

Other authors also consider non-military domains and instruments. Accordingly, Manzo Vince understands CDD to refer to deterrent efforts on land, at sea, in the air, in space, in cyberspace and through economic sanctions as well as other non-violent instruments.[14] King Mallory, too, includes both non-military instruments and non-military domains, arguing that CDD is about preventing escalation in any domain and across them.[15] Sean Monaghan, Patrick Cullen and Njord Wegge assert that contemporary deterrence strategies should include an array of non-military means to detect, deter and respond in a tailored way.[16] More generically, Erik Gartzke and Jon R. Lindsay conceive of CDD as "the use of threats of one type, or some combination of different types, to dissuade a target from taking actions of another type to attempt to change the status quo".[17]

[12]Scouras et al. 2017.

[13]Dawkins 2009, p. 12.

[14]Vince 2015, p. 3.

[15]Mallory 2018, pp. 7–12. Vertical escalation, in the crisis escalation management literature, refers to escalating the intensity of force within one specific domain. Horizontal escalation refers to the expansion of escalation in other geographical domains, but can also describe escalation to non-traditional domains. For the original work, see Kahn 1965. For more recent elaborations on the concepts, see Morgan et al. 2008; Sweijs et al. 2016.

[16]Cullen and Wegge 2019.

[17]Lindsay and Gartzke 2019a, p. 4.

8.3 The CDD Literature: Practical Innovation Versus Theoretical Reconceptualisation

8.3.1 Innovation in Practical Application

Over the past decade or so, two approaches to CDD have emerged. The first approach emphasises that CDD requires merely the extension and refinement of the practical application of general deterrence theory. Authors within this approach argue that deterrence has always been cross domain in nature, albeit only in the context of traditional military domains.[18] Despite the emergence of new domains, deterrence in today's world is as such not different, so they argue.[19] Accordingly, Christopher Buckley asserts that cross domain deterrence has been practiced in the West for a very long time simply because "deterrence policy and strategy are concepts too big to be constrained in a single domain."[20] Still, it is acknowledged that particular aspects of deterrence in practice are in need of refinement. Gartzke and Lindsay, for example, observe that the "increasing complexity in the entire portfolio of means now available now appears to necessitate the refinement of deterrence as both a military and political process."[21] But what does refinement precisely entail for CDD to be effective? The authors in the refinement camp tend to focus on practical problems associated with the necessary conditions for effective CDD. Important requirements of deterrence in general that they focus on include attribution, threat credibility and proportionality, signalling and escalation management.[22] Attribution depends on the ability and the willingness to ascribe responsibility for a particular act to an actor. Without the possibility of attribution, transgressors can act undetected and therefore escape allocation of blame. Credibility is rooted in the perceived capability and willingness to act. It is crucial for deterrence to work because adversaries have to believe they will suffer negative consequences for their wrongdoings. Threats that are not credible are irrelevant for deterrence purposes. In general, threats which are proportional to their triggers are likely to be perceived more credible than disproportionate ones. Signalling refers to the process of communicating one's willingness and capabilities to act to instil that belief in the adversary. Attribution, credibility, threat proportionality and signalling together are prerequisites for escalation management, which is the regulation of the

[18]Mallory 2018, p. 6.

[19]Denning 2015.

[20]Buckley 2018.

[21]Lindsay and Gartzke 2016, p. 24. The quote is taken from the original draft of the chapter but it did not make it into the final version of the volume.

[22]George and Smoke 1974, p. 64; Long 2008, pp. 7–8.

intensity and scope of the conflict.[23] These four themes are given elaborate treatment in the CDD literature in the context of today's challenges.[24]

8.3.2 Attribution

CDD authors point out that the emergence of new domains and the proliferation of hostile actors complicates attribution in the cross-domain context. Both state and non-state actors can dispose of a range of military and non-military instruments to cause damage from afar. Geographic proximity is no longer required. Proxy wars have become increasingly salient, in the context of a steep increase in internationalized intrastate conflicts.[25] The democratization of the means of violence in combination with the foggy nature of new domains, especially cyber space, are singled out as formidable challenges to attribution in the cross domain context.[26] Special Forces and irregular combatants without uniforms, both of which are hard to identify, constitute key actors of choice to carry out contemporary military operations.[27] Low cost unmanned aerial vehicles enable conflict actors, including non-state actors such as ISIS in Iraq and Syria and the Houthis in Yemen, to target objects of value from a safe distance.[28] Individual grey zone events "are difficult to distinguish from one-off actions, statecraft, or diplomacy".[29] In the virtual realm, offenders can avoid attribution by hiding behind the anonymity provided by cyber space.[30] Though cyber attribution is possible in general, it is seldom certain in particular cases.[31] Perpetrators can exploit the complexity of cyberspace to pretend they act on behalf of a third party.[32] Furthermore, collecting sufficient evidence about the origins of cyber-attacks may take months.[33] By that time, too much time has passed for an effective response to effectuate deterrence.[34] Attribution in space brings its own set of challenges. The devices that scan the environment, those which keep track of space systems' health as well as those which identify the

[23]Morgan et al. 2008, p. 8.
[24]And in practical tabletop exercises, such as Wuest 2018.
[25]Innes 2012.
[26]Lehman 2019, p. 78.
[27]Cormac and Aldrich 2018, p. 479.
[28]Sayler 2015.
[29]Sheppard and Conklin 2019, p. 1.
[30]Nye 2017, pp. 49–52; Kello 2017, pp. 198–200.
[31]Klimburg 2017.
[32]Andres 2017, p. 94.
[33]Brantly 2018a, pp. 41, 45.
[34]Schneider 2019, pp. 105–6; Jackson 2019, p. 114.

origins of the hostile activities, have many blind spots.[35] Additionally, actors in possession of space assets will likely only know they have been attacked because of the effects of the attack. Also, space weather can produce damage akin to the adversarial action.[36] The origins of the attack and the identity of the perpetrator are therefore hard to pin down. The widespread use of non-military measures adds another layer of complexity to the attribution challenge. The different actors taking part in election meddling, disinformation campaigns, espionage, intelligence theft, critical infrastructure infiltration, political corruption or market stock manipulation may be hard to identify in acceptable time frames, or at all.[37] Overall, recent technological progress combined with the proliferation of actors and domains complicates attribution in both military and non-military domains and across them.

Yet, CDD scholars come up with various solutions to these obstacles to attribution which are first and foremost practical and technical rather than theoretical in nature. In general, the scholars acknowledge that the solutions to the attribution challenge across domains require international and inter-organizational cooperation, information sharing, technical expertise, analytical skills as well as political will. To deal with the hard-to-identify non-state actors and the wide spectrum of instruments at their disposal, it is suggested to attribute and threaten those upon whose help the non-state actors may be dependent. The assumption here is that these supporting actors are often states, which should render attribution easier.[38] In cyberspace, solutions are sought in the combination of technical, cognitive and behavioural expertise to help lift the fog of anonymity and enable effective responses.[39] It is argued that cross triangulation of the digital footprint, geographical origin, modus operandi, as well as geopolitical intent, renders attribution in cyber space in fact possible in the fast majority of cases.[40] Adversarial interest is also singled out as being particularly relevant in the attribution process.[41] Additionally, cyber-attacks intended to cause serious damage are more likely than not to be accompanied by non-cyber measures, which should also help identify the potential perpetrator.[42] Lack of political will may be a bigger obstacle than technical limitations. It is pointed out, for instance, that Obama's administration was well aware of the identity of the election meddling perpetrators in 2016 but nonetheless decided not to

[35]Suzuki 2018, p. 45.

[36]Harrison 2014, p. 117.

[37]See for example Treverton 2018.

[38]Mallory 2018, pp. 10–17.

[39]Iasiello 2014, p. 58.

[40]Valeriano and Maness 2015, p. 10. See the guide to cyber attribution specifying general indicators and examples of successful attribution by Office of the Director of National Intelligence 2018.

[41]Blagden 2020.

[42]Davis 2017, p. 80.

ascribe responsibility publicly so as to avoid further escalation.[43] It is also argued that the attribution problem can be bypassed by heavier reliance on deterrence by denial. Deterrence by denial in the cyber context can be further enhanced by military, political or economic measures to secure physical infrastructure and supply lines.[44] Attribution in the cyber domain is thus certainly more complex but authors argue that obstacles can be solved with the appropriate amount of expertise and will.

Myriad solutions to attribution problems in other domains are also proposed. In space, CDD authors focus not only on the hardening of satellite assets to bolster deterrence through denial; they also suggest the strengthening of situational awareness through monitoring capabilities that enable attribution; the assessment of geopolitical risk based on analysis of strategic intent and space capabilities; and the traditional exploitation of human intelligence sources.[45] In the terrestrial military domains, it is argued that attribution is progressively less of a problem. Attribution of actions executed by irregular forces can exploit data from social media, photos and position tracking applications.[46] Western countries were thus able to identify and attribute Russian troop movements near the Ukrainian border during the summer of 2014. Likewise, the US was able to quickly ascribe the 2019 hostile activities in the Persian Gulf to the Iranian Revolutionary Guards units.[47] North Korean missiles launches over the past decade were also time and again detected by US satellite systems.[48] Finally, attribution of actions outside these military domains can also be enhanced, it is suggested, by tracing overall patterns. Authors point out for instance that one diplomatic visit of a foreign official may not be significant, but when placed in a broader picture, and when combined with other actions, it may allow for the identification of an overall pattern of coercive activities.[49] On a more practical note, Linda Robinson et al. suggest that hybrid campaign analysis units that can expose systematic patterns and generate more holistic threat pictures, will contribute to cross domain attribution capabilities.[50] In sum, authors in the refinement strand suggest that attribution challenges can be addressed and overcome largely through the implementation of a series of practical recommendations.

[43]Healey 2018.

[44]Schneider 2019, pp. 112–113.

[45]Harrison 2014, p. 117; Kopec 2019, p. 123; Bahney et al. 2019, p. 139.

[46]Mallory 2018, p. 13.

[47]Yee et al. 2019.

[48]Wall 2019.

[49]Sheppard and Conklin 2019, p. 1.

[50]Robinson et al. 2018.

8.3.3 Threat Credibility and Proportionality

The issue of how to render deterrent threats credible in CDD is made more complicated by the inherent disproportionality of responses across domains and instruments of power.[51] In short, decision makers lack agreed-upon guidelines for proportional responses to the wide array of potential hostilities in CDD.[52] This is different from within-domain deterrence as Thomas Schelling's captured in his observation that "there is an idiom in this interaction, a tendency to keeps things in the same currency, to respond in the same language, to make the punishment fit the character of the crime."[53]

The conversion mechanism between violent and non-violent actions and their effects is seen as the biggest hurdle to threat proportionality.[54] Using violence against non-violent hostilities such as theft, espionage, infiltration or election meddling is likely to be seen as disproportionate by many. This is further exacerbated by the multitude of state and non-state actors, each of which may have different beliefs about the appropriate conversion ratio between violent and non-violent measures.[55] As one scholar puts it, "while the United States could threaten to retaliate against cyberattacks asymmetrically through economic sanctions or military threats, there is a significant chance that such actions would appear escalatory, disproportionate, or otherwise inappropriate to the American public or the international community."[56] Furthermore, actors operating through cyberspace are likely to have different degrees of tolerance for escalation risks because of their "anonymity, invulnerability, and global flexibility".[57] This exacerbates the proportionality asymmetry because it is not clear how individual actors and groups appraise the severity of cyberattacks. Moreover, retaliatory threats involving actions in cyberspace may have significant second and third order consequences. Their ultimate proportionality is thus hard to assess beforehand.[58] Additionally, propaganda, infiltration, espionage, economic sanctions and stock market manipulations tend to produce their effects slower than the implements of violence on land, on sea, in the air or in space.[59] Ultimately the conversion ratio between violent and non-violent measures is unclear because the former tend to have more direct and immediate effects while the latter tend to rely on more gradual and second order effects.

---

[51] See for instance Dawkins 2009, p. 12.
[52] Morrow 2019, pp. 187–188.
[53] Schelling 1966, pp. 146–149.
[54] Waxman 2013, pp. 111–113.
[55] Lewis 2010, pp. 2–3.
[56] Andres 2017, p. 96.
[57] Trujillo 2014, p. 49.
[58] Romanosky and Goldman 2016.
[59] Milevski 2019.

Even when it comes to conversion within single instruments of violence or against similar targets, proportionality assessments are not necessarily straightforward. For example, in space, the problem of proportionality is exacerbated by the differences in value which the individual actors tend to place on the same assets. The US is much more dependent than China on its satellites, both for military and civilian purposes. Therefore, the simple cost-benefit equation of destroying one satellite for each one destroyed by the enemy is asymmetric and therefore disproportional.[60] In fact, the costs incurred by the US are disproportionately higher.[61] It is argued that this undermines the credibility of US threats to harm space assets of states that do not rely on these systems in equal measure.[62] Finally, attacks against targets in and through new domains may cause considerable collateral damage which again further complicates proportionality assessments. For example, retaliation against space objects may cause debris which can threaten both friendly and hostile activities in outer space.[63] Alternatively, threatening terrestrial attacks in response to hostilities against satellites may be deemed disproportionate because the former may result in human casualties while the latter is likely to produce only material damage.[64] In this regard, authors point at patterns of failed deterrence when it comes to deterring less destructive hostilities.[65]

In tackling proportionality and credibility in CDD, scholars propose various solutions. In general, authors discuss strengthening cross domain deterrent postures by explicitly formulating cross domain threats in deterring domain specific actions, for instance by including conventional or even nuclear responses to enhance the credibility of threats seeking to deter attacks on critical assets in cyber space and space.[66] Some treatments suggest that a degree of proportionality can be established by focusing on the effects of specific actions rather than on the specific instruments used in this process.[67] Schneider, for example, speculates that cyber sabotage of a radar system can be countered proportionately by the electromagnetic jamming of a similar target. However, as she notes, this is likely to work better with direct, kinetic effects than with less direct, and less tangible effects. Smeets and Lin point out that states can build up credibility by regularly deploying a capability in practice. Actors with a clear track record of using particular capabilities, whether violent or not, may

[60]Lewis 2010, p. 3.
[61]Suzuki 2018, p. 46.
[62]Lambakis 2019, p. 503; Morgan 2010, p. xiii.
[63]Kopec 2019, pp. 125–126.
[64]Bahney et al. 2019, p. 140.
[65]Lewis 2013, p. 62.
[66]Lindsay 2015, p. 58.
[67]Manzo 2011, p. 7.

be able to develop sufficient reputation to offset the lack of credibility posed by the instruments themselves.[68]

CDD is seen as particularly relevant in the context of cyber deterrence. It is argued that cyber deterrence also requires a broad mix of military, diplomatic, economic and legal measures,[69] synchronised within an overall deterrence posture. To bolster credibility, "cyber deterrence needs to be a well-integrated defence component that is in tune with non-cyber policy initiatives, and to accomplish this, policymakers need to juxtapose carefully cyber deterrence means and ends to those involved in broader defence policies".[70] For the sake of credibility, cyber deterrence improvements need to be "mutually reinforcing", to have the potential to surprise the adversaries as well as to flexibly manoeuvre between both denial and punishment options. Furthermore, some argue that states are likely to consider truly destructive cyberattacks as regular acts of war, which should make threats of conventional military retaliation credible, as international law already allows such responses when the principles of necessity and proportionality are adhered to.[71]

Some scholars are also optimistic about the credibility of other non-violent measures. It is argued that election meddling too can be deterred by the threats of economic sanctions targeted against energy, banking and defence sectors.[72] Additionally, in response to serious threats posed by authoritarian governments, Western democracies can threaten to disrupt the former's protected information sphere and to leak sensitive information about the regime's misconduct to the foreign public.[73] Finally, as Jervis reminds us, it is necessary to realize that "threats need not be completely credible in order to be effective": it may be enough for threats to be probable rather than certain, no matter whether one employs violent or non-violent measures; "credibility is not an objective, nor is it a property of the person or state making the threat. Rather it is 'owned' by the target."[74] This underscores that conversion rates ultimately hinge on the perception of the beholder.

To deal with the proportionality issue as it relates to violent instruments, a generic solution that is proposed is to rely on a set of strategies to resolve the proportionality issue in different contexts. Anthony Juarez for instance lists counter-force, counter value, tit for tat, denial and ambiguity as potential options.[75] It is also argued that the supposed asymmetries in interests and values as related to space should not be overrated. For example, while some nations may not be as

[68]Smeets and Lin 2018, p. 63. Although the overall role of reputation is contested see for instance Mercer 1996; Press 2005.

[69]Wilner 2019, p. 9.

[70]Mandel 2017, p. 234.

[71]Davis 2017, p. 80.

[72]Wright 2019.

[73]Mallory 2018, p. 11.

[74]Jervis 2016, pp. 67–68.

[75]Juarez 2016, p. 6.

dependent on the satellites for their military utility, they may still value them highly for economic, cultural or prestige reasons and will therefore consider them vital assets.[76] With respect to the US it is said that it can credibly threaten retaliation against attacks aimed at its space assets everywhere precisely because its space assets are so important.[77] To deal with the disproportionality issue, it is recommended to focus on the overall effects rather than on specific instruments. In the context of space, this should involve a broad menu of "kinetic or non-kinetic attacks on adversary command, control, communication, intelligence, surveillance, and reconnaissance (C3ISR) and reconnaissance, surveillance, targeting, and attack (RSTA) assets in the land, air, and sea domains".[78] Overall, the recommendations from authors who are concerned with the effectuation of CDD in this refinement strand focus on establishing proportionality and increasing credibility through the adoption of a combination of these practical measures.

8.3.4 Signalling

Signalling in the cross-domain context is more complex for two reasons which are closely related to establishing proportionality. First, it is harder to relate signals about particular actions in one domain to anticipated reactions in another in line with Schelling's previously cited observation. Moreover, while signals relying on military instruments may resonate more than those relying on non-military instruments, they also come with higher risks of misunderstandings. For example, a signal of resolve to respond to cyberattacks by moving platforms for the launch of conventional or nuclear weapons may be easily interpreted as a preparation for hostilities rather than as an adjustment of the deterrence posture.[79] Conversely, signalling purely in cyber space may be difficult, because unlike in other domains, the relevant infrastructure of that domain is not under the exclusive control of the government.[80] Consequently, signals may get lost or be ignored by the adversaries.[81] Striking the right balance between over signalling on the one hand and under signalling on the other thus constitutes a paramount challenge to communication in the cross domain context. Second, a number of modern instruments and tactics are effective precisely because they are secret. This implies a serious trade-off for the signaller who runs the risk of losing the advantage yielded by the capability the moment it signals its possession. After all, it allows adversaries to devise effective countermeasures, which is especially pertinent in cyberspace, but

[76]Harrison 2014, p. 115.
[77]Buckley 2018.
[78]Mallory 2018, p. 10.
[79]Manzo 2015, p. 97.
[80]Rovner 2019.
[81]Iasiello 2014, p. 57; Valeriano and Maness 2015, p. 60.

also applies to hybrid operations.[82] This then raises the question of how to signal true capabilities while maintaining their utility for prospective hostilities.

CDD authors discuss an assortment of, once again, predominantly practical measures to meet these signalling challenges. For example, it is argued that the issue of tying threats across domains can be tackled by synchronized signalling at different levels of conflict. At the political level, signalling takes the form of public and private communication as well as norm development, at the strategic level it conveys the developments of doctrines about the actions and reactions, and at the tactical level it contains the actual application of particular forms of power to demonstrate resolve and capabilities.[83] The US successful orchestration of this kind of effort across different levels to signal its discontent with Chinese espionage activities during the Obama administration is a case in point.[84] To signal the relationship between different domains is thus possible but it requires the synergistic employment of communication across more levels than previously.

To tackle the issue of secrecy versus effectiveness, several suggestions are offered. One approach, which builds upon the recognition of the temporary nature of cyber capabilities noted by several scholars, may rely on building up a redundant portfolio of those capabilities, some of which can then be regularly used to demonstrate cyber capabilities.[85] The logic behind this option is that cyber weapons by their very nature are transitory—they lose their effectiveness over time because cyber vulnerabilities are exposed and patched.[86] Therefore, they can be disposed of for signalling both capability and resolve without losing their effectiveness. Other scholars suggest alternative ways that bypass the issue altogether by public advertisement of attribution technologies.[87] This way actors signal both their will and capabilities to allocate blame if necessary alongside announcement of the type of weapons and/or attacks they consider to be the most threatening. It is also argued that cyber weapons in fact possess signalling advantages compared to traditional instruments on the grounds that they can be used in a demonstration of force without starting the conflict they seek to prevent because they do not necessarily involve violent, kinetic effects.[88] That quality renders them sufficient to signal intent while avoiding escalation.[89] Additionally, states can rely on a combination of public speeches and real action to signal their cyber-capabilities. More states have been openly talking about the possession of sufficient cyber capabilities in recent

[82]Green and Long 2019, p. 206

[83]Sweijs and Zilincik 2019, p. 24.

[84]Brantly 2018a, pp. 18–19.

[85]Smeets 2017.

[86]Ablon and Bogart 2017.

[87]Lindsay 2015, p. 58.

[88]Lonsdale's argument does not go uncontested. See for example Stone 2013. Also, Lonsdale himself concedes that though non-violent in their nature, cyberattacks can produce violent consequences indirectly.

[89]Lonsdale 2018, p. 417; Schneider 2019, pp. 116–117.

years, some of whom have followed up with actions, such as Russia in Ukraine and the US in the context of its strategy of persistent engagement.[90] Some actors may be willing to signal more than others because of their strategic culture.[91] Signalling one's capabilities may even not inevitably lead to the loss of effectiveness, because not all adversaries are able or willing to patch the revealed vulnerabilities,[92] Moreover, cross domain signalling by military, political or economic measures may alleviate the problem with clandestine capabilities because conventional forces, diplomatic pressure and economic sanctions do not lose their effectiveness once exercised in an adversarial relationship.[93] CDD refinement authors thus conceive a combination of these practical measures to facilitate signalling across domains and solve the trade-off between secrecy and effectiveness.

A number of suggestions have also been presented with respect to signalling outside of the cyber domain. King Mallory observes that signalling can rely on explicit moral Manicheism through clear verbal statement that there is no middle ground or grey zone in order to persuade adversaries that any kind of hostilities, direct or indirect, will lead to retaliation.[94] Signalling of both will and capability is also possible against hybrid intrusions, especially with rapidly deployable response teams of police and Special Forces which convey to the adversary that it is not likely to achieve its interests. Other means of signalling include implicit warnings reflected in changes in postures in combination with public statements.[95] Others suggest that "acts of retorsion" including economic sanctions and diplomatic coercion/isolation are perfect signalling instruments.[96] The authors in this literature have thus come up with a broad portfolio of signalling measures across all domains.

8.3.5 Escalation Management

The combination of issues discussed in relationship to attribution, threat proportionality and signalling makes escalation management much more difficult in CDD.[97] The attribution problem injects uncertainty into the deterrence relationship because it renders unclear under which conditions the deterring actor will deem it appropriate to escalate. Challenges associated with credibility and proportionality undermine basic tenets of successful escalation management simply because of the

[90]Klimburg 2020; Geers 2015.
[91]Schneider 2019, pp. 117–118.
[92]Green and Long 2019, p. 231. Lindsay 2015, p. 58.
[93]Lindsay 2015, p. 58.
[94]Mallory 2018, pp. 10–15.
[95]Lewis 2010, p. 4.
[96]Davis 2017, p. 81.
[97]See the concluding section in "A New Look at the 21st Century Crossdomain Deterrence Initiative" 2016.

unpredictable dynamics across domains. Complexity of signalling further befuddles escalation management in practice because it is unclear whether signals are both sent and received. Accordingly, the diversity of escalation dynamics of cross domain deterrence is singled out as "a core analytic issue".[98]

An assortment of sources of instability for escalation management in CDD are discussed many of which are directly or indirectly related to issues addressed previously. First and foremost, there is no shared framework to describe and therefore manage escalation across domains.[99] Without such a framework "decision makers will have difficulty distinguishing between proportional and escalatory attacks and reprisals that cross from traditional strategic domains into these newer ones and vice versa".[100] Second, there are many sources of instability when it comes to particular measures and weapons across domains. Western superiority in conventional weapons motivates adversaries to actively seek and exploit asymmetric and diverse measures with varying kinetic and non-kinetic effects and with differing degrees of proportionality.[101] Some of the instruments and tactics operate across domains that cross potential thresholds faster than in the past.[102] In this context, the use of unmanned and semi-autonomous systems and, in the future, other AI enhanced weapon systems may be particularly destabilizing.[103] Furthermore, the nature of the cyber and space domains and the character of technologies used in these domains may generate escalation risks through first-strike instabilities.[104] This renders these domains not only inherently unstable but also implies spill over effects to other domains in CDD.[105] Consequently, the anticipated effects are sometimes difficult to gauge before their actual employment.[106] Third, proportionality perceptions of actions in particular domains vary considerably from one actor to the next.[107] For example, Russia and China tend to see the integration of military, political and economic tools in a much more holistic fashion and for this reason they are likely to appraise the conversion rate between individual domains differently. As Adamsky explains in this volume and elsewhere the Russians combine nuclear, conventional and information measures to deter continuously and across domains.[108] Dean Cheng in this volume and elsewhere, describes the Chinese understanding of deterrence to involve "political activity and

[98]Brimley 2010, p. 129.

[99]As Jervis points out, even frameworks for cyber domain escalations are rare to come by. See Jervis 2016, p. 71.

[100]Manzo 2011, p. 4.

[101]Andres 2017, p. 92; Wilner 2019, p. 9.

[102]Morgan et al. 2008, p. 168.

[103]Johnson 2020.

[104]Frear et al. 2018, p. 16.

[105]Kopec 2019, p. 125.

[106]Manzo 2015, p. 97.

[107]Manzo 2011, p. 4; Lewis 2010, p. 3.

[108]Adamsky 2015, p. 37.

psychological warfare".[109] Any combination of these three challenges may hinder attempts at successful escalation management in any particular conflict.

CDD authors once again have come up with a range of proposals how to address these issues. First and foremost, they agree that it is necessary to develop a shared framework which would encompass the expectations for escalation dynamics.[110] There are several distinct approaches to the development of a shared framework. Some scholars point to the salient function of international law. Game theorist James Morrow, for example, argues that the developments in international law can constitute a first step towards the development of such a framework. Law alleviates the uncertainties about proportionality by explicitly stating what is acceptable, what is the appropriate response as well as how these actions relate across specific domains. As a coordination mechanism, law contributes to a common understanding of proportionality. Though it is unlikely to eliminate competition, it may channel hostilities into more manageable forms.[111] In this vein, others argue that an international cyber warfare convention would improve the prospects for both deterrence by punishment and by denial "by clarifying what counts [as] an act of cyber-aggression and what level of retaliation is deemed acceptable by the international community, an ICWC would thereby enhance states' capacity to adopt and communicate an effective deterrent posture".[112] Another perspective on framework development builds upon the notion of different kinds of escalation ladders, including a "provocation framework" to elucidate thresholds in "grey-zone" competition and improve escalation management by helping "policymakers understand the value of their actions and how reciprocal and proportional responses achieve strategic effect… ".[113] Such a framework is supposed to work as an explicit "declaratory policy" to signal both commitment and expectations of proportionality.

Attempts have also been made to further develop escalation ladders to establish the logic of escalation in the context of single domains,[114] as well as in the interaction between different domains.[115]

Here, an interesting schism about whether to focus on instruments or on effects emerges. On one hand, it has been argued for cross domain frameworks to be based on the "severity of various military and non-military actions based on the full range of their anticipated effects, rather than assuming that military actions represent an escalation from non-military actions".[116] On the other hand, "cyber operations might not have the same saliency or emotional effect as conventional operations—

[109]Cheng 2017, p. 1.
[110]Manzo 2015, p. 92; Sweijs et al. 2016, p. 60.
[111]Morrow 2019, pp. 198–204.
[112]Eilstrup-Sangiovanni 2018, p. 398.
[113]Ruecking 2018, p. 15.
[114]Kopec 2019, p. 126; Szymanski 2019, p. 97.
[115]Caton 2019, pp. 28–32.
[116]Rosenberg and Tama 2019, p. 9.

even when they create the same physically destructive effects".[117] This second line of research, therefore, indicates that psychological effects vary across different instruments regardless of the physical damage these instruments cause.[118] Relatedly, it is also possible that cyber instruments are "poor tools for escalatory purposes" because of the limited cost-generation potential of offensive cyber operations".[119] This echoes the observations that actors tend to deescalate rather than escalate in the cyber domain because cyber tools enable actors to release tensions by "sub crisis management manoeuvring".[120] These practical ideas concerning the development of shared frameworks, whether alone or in some combination, thus seek to address problems associated with escalation management in CDD.

Authors working on CDD have also proposed several solutions to tackle the problems of destabilizing measures and of varying perceptions of proportionality. To deal with the former, it may be wise to avoid offensive activity with specific weapons (nuclear) and against specific targets (command and control).[121] Additionally, the vulnerable assets should be better protected. Satellites should be dispersed across broad space and have their passive and active defences improved.[122] Economic interdependence too, may have a stabilizing effect by motivating restraint in interactions. Finally, new domains tend to create mutual vulnerabilities which can incentivize prudence and caution out of fear for retaliation. Declarations of restraint as well as the developments of some basic thresholds for response are seen as time tested mechanisms.[123] This may prove particularly useful in the cyber and space domains. Other recommendations lean towards the opposite direction, with experts suggesting not to show restraint but rather to show resolve and the will to retaliate in order to establish escalation dominance up front.[124] How to combine the two contradictory approaches continues to be a pernicious problem, and requires future research and also practice to solve.[125] The ideal situation is the one in which each actor can exercise restraint but still radiate resolve.[126] These diverging recommendations imply that successful escalation management depends on the practical application in particular contexts rather than on general truths. Overall, the solutions for escalation management proposed in the refinement camp are of a predominantly practical nature. They build on, but do not

[117]Schneider 2019, p. 119.
[118]Kreps and Schneider 2019.
[119]Borghard and Lonergan 2019.
[120]Jensen and Valeriano 2019, p. 40.
[121]Manzo 2015, pp. 94–97.
[122]Harrison 2014, p. 116; MacDonald 2013, pp. 91; Morgan 2010, pp. xiv–xv.
[123]Kopec 2019, p. 126; Manzo 2015, p. 97.
[124]Jacobsen 2016, p. 7.
[125]Durkalec et al. 2018, p. 14.
[126]Frear et al. 2018.

extend, the logic of classic deterrence theory while offering a range of valuable practical insights how to effectuate CDD in today's world.

8.4 Refinement and Reinterpretation—Expansion and Reconceptualisation

The second strand in the CDD literature argues that the character of contemporary challenges requires the broadening and deepening of our understanding of deterrence. Instead of offering practical recommendations on how to effectuate CDD in light of changing strategic conditions, authors propose theoretical and conceptual additions and innovations to existing concepts of deterrence rooted in deterrence by punishment and deterrence by denial. Some authors offer additional theoretical concepts to update deterrence; other authors in effect seek to reconceptualise deterrence in light of the nature of cross-domain challenges. This stems from the recognition and conviction that new domains require new approaches. Finding incremental practical fixes simply does not suffice, so they argue. It is thought that the traditional parameters that may have allowed deterrence to work in previous times, simply no longer hold in the context of today's multipolar, connected and complex strategic environment. The greater diversity of actors that dispose of an even greater diversity of means that can successfully threaten each other in this environment either undermines deterrence or may even render it impossible.

8.4.1 Refinement of Traditional Concepts of Deterrence

Some of the additions are theoretical refinements. For instance, in order to deter across both old and new domains, concepts such as cumulative, punctuated and layered deterrence have been introduced. The concept of cumulative deterrence is based on Israel's strategic experience. Israel has defended itself against a diverse spectrum of attacks conducted by state and non-state actors over a long period of time, partly by "attacking the rival repeatedly in response to specific behaviours, over a long period of time, sometimes even disproportionally to its aggressive actions".[127] Or, as we put it in a previous publication on cross domain deterrence in the context of hybrid conflict, "cumulative deterrence conceptualises deterrence as a continuous, longer term process in which a one-off transgression does not spell failure but adversarial behaviour is shaped by the deterrer in a concerted effort."[128] Within the framework of cumulative deterrence, deterrers understand the necessity of absorbing some attacks in order to prevent others. This marks a clear departure

[127]Tor 2015, p. 112.

[128]Sweijs and Zilincik 2019, p. 23.

from a more absolutist notion encapsulated in traditional deterrence approaches aimed at deterring all attacks. The concept of cumulative deterrence may indeed be better suited to the less impactful but more frequent and ambiguous amalgamation of contemporary security threats and actors rather than to deterring the threat of a nuclear attack.[129] Another alternative is punctuated deterrence, which conveys punishment to address a series of actions and cumulative effects. The difference between cumulative and punctuated deterrence is that within the framework of cumulative deterrence, deterrers respond continuously over long time periods to single attacks, while in the case of punctuated deterrence they respond gradually over time and in a punctuated manner.[130] In the context of space deterrence, some authors have come up with the notion of layered deterrence, which includes a simultaneous combination of international norms, entanglement, retaliation, and denial of benefit which can be conducted across domains.[131]

8.4.2 Reinterpretation of Deterrence by Denial

In trying to come to terms with the nature of today's strategic challenges, authors have also sought to expand on traditional concepts of deterrence by denial and punishment, even trying to merge the two into one mechanism. Recent years have seen the introduction of notions such as offensive denial and resilient denial, punishment through stigmatization, and entanglement, as well as the substitution of dissuasion for deterrence. With respect to deterrence by denial authors have introduced the distinction between tactical and strategic denial.[132] Tactical denial refers to denying the adversary the prospect of attaining the direct impact of a particular hostile action, while strategic denial refers to denying it the political benefits that it expects to derive. While the former still aligns with traditional conceptions of deterrence by denial, the latter constitutes a significant broadening of the concept. Yet also tactical denial has been significantly expanded, most importantly by including offensive pre-emptive action. Traditional deterrence theoreticians assumed that denial is inherently tied to defensive measures, whether active or passive ones. The complexity and the opportunities presented by today's strategic landscape domains have led them to theorise ways in which offensive action can be used to deny the adversaries the means to conduct offensive action. This, again, is discussed most often in relation to the cyber domain.[133] It is also observable in strategic practice, as the US has started to pursue its persistent engagement, which is it seeks to "defend forward" by preventively denying the

[129]Rid 2012, p. 125.
[130]Kello 2017, pp. 208–209.
[131]Harrison et al. 2009, pp. 17–26.
[132]Kroenig and Pavel 2012.
[133]Sharma 2010.

adversaries their means for the conduct of hostile operations.[134] The underlying logic, however, as such holds for every other domain in which offensive means can degrade the adversaries' capabilities to fight before the actual hostile interaction takes place. It is possible to conceive of denial in more traditional domains as encapsulating pre-emptive or preventive strikes against adversarial military capabilities.[135] Similarly, Israel has relied on a strategy of cumulative attrition in order to deter its enemies from carrying out immediate attacks by denying them the capability to do so.[136] Besides, capabilities in other domains tend to rely on cyber measures to varying degrees hence the use of offensive denial may impact land, naval, air and space domains as well. Overall, this approach recognizes the fact that the adversaries' capabilities and their will to fight may be dependent upon each other and thus by denying the opportunity to use those capabilities is also likely to degrade their will to fight.

Where it comes to strategic denial, resilience is singled out as a key component.[137] Resilience is conceived as the ability to absorb the direct impact of the hostile activity in question without suffering any long-lasting impact. While originally proposed in the context of deterring terrorist attacks, recent scholarship proposes that resilience can be a strategic asset across multiple domains of competition and may be effective against both state and non-state actors.[138] Ultimately, strengthening resilience is envisaged as a cross domain effort because its objective is to prepare whole societies in a cross sectoral approach to withstand adversarial activities. Once attained, resilience then signals to the adversaries the futility of carrying out potential attacks by nullifying the potential benefits to be derived from a broad spectrum of hostile measures. To deal with the ever-increasing complexity of contemporary actors and domains, deterrence by denial has thus been conceptually stretched by including new approaches that include other types of effects.

8.4.3 Expansion of Deterrence by Punishment: Norms, Delegitimisation and Entanglement

Scholars have also proposed a broader gamut of measures encompassed under deterrence by punishment. The traditional concept is expanded to encompass deterrence through norms, delegitimisation and entanglement. Punishment through norms seeks to convince potential transgressors not to engage in certain behaviour

[134]Healey 2019.

[135]Wirtz 2018, p. 70.

[136]Efraim and Shamir 2014.

[137]See also Chap. 18 in this volume by Cees van Doorn and Theo Brinkel.

[138]Hartmann 2017; Hellman 2019.

by presenting them with the prospect of social costs.[139] It seeks to alter the cost calculus of those who do not abide by the positive standards of behaviour, while deterrence by taboos seeks to do the same to those who engage in hostilities that are generally seen as off-limits. Breaking any of these two standards risks incurring not only a domestic backlash but also the loss of international prestige and ostracisation which is detrimental to vital interests of both state and non-state actors. Deterrence by association expands on that logic. It constitutes "a political mechanism in order to 'call-out' poor behaviour and strongly condemn such actions publicly, by those with the right authority, because it acts as a clear signal to others in the community of actors what is right and wrong behaviour".[140] This extended version of deterrence by punishment is increasingly being discussed in the context of deterrence in new domains and in relation to both state and non-state actors but is equally applicable to any other domain.[141]

A second alternative strategy, delegitimisation, is loosely based on the logic of punishment as it aims "to raise the costs of participating in terrorism by challenging the normative, religious, and socio-political rationales individuals rely upon when participating in violence".[142] Authors in this strand also argue that this approach allows for the classification of both particular instruments and particular targets as unacceptable. The traditional deterrence literature also addressed this, but it may be even more relevant in the cross-domain context, because the new context makes it possible to channel the conflict into more manageable domains. In some cases, such as with nuclear threats, the focus on the stigmatisation of particular weapons may be more effective. For instance, the stigmatisation of biological, chemical and nuclear weapons which has developed gradually during the last century, was closely connected to the destructive nature of these weapons.[143] This logic may be applicable to space deterrence too if it is accepted "that encouraging behavioural norms regarding the peaceful use of space—and thereby increasing the political stigma of using weapons in space—is desirable…" because "even relatively weak political stigmas can deter attacks in space for players with something to lose."[144] It is plausible, for example, that attacks against satellites should be discouraged by the development of an appropriate normative framework.[145] In other cases, such as the cyber domain, targets rather than instruments may warrant more attention.[146] Deterrence through norms may thus adhere to the original logic of deterrence by violent punishment but certainly stretches its scope. It relies on a broader concept of

[139]Ryan 2017.
[140]Ryan 2017, p. 335.
[141]Nye 2017, p. 62.
[142]Wilner 2011, p. 27.
[143]Shamai 2020.
[144]Triezenberg 2017, p. 2.
[145]Lewis 2013, p. 79.
[146]Nye 2017, p. 61.

punishment by including the social and psychological costs in order to deter actions from engaging in certain behaviour.

A third way in which traditional concepts of punishment are stretched revolves around entanglement.[147] Entanglement relies on fostering interdependence between actors and contributes to deterrence success by shaping the cost calculus of potential adversaries, as suggested by Joseph Nye. The assumption is that actors entangled in mutually dependency relationships will refrain from launching attacks because they themselves will incur costs too. It works by persuading potential adversaries that the continuation of the status quo is in their own interest, hence they should be reluctant to launch an attack in the first place.[148] The logic of entanglement, in the cyber domain and beyond, works by "adding more factors into the deterrence cost calculus— economic, political and diplomatic, for instance— then an adversary can be entangled…since they would have to suffer the consequences in other areas of their relations."[149] Essentially, entanglement operates by "mutual establishment and recognition as well as perception management of benefits both in the present and over time".[150] Or, to put it another way, entanglement works by persuading the relevant actors that they are "stakeholders in cyberspace" which should motivate them to exercise restraint in offensive behaviour.[151] Due to their mutual interdependence, this kind of deterrence is most often discussed in the context of the overall Sino-American relationship.[152] But that logic may also apply to the space domain because attacks against commercial satellites can impede international trade and finance.[153] Deterrence through norms and deterrence through entanglement are thus seen as necessary expansions in today's globally connected world. The theoretical innovations offered expand the scope of deterrence by taking a more holistic view of the overall incentive structure of potential targets of deterrence and including less tangible factors such as identity and social belief systems into consideration as well as non-military dimensions to affect the cost-benefit calculus of potential adversaries.

8.4.4 From Deterrence to Dissuasion

Finally, authors argue that deterrence of contemporary threats requires expanding classical concepts of deterrence not just in terms of the ways and means but also in its very nature. Taking stock of the theoretical additions and innovations to address

[147]Brantly 2018a.
[148]Nye 2017, p. 58.
[149]Ryan 2017, pp. 336–337.
[150]Brantly 2018b.
[151]Jasper 2015, p. 67.
[152]Pontbriand 2019.
[153]Rao et al. 2017, p. 55.

today's challenges, they argue that our common understanding of deterrence needs to be reconceptualised or rather that fundamental features that were mentioned in the classic deterrence literature require much greater emphasis. They argue that deterrence will have to focus both on persuasion and dissuasion and include both positive and negative incentives in order to prevent adversaries from engaging in undesired behaviour. Dissuasion, for example, can be seen within a broader approach to deterrence as a form that includes both threats and inducements but also "reassurances and benefits that make a world without aggression more attractive".[154] The advantage of dissuasion is that it can be pursued "through international institutions, treaties, economic sanctions, raising reputation costs, soft balancing, and diplomatic engagement".[155] Dissuasion, a subset of what can be termed "compliance seeking efforts", is supposed to include not only negative but also positive measures and it can work both by increasing the attractiveness of particular options and by decreasing the desirability of others.[156] While these ruminations may seem to be a classic case of concept creep, it is worth noting that they can also be considered a rediscovery of insights already coined by classical deterrence theorists. After all, in the early 1960s Glenn Snyder defined deterrence as "the power to dissuade" which is done by "the implicit or explicit threat of applying some sanction if the forbidden act is performed, or by the promise of a reward if the act is not performed" so that it constitutes "a process of influencing the enemy's intentions, whatever the circumstances".[157]

8.5 Conclusion

Strategic concepts emerge in particular strategic contexts to deal with specific challenges in a given period. Some strategic concepts wither away once the strategic environment evolves, others persist but are adapted. Our review of the CDD literature finds a thriving scholarly and professional debate about the use and utility of deterrence in the context of today's cross domain challenges. Our review reveals significant continuities but also significant changes in the insights offered by the CDD literature compared to the preceding waves in the deterrence literature. Deterrence has been cross domain in character since its early beginnings, prompting some to pose the question whether CDD is nothing more than old wine being served in new bottles. Accordingly, Gartzke and Lindsay start their 2019 edited volume by asking "whether CDD provides any additional analytical traction beyond classical notions of deterrence…" because "deterrence in practice has always dealt with …different military services with different nuclear, conventional, and

[154]Mazarr 2018, p. 5; see also Nye 2017.
[155]Paul 2018, p. 35.
[156]De Spiegeleire et al. 2020.
[157]Snyder 1961, pp. 106–107.

unconventional weapons, together with various diplomatic, economic, and cultural instruments of national power."[158] The continuities with traditional deterrence literature are indeed considerable: traditional concepts of deterrence by punishment and denial are still part and parcel of the strategic lexicon; the literature keeps returning to favouring conditions of successful deterrence including the communication of credible threats of cost imposition which is rooted in robust capabilities and will. At the same time, there is certainly no stasis in the CDD literature. As demonstrated in the review offered in this chapter, significant developments can be found both in terms of practical application and theoretical innovation. This speaks to the idea that CDD is more than just old wine being served in new bottles. Overall, our review warrants three main conclusions.

First, authors have spent considerable effort on the practical application of key tenets of traditional deterrence theory in the context of contemporary strategic challenges. This has resulted in an assortment of innovative ideas predominantly focused on practical measures and opportunities to deal with challenges related to attribution, threat credibility and proportionality, signalling and escalation management.

Second, authors have also come up with a number of theoretical advancements. In addressing today's strategic challenges, they have refined and expanded on traditional concepts of deterrence by stressing that successful deterrence should be envisaged as a continuous process, by usefully differentiating in deterrence by denial between tactical and strategic impacts, by adding resilience to the other side of the denial coin; by incorporating social costs in the deterrence by punishment equation; and by complementing the traditional dominant focus on negative payoff structures with attention to the role played by positive incentive structures.

Third, in light of these refinements and expansions of the concept deterrence, the question is warranted whether this enlightened notion of deterrence is still in fact about the act of *deterring* an opponent or whether it in effect constitutes a reconceptualisation of the essence of deterrence by making it about *dissuading* but also *persuading* instead of *deterring*. After all, this expanded concept of dissuasion implies a more diverse range of instruments, both military and non-military, which can be used both as a stick and a carrot, both to compel and to deter, both to persuade and to dissuade, which brings it back to the broader coercive diplomacy literature from which it originally emerged.

Our own assessment finally is that dissuasion, rather than being akin to deterrence, is more fitting as an overarching concept which encompasses the various means and ways by which one can dissuade the adversary to abstain from the action.[159] As such it includes both positive inducements and negative threats. Dissuasion can thus work as an umbrella term for deterrence by denial and punishment, norms, entanglement, resilience and assurance. Given the salience of the

[158]Lindsay and Gartzke 2019a, pp. 3–4. They eventually find CDD to be more than just old wine because it emphasises the importance of means much more than was customary in the traditional deterrence writings. See Lindsay and Gartzke 2019b, pp. 335–340.

[159]We would like to thank Stephan De Spiegeleire for his contribution to the development of this idea and for extended discussions on this topic. See also De Spiegeleire et al. 2020.

hostilities conducted below the legal thresholds of international law as well as the inability or reluctance of states to respond to varied intrusion across all domains. This broader concept of dissuasion may be more appropriate in the context of the strategic challenges in today's world.

References

Ablon L, Bogart A (2017) Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits. RAND Corporation, Santa Monica

Adamsky D (2015) Cross-Domain Coercion: The Current Russian Art of Strategy. Security Studies Center, Paris

Andres R (2017) Cyber Grey Space Deterrence. PRISM 7:91–98

Bahney B W, Pearl J, Markey M (2019) Antisatellite Weapons and the Growing Instability of Deterrence. In: Lindsay J R, Gartzke E A (eds) Cross-Domain Deterrence: Strategy in an Era. Oxford University Press, Oxford, 121–143

Black J (2018) Combined Operations: A Global History of Amphibious and Airborne Warfare. Rowman and Littlefield, London

Blagden D (2020) Deterring Cyber Coercion: The Exaggerated Problem of Attribution. Survival 62:131–148

Borghard E D, Lonergan SW (2019) Cyber Operations as Imperfect Tools of Escalation. Strategic Studies Quarterly 13:122–145

Brantly A (2018a) Back to Reality: Cross Domain Deterrence and Cyberspace. Virginia Tech, Boston

Brantly A (2018b) Conceptualizing Cyber Deterrence by Entanglement. Social Science Research Network, Rochester, NY

Brimley S (2010) Promoting Security in Common Domains. The Washington Quarterly 33:119–132

Buckley C H (2018) Building 'Space' into Multi-Domain Deterrence Strategy. http://www.airpowerstrategy.com/2018/12/01/space-deterrence/. Accessed 30 May 2020

Caton J L (2019) The Army Role in Achieving Deterrence in Cyberspace. Strategic Studies Institute, Carlisle

Cheng D (2017) Evolving Chinese Thinking About Deterrence: The Nuclear Dimension. The Heritage Foundation, Washington

Cioffi-Revilla C (1999) Origins and Age of Deterrence: Comparative Research on Old World and New World Systems. Cross-Cultural Research 33:239–264

Cormac R, Aldrich R (2018) Grey Is the New Black: Covert Action and Implausible Deniability. International Affairs 94:477–494

Cullen P, Wegge N (2019) Countering Hybrid Warfare. Development, Concepts and Doctrine Centre, Shrivenham

Davis J E (2017) Remarks by Jonathan E. Davis. Proceedings of the ASIL Annual Meeting 110:78–81

Dawkins JC (2009) Rising Dragon: Deterring China in 2035. Defense Technical Information Center, Fort Belvoir, VA

De Spiegeleire S, Holynska K, Batoh Y, Sweijs T (2020) Reimagining Deterrence: Towards Strategic (Dis)Suasion Design. The Hague Centre for Strategic Studies, The Hague

Denning D E (2015) Rethinking the Cyber Domain and Deterrence. Joint Force Quarterly 7:8–15

Durkalec J, Paige G, Shykov O (2018) 5th Annual LLNL Deterrence Workshop Multi-Domain Strategic Competition: Rewards and Risks. Lawrence Livermore National Laboratory, Livermore

Efraim I, Shamir E (2014) Mowing the Grass: Israel's Strategy for Protracted Intractable Conflict. Journal of Strategic Studies 37:65–90
Eilstrup-Sangiovanni M (2018) Why the World Needs an International Cyberwar Convention. Philosophy and Technology 31:379–407
Frear T, Kulesza L, Raynova D (2018) Russia and NATO: How to Overcome Deterrence Instability? https://www.europeanleadershipnetwork.org/report/russia-and-nato-how-to-overcome-deterrence-instability/. Accessed 30 May 2020
Fridman O (2018) Russian 'Hybrid Warfare': Resurgence and Politicization. Oxford University Press, Oxford
Geers K (2015) Cyber War in Perspective: Russian Aggression against Ukraine. NATO CCD COE, Tallinn
George A, Smoke R (1974) Deterrence in American Foreign Policy. Columbia University Press, New York
Green BR, Long AG (2019) Signalling with Secrets: Evidence on Soviet Perception and Counterforce Developments in the Late Cold War. In: Lindsay JR, Gartzke EA (eds) Cross-Domain Deterrence: Strategy in an Era of Complexity. Oxford University Press, Oxford, 205–233
Harrison R (2014) The Role of Space in Deterrence. In: Schrogl K-U et al. (eds) Handbook of Space Security. Springer, Prague, 113–130
Harrison R, Jackson D, Shackelford C (2009) Space Deterrence: The Delicate Balance of Risk. Space and Defense 3: 1-30
Hartmann U (2017) The Evolution of the Hybrid Threat, and Resilience as a Countermeasure. Center for Security Studies, Zurich
Hayes R E, Alberts DS (2003) Power to the Edge: Command and Control in the Information Age. Department of Defense, Washington
Healey J (2018) Not the Cyber Deterrence the United States Wants. https://www.cfr.org/blog/not-cyber-deterrence-united-states-wants. Accessed 30 May 2020
Healey J (2019) The Implications of Persistent (and Permanent) Engagement in Cyberspace Journal of Cybersecurity. Journal of Cybersecurity 5:1–15
Hellman A (2019) How Has European Geostrategic Thinking towards Russia Shifted since 2014? https://www.europeanleadershipnetwork.org/policy-brief/how-has-european-geostrategic-thinking-towards-russia-shifted-since-2014/. Accessed 30 May 2020
Hoffman, F G (2018) Examining Complex Forms of Conflict: Grey Zone and Hybrid Challenges. PRISM 7:30–47
Iasiello E (2014) Is Cyber Deterrence an Illusory Course of Action? Journal of Strategic Security 7:54–67
Innes M A (2012) Making Sense of Proxy Wars: States, Surrogates & the Use of Force. Potomac Books, Lincoln
Jackson N J (2019) Deterrence, Resilience and Hybrid Wars: The Case of Canada and NATO. Journal of Military and Strategic Studies 19:104–25
Jacobsen E (2016) 3rd Annual Cross-Domain Deterrence Seminar: Towards Integrated Strategic Deterrence. Lawrence Livermore National Laboratory, Livermore
Jasper S (2015) Deterring Malicious Behaviour in Cyberspace. Strategic Studies Quarterly 9:60–85
Jensen B, Valeriano B (2019) What Do We Know About Cyber Escalation? Observations from Simulations and Surveys. Scowcroft Center for Strategy and Security, Washington
Jervis R (2016) Some Thoughts on Deterrence in the Cyber Era. Journal of Information Warfare 15:66–73
Johnson D E (2018) Shared Problems - The Lessons of AirLand Battle and the 31 Initiatives for Multi-Domain Battle. RAND Corporation, Santa Monica
Johnson J S (2020) Artificial Intelligence: A Threat to Strategic Stability. Strategic Studies Quarterly 14:16–39
Juarez A (2016) 2015 Cross-Domain Deterrence Seminar Summary Report. Lawrence Livermore National Laboratory, Livermore
Kahn H (1965) On Escalation: Metaphors and Scenarios. Praeger, Santa Barbara

Kello L (2017) The Virtual Weapon and International Order. Yale University Press, Yale.
Kennan G (1948) Policy Planning Staff Memorandum. http://academic.brooklyn.cuny.edu/history/johnson/65ciafounding3.htm. Accessed 30 May 2020
Klimburg A (2017) The Darkening Web: The War for Cyberspace. Penguin Books, New York
Klimburg A (2020) Mixed Signals. Survival 62:107–130
Knopf J W (2010) The Fourth Wave in Deterrence Research. Contemporary Security Policy 31:1–33
Kopec R (2019) Space Deterrence: In Search of a 'Magical Formula. Space Policy 47:121–129
Kreps S, Schneider J (2019) Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving beyond Effects-Based Logics. Journal of Cybersecurity 5:1–11
Kroenig M, Pavel B (2012) How to Deter Terrorism. The Washington Quarterly 35:21–36
Lambakis S (2019) A Guide for Thinking about Space Deterrence and China, Comparative Strategy 38:497–553
Lehman R (2019) Simplicity and Complexity in the Nth Nuclear Era. In: Lindsay JR, Gartzke EA (eds) Cross-Domain Deterrence: Strategy in an Era of Complexity. Oxford University Press, Oxford, 66-91
Lewis J A (2010) Cross-Domain Deterrence and Credible Threats. Center for Strategic and International Studies, Washington
Lewis JA (2013) Reconsidering Deterrence for Space and Cyberspace. In: Krepon M, Thompson J (eds) Anti-Satellite Weapons, Deterrence and Sino-American Space Relations. The Stimson Center, Washington, 61–80
Lindsay J R (2015) Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack. Journal of Cybersecurity 1:53–67
Lindsay J R, Gartzke E A (2016) Draft: Cross-Domain Deterrence as a Practical Problem and a Theoretical Concept. In: Lindsay JR, Gartzke EA (eds) Cross-Domain Deterrence: Strategy in an Era of Complexity. Oxford University Press, Oxford, 1–35
Lindsay J R, Gartzke E A (2019a) Introduction: Cross-Domain Deterrence, From Practice to Theory. In: Lindsay J R, Gartzke E A (eds) Cross-Domain Deterrence: Strategy in an Era of Complexity. Oxford University Press, Oxford, 1–26
Lindsay J R, Gartzke E A (2019b) Conclusion: The Analytic Potential of Cross-Domain Deterrence. In: Lindsay J R, Gartzke E A (eds) Cross-Domain Deterrence: Strategy in an Era of Complexity. Oxford University Press, Oxford, 335–371
Long A (2008) Deterrence – From Cold War to Long War. RAND Corporation, Santa Monica
Lonsdale D J (2018) Warfighting for Cyber Deterrence: A Strategic and Moral Imperative. Philosophy & Technology 31:409–429
Luttwak E (2002) Strategy: The Logic of War and Peace. The Belknap Press of Harvard University Press, London
MacDonald B W (2013) Deterrence and Crisis Stability in Space and Cyberspace. In: Krepon M, Thompson J (eds) Anti-Satellite Weapons, Deterrence and Sino-American Space Relations. The Stimson Center, Washington, 81–100
Mallory K (2018) New Challenges in Cross-Domain Deterrence. RAND Corporation, Santa Monica
Mandel R (2017) Optimizing Cyberdeterrence: A Comprehensive Strategy for Preventing Foreign Cyberattacks. Georgetown University Press, Washington
Manzo V (2011) Deterrence and Escalation in Cross-Domain Operations: Where Do Space and Cyberspace Fit? https://ndupress.ndu.edu/Portals/68/Documents/stratforum/SF-272.pdf. Accessed 30 May 2020
Manzo V (2015) After the First Shots Managing Escalation in Northeast Asia. Joint Force Quarterly 77:91–100
Mazarr M J (2018) Understanding Deterrence. Santa Monica, RAND Corporation
Mercer J (1996) Reputation and International Politics. Cornell University Press, Ithaca
Milevski L (2019) Grand Strategy Is Attrition. Strategic Studies Institute, Carlisle
Morgan F E (2010) Deterrence and First-Strike Stability in Space: A Preliminary Assessment. RAND Corporation, Santa Monica

Morgan F E, Mueller K P, Medeiros E S, Pollpeter K L, Cliff R (2008) Dangerous Thresholds: Managing Escalation in the 21st Century. RAND Corporation, Santa Monica
Morris LJ, Mazarr MJ, Hornung JW, Pezard S, Binnendijk A, Kepe M (2019) Gaining competitive advantage in the gray zone. RAND Corporation, Santa Monica
Morrow J D (2019) International Law and the Common Knowledge Requirements of Cross-Domain Deterrence. In: Lindsay J R, Gartzke E A (eds) Cross-Domain Deterrence: Strategy in an Era of Complexity. Oxford University Press, Oxford, 187–204
Naroll R (1974) Military Deterrence in History: A Pilot Cross-Historical Survey. State University of New York Press, Albany
Nye J S (2017) Deterrence and Dissuasion in Cyberspace. International Security 41:44–71
Office of the Director of National Intelligence (2018) A Guide to Cyber Attribution. https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf. Accessed 30 May 2020
Paul T V (2018) Reimagining Deterrence: New Security Threats and Challenges to the Deterrence Paradigm. In: Wasser et al. (eds) Comprehensive Deterrence Forum. RAND Corporation, Santa Monica, 31–36
Pontbriand K (2019) Cyber Entanglement: A Framework for the Study of U.S.–China Relations. In: Cruz T, Simoes P (eds) Proceedings of the 18th European Conference on Cyber Warfare and Security ECCWS 2019. ACPI, Coimbra, 702–709
Press D G (2005) The Credibility of Power: Assessing Threats During the 'Appeasement' Crises of the 1930s. International Security 29:136–169
Rao V R, Gopalakrishnan V, Abhijeet K, Sadeh E (2017) International Space Governance: Challenges for the Global Space Community. In: Rao V R, Gopalakrishnan V, Abhijeet K, Sadeh E (eds) Recent Developments in Space Law. Springer, Singapore, 43–59
Rid T (2012) Deterrence beyond the State: The Israeli Experience. Contemporary Security Policy 33:124-147
Robinson L, Helmus TC, Cohen RS, Alireza N, Radin A, Magnuson M, Migacheva K (2018) Modern Political Warfare: Current Practices and Possible Responses. RAND Corporation, Santa Monica
Romanosky S, Goldman Z (2016) Cyber Collateral Damage. Procedia Computer Science 95:10–17
Rosenberg E, Tama J (2019) Strengthening the Economic Arsenal: Bolstering the Deterrent and Signalling Effects of Sanctions. Center for New American Security, Washington
Rovner J (2019) Can the United States Deter Election Meddling? https://warontherocks.com/2019/11/can-the-united-states-deter-election-meddling. Accessed 30 May 2020
Ruecking D W (2018) Winning in the Grey Zone: A Provocation Framework Approach. US Naval War College, Newport
Ryan N (2017) Five Kinds of Cyber Deterrence. Philosophy & Technology 31:331–338
Sayler K (2015) A World of Proliferated Drones: A Technology Primer. Center for New American Security, Washington
Schelling T C (1966) Arms and Influence. Yale University Press, New Haven
Schneider J (2019) Deterrence in and through Cyberspace. In: Lindsay J R, Gartzke E A (eds) Cross-Domain Deterrence: Strategy in an Era of Complexity. Oxford University Press, Oxford, 95–120
Scouras J, Smyth E, Mahnken T (2017) Cross-Domain Deterrence in US–China Strategy. Johns Hopkins Applied Physics Laboratory, Laurel
Shamai P (2020) What's in a Name? Deterrence and the Stigmatisation of WMD. In: Filippidou A (ed) Deterrence: Concepts and Approaches for Current and Emerging Threats. Springer, Basel, 77–96
Sharma A (2010) Cyber Wars: A Paradigm Shift from Means to Ends. Strategic Analysis 34:62–73
Sheppard L, Conklin M (2019) Warning for the Grey Zone. Center for Strategic and International Studies, Washington
Smeets M (2017) A Matter of Time: On the Transitory Nature of Cyberweapons. Journal of Strategic Studies 41:6–32

Smeets M, Lin H S (2018) Offensive Cyber Capabilities: To What Ends? In: Minarik T, Jakschis R, Lindstrom S (eds) 10th International Conference on Cyber Conflict CyCon X: Maximising Effects. NATO CCD COE, Tallinn, 55–72
Snyder G H (1961) Deterrence and Defence: Toward a Theory of National Security. Princeton University Press, Princeton
Stoker D, Whiteside C (2020) Blurred Lines: Grey-Zone Conflict and Hybrid War—Two Failures of American Strategic Thinking. Naval War College Review 73:1–37
Stone J (2013) Cyber War Will Take Place! Journal of Strategic Studies 36:101–108
Suzuki K (2018) A Japanese Perspective on Space Deterrence and the Role of the Japan-US Alliance in Sino-US Escalation Management. In: Wright N (ed) Outer Space; Earthly Escalation? Chinese Perspectives on Space Operations and Escalation. Department of Defense, Washington, 44–48
Sweijs T, Bekkers B, De Spiegeleire S, Oosterveld W (2016) Back to the Brink: Escalation and Interstate Crisis. The Hague Centre for Strategic Studies, The Hague
Sweijs T, Zilincik S (2019) Cross Domain Deterrence and Hybrid Conflict. The Hague Centre for Strategic Studies, The Hague
Szymanski P (2019) Techniques for Great Power Space War. Strategic Studies Quarterly 13: 78–104
Tor U (2015) Cumulative Deterrence' as a New Paradigm for Cyber Deterrence. Journal of Strategic Studies 40:92–117
Treverton G F (2018) The Intelligence Challenges of Hybrid Threats: Focus on Cyber and Virtual Realm. Center for Asymmetric Threat Studies, Stockholm
Triezenberg B L (2017) Deterring Space War - An Exploratory Analysis Incorporating Prospect Theory into a Game Theoretic Model of Space Warfare. RAND Corporation, Santa Monica
Trujillo C (2014) The Limits of Cyberspace Deterrence. Joint Force Quarterly 75:44–52
University of California (2016) A New Look at the Cross-domain Deterrence Initiative https://deterrence.ucsd.edu/_files/CDDI2-Workshop-Summary-080916.pdf. Accessed 30 May 2020
Valeriano B, Maness R C (2015) Cyber War versus Cyber Realities. Oxford University Press, Oxford
Vince R J (2015) Cross-Domain Deterrence Seminar Summary Notes. Center for Global Security Research, Livermore
Wall M (2019) North Korea's Short-Range Missile Test Spotted from Space. https://www.space.com/north-korea-missile-test-satellite-photo.html. Accessed 30 May 2020
Waxman M C (2013) Self-Defensive Force Against Cyber Attacks: Legal, Strategic and Political Dimensions. International Law Studies 89:109–122
Wilner A (2011) Deterring the Undeterrable: Coercion, Denial, and Delegitimization in Counterterrorism. The Journal of Strategic Studies 34:3–37
Wilner A (2019) US Cyber Deterrence: Practice Guiding Theory. Journal of Strategic Studies 42:245–280
Wirtz J J (2018) How Does Nuclear Deterrence Differ from Conventional Deterrence? Strategic Studies Quarterly 12:58–75

Wright T (2019) Democrats Must Act Now to Deter Foreign Interference in the 2020 Election. https://www.theatlantic.com/ideas/archive/2019/10/democrats-can-stop-political-interference-2020/599329/. Accessed 30 May 2020

Wuest C (2018) Multi-Domain Deterrence Table Top Exercise Summary. Lawrence Livermore National Laboratory, Livermore

Yee V, Yonette J, Magra I (2019) Iran Says It Has Seized Another Oil Tanker in Persian Gulf. https://www.nytimes.com/2019/08/04/world/middleeast/iran-oil-tanker-persian-gulf.htm. Accessed 30 May 2020

Dr. Tim Sweijs is the Director of Research at The Hague Centre for Strategic Studies and a Research Fellow at the Netherlands Defence Academy. He is the initiator, creator and author of numerous studies, methodologies, and tools for horizon scanning, early warning, conflict analysis, national security risk assessment, and strategy and capability development. He serves as an Adviser Technology, Conflict and National Interest to the UK Government's Stabilisation Unit. Tim holds degrees in War Studies (Ph.D., M.A.), International Relations (M.sc.) and Philosophy (B.A.) from King's College, London and the University of Amsterdam.

Samuel Zilincik is a doctoral student of Security and Strategic studies at Masaryk University and a teaching assistant at the University of Defence in the Czech Republic. He also has conducted internships at the Hague Centre for Strategic Studies in the Netherlands), at the Centre for Security and Prevention in the Czech Republic, and at the Strategic Policy Institute in Slovakia.

Part II
Non-Western Concepts of Deterrence

Chapter 9
Deterrence à la Ruse: Its Uniqueness, Sources and Implications

Dmitry Adamsky

Contents

Abstract This chapter traces the evolution of Russian thinking on deterrence and makes three arguments. First, the Russian approach to deterrence differs from the Western conceptualization of this term. Deterrence *a la* Ruse is much broader than the meaning that Western experts have in mind. It stands for the use of threats to maintain the status quo, to change it, to shape the strategic environment within which the interaction occurs, to prevent escalation and to de-escalate. The term is used to describe activities towards and during military conflict, and spans all phases of war. Second, the peculiar usage of the term deterrence in the Russian expert community reflects the imprint of Russian strategic culture, and of the Russian military transformation that has been ongoing since the Soviet collapse. Finally, the unique Russian conceptualization of deterrence has implications for both practitioners and theoreticians of international security policy.

This chapter is based on Adamsky 2010, 2015, 2017a, b, 2019.

D. Adamsky (✉)
School of Government, Diplomacy and Strategy, IDC Herzliya University, Herzliya, Israel
e-mail: dadamsky@idc.ac.il

F. Osinga and T. Sweijs (eds.), *NL ARMS Netherlands Annual Review of Military Studies 2020*, NL ARMS, https://doi.org/10.1007/978-94-6265-419-8_9

Keywords deterrence · coercion · strategic culture · ideational factors · military innovations

9.1 Introduction

Since the Soviet collapse, the Russian theorizing of deterrence has been evolving through debates among various schools of strategic thought in Russia. Though frequently lacking official codification and a consistent terminological apparatus, it nonetheless has been informing Russian military theory and practice. As a result, Russian experts among themselves, and their Western colleagues, often mean different things when using the same terms and use different terms to refer to the same things. This chapter traces the evolution of Russian thinking on deterrence during the last three decades. It addresses the available corpus of knowledge that has accumulated in Russia and makes three interrelated arguments. First, the Russian approach to deterrence differs from the Western conceptualization of this term. Specifically, the interpretation of this concept in the Russian strategic lexicon is much broader than the meaning that Western experts have in mind. In a nutshell, deterrence *à la Ruse* stands for the use of threats, sometimes accompanied by limited use of force, to maintain the status quo ("to deter" in Western parlance), to change it ("to compel" in Western parlance), to shape the strategic environment within which the interaction occurs, to prevent escalation and to de-escalate. The term is used to describe signaling and activities both towards and during military conflict, and spans all phases of war. As such, the Russian interpretation of deterrence is closer to the Western conceptualization of "coercion", in its prewar and intra-war forms. Second, the peculiar usage of the term deterrence in the Russian expert community reflects the imprint of Russian strategic culture, and of the Russian military transformation that has been ongoing since the Soviet collapse. Finally, the unique Russian conceptualization of deterrence has implications for both practitioners and theoreticians of international security policy. The following sections elaborate on the above three claims.

9.2 Etymological Uniqueness and Logical Idiosyncrasy

In a nutshell, deterrence *à la Ruse* is similar to its Western analogue—it is all about the manipulation of negative incentives, threats aimed at shaping the strategic calculus, strategic choices and strategic behavior of the adversary. However, beyond that, the Russian approach exhibits dissimilarities to its Western equivalent. Three differences, etymological, logical and scope-related, loom large. This is not an issue of mistranslation, but rather concerns the implicit meanings, which underline the unique Russian terms.

First, etymologically, the English term deterrence is translated to Russian as *sderzhivanie*. This Russian word relates to an effort to hold, to restrain, or to contain someone or something that is in motion, or about to erupt, such as emotions, tears, horses, pressure, or aggression, to keep it from happening. In contrast to the English root *terror*, it does not derive from the word fear, although it does imply the threat of making a particular choice of the adversary not worthwhile in the cost-benefit terms operating in the mind of the other side. The Russian word *ustrashenie*, intimidation, which derives from the root *fear* (*strakh*), is the closest approximation to *terror* in English, but has been used more seldom, as compared to *sderzhivanie*. During the Cold War, when the Soviet strategic community followed the Western discourse on deterrence, the word intimidation, *ustrashenie*, was almost by default employed to describe how the collective West was trying to coerce the USSR by using military threats. In keeping with tradition, in the current Russian discourse, intimidation is used more often than not either along the same lines or in order to translate one of the two deterrence strategies—*deterrence by punishment* (*sderzhivanie ustrasheniem*).[1] Contemporary Russian experts very seldom use this term to describe Russian actions, as within the Russian mental-cultural context intimidation has a negative connotation of a forceful, offensive and aggressive act. Not for propaganda purposes but following their natural instincts, Russian experts dealing with deterrence theory define Moscow as operating from a position of defense and "counter-coercion" (*kontrsderzhivanie*),[2] which makes the usage of the term *intimidation* inappropriate.[3]

Second, in terms of its internal logic and rationale, the interpretation of this concept in the Russian strategic lexicon is much broader than the meaning that Western experts have in mind. Deterrence *à la Ruse* stands for the use of threats, sometimes accompanied by limited use of force, to preserve the status quo ("to deter" in Western parlance), to change it ("to compel" in Western parlance), to shape the strategic environment within which the interaction occurs, to prevent escalation and to de-escalate during actual fighting. In Western usage, the term 'deterrence' implies a more reactive modus operandi, while the term 'compellence' has a more proactive connotation. The Russian discourse uses the term deterrence to refer to both, although there is a clear line between them in the Western lexicon and terminology. There is no established term for coercion, as an umbrella term for both deterrence and compellence. The Russian discourse often utilizes the term deterrence but rarely the term compellence to express a concept similar to the Western term coercion. The context usually indicates which of the forms of influence the authors are referring to. The common denominator is that it is about an effort to

[1]Pechatnov 2010.

[2]Sterlin et al. 2019; Ponomarev et al. 2019.

[3]In a way, this resonates with the original George's definition of coercive diplomacy which tried to make the case for the analytical distinction between coercive diplomacy for offensive purposes (blackmail) and defensive purposes (coercive diplomacy). The author would like to thank Tim Sweys for sharing this observation.

impose your strategic will on the other side by activities below the threshold of major military activity or the use of brute force.[4]

Finally, in terms of the scope and place of this effort within strategic interaction, the term is used to describe signaling and activities both towards and during military conflict, and it spans all phases of war. Thus, to use the terminology of Western strategic studies in order to categorize deterrence à la Ruse, this term in Russian parlance encapsulates several types of deterrence at once: not only to prevent hostilities (broad deterrence), but also to prevent specific moves within the hostilities (narrow deterrence).[5] As such, the Russian interpretation of deterrence is closer to the Western conceptualization of "coercion" in its prewar and intra-war forms.

9.3 The Russian Approach to Deterrence: Sources and Evolution of Theory

Why this uniqueness of "deterrence *à la Ruse*"? Why does it differ from the Western conceptualization? The current stage of the concept's evolution within the Russian expert community reflects the imprint of three factors: (I) the peculiar genealogy of this term in the Soviet-Russian expert community, (II) the transformation of the Russian military, mainly in the realm of threat perception and weapons modernization since the Soviet collapse; and (III) the characteristics of Russian strategic culture.

9.3.1 Imprint of Intellectual History

The intellectual history of the term in the Russian professional discourse is about five decades shorter than in the West. It has been entering the Russian lexicon incrementally since the Soviet collapse. This produced a conceptual catching up dynamic, as the Soviet and then Russian expert community has been adopting certain terms from the Western, or what it calls Anglo-Saxon, strategic lexicon, but giving them, in the words of Russian experts themselves, a Russian cultural reading and interpretation.[6] As a result, we find not only a conceptual mishmash and less terminological synchronization within the expert community than in the West, but also unique Russian strategic terms and meanings which are expressed today in Western terms, although essentially they mean somewhat different things.

[4]Adamsky 2017a, b.

[5]For example: Paul et al. 2009.

[6]Sterlin et al. 2019; Ponomarev et al. 2019; Pechatnov 2010.

During the 1990s, against the backdrop of acute conventional military inferiority vis-à-vis the West, the Russian political leadership changed the role of the tactical nuclear arsenal from fighting a war to supporting deterrence. This paradigm shift threw the Russian strategic discipline into a state of "knowledge crisis". Russian military experts realized that the nuclear arsenal had been assigned a new role, but lacked a theory for turning limited nuclear use into an extension of politics. Confused, they qualified their state of knowledge as "the first steps in conceptualization of the newly emerging problem",[7] as they lacked an indigenous Soviet corpus of knowledge to lean upon when the need arose to de-escalate a conventional regional conflict by means of nuclear coercion. To fill this conceptual deficit, they looked to the West, but back then the Western body of deterrence thought was *terra incognita* for Russian strategic studies, still a brainchild of the Soviet epoch. The Soviet corpus of military thought offered poor guidance on deterrence theory and limited nuclear use, since it thoroughly rejected both upfront. Although Moscow and Washington had a relatively similar basic view of deterrence logic, the Soviet theoreticians thought of and described deterrence differently from their U.S. counterparts.[8]

Deterrence was not a central concept in Moscow's strategic thinking due to the dichotomous Soviet attitude to nuclear war.[9] Intuitively, of course, the Soviet leadership acted along the logic of MAD (Mutual Assured Destruction) and internalized the facts of life under it. Moscow's military policy was aimed at discouraging the U.S. from initiating a nuclear strike by assuring that nuclear aggression would not remain unanswered. However, "unlike their U.S. counterparts the Soviets did not develop an elaborate doctrine of deterrence enhanced by various strategies of nuclear use, selective targeting," and escalation dominance, and did not explore the options for intermediate levels of nuclear warfare, relying instead on the threat of massive retaliation. The Soviet political-military leadership "neither embraced nor ever really accepted the possibility of fighting a limited nuclear war, or of managing a nuclear war by climbing a ladder of escalation."[10]

Operating within a different cultural and ideational system, Soviet military strategists, in contrast to their NATO counterparts, never abandoned the aim of war victory and had a coherent nuclear war fighting strategy, which did not differentiate between conventional and nuclear war.[11] Soviet strategic thought imposed a professional ban on researching the theory of "limited nuclear war".[12] The logic of

[7]Kreidin 1999; Kreidin 1998.

[8]Hines et al. 1995; Karaganov 2011; Lupovici 2010.

[9]Hines et al. 1995, pp. 1–2, 22–4, 26, 50; Arbatov and Dvorkin 2011; Payne 2001; Sinovets 2008; Nezhinskii and Chelyshev 1995.

[10]Hines et al. 1995.

[11]Heuser 1988.

[12]Kokoshin 2003a, b; Sinovets 2008, pp. 33–34. There was one exception, which however had no influence on Soviet strategic thought, see Hines et al. 1995.

flexible response was rejected upfront,[13] the notions of "escalation dominance" and "control" were rebuffed, and the view of TNW as a limited war tool was perceived as doctrinal nonsense.[14] The "bargaining" concept was disregarded as being based on false metaphysics and an invalid worldview. Suggestions along the lines of U.S. deterrence theory were considered a "monstrous heresy".[15] Soviet military theory saw fighting a regional war with tactical nuclear munitions as an operational activity that did not require a separate conceptual outline. All nuclear and conventional efforts, of all services, on all levels and in all theaters of operations, were seen as interconnected and aimed at producing victory. Obviously, this logic was very different from the one needed in the 1990s.[16]

Although the U.S. idea of nuclear weapons as a means of deterrence was acknowledged in the Soviet military doctrine, the mission of equalizing conventional capabilities that Russian nuclear weapons acquired in the late 1990s, was non-existent in the Soviet corpus of knowledge. In describing operational and strategic procedures, the doctrinal literature, of which the 1985 edition of the Soviet military encyclopedia is indicative, lacked the term *deterrence*. The Strategic Mission Missile Troops (RVSN), the title of the corps from Soviet times, was given the euphemism *sili strategicheskogo sderazhivania* (forces of strategic deterrence) only towards the late 1990s, which was doctrinally codified in official military dictionaries and encyclopedias only in the early 2000s.

9.3.2 Imprint of Strategic Practice

As elsewhere worldwide, Russian strategic theory has had a dialectical relationship with Moscow's strategic practice. As such, it has reflected no less than it has informed the evolution of threat perception and the transformation of the Russian armed forces. The development of deterrence theory in Russia since the Soviet collapse came in three interrelated waves, or stages, which reflect the contemporary history of Russian military modernization and the essence of the Russian perception of the changing nature of war. An understanding of these paradigmatic changes in Russian military thinking is essential for grasping the current wave of Russian theory and practice of coercion.

The first stage in theory development involved the recognition of nuclear deterrence. It lasted from the Soviet collapse until roughly the early 2000s, and focused on the notion of deterring potential aggression, both conventional and non-conventional, by nuclear means, both strategic and nonstrategic, in a regional conventional war. When the notion of limited nuclear war and the missions

[13]Fenenko 2011.

[14]Hines et al. 1995.

[15]Sinovets 2008, pp. 12, 40–43; Arbatov and Dvorkin 2011, pp. 17–19.

[16]Kokoshin 2003a, b, pp. 317–318.

associated with it started to appear in Russian official publications in the late 1990s-early 2000s,[17] Russian experts started to develop the requisite knowledge to inform a "regional nuclear deterrence" posture and nonstrategic nuclear weapons (NSNW) missions from scratch.[18] A wave of publications on various aspects of deterrence emerged in the late 1990s, gathering momentum towards the end of the first decade of the 2000s. Senior and mid-career General Staff and Defense Ministry officers, along with experts from government-affiliated think-tanks, were the authors.[19] In developing deterrence theory, they adapted the terminology from US strategic theory, and introduced doctrinal novelties that emulated theoretical postulates from international relations literature about limited nuclear war.[20] The topics, which may sound like Cold War déjà vu, included basic conditions for establishing a deterrence regime, the mechanism of deterrence realization, escalation dominance, signaling credibility, the role of rationality in calculating unacceptable and minimal damage, and procedures of deterrence management.[21]

The publications' overall tone was one of exploration and recommendation—introducing new theory and terminology, and establishing novel practices. For about a decade, professional periodicals debated the role of NSNW in deterring and de-escalating regional conventional aggression. This debate generated ample assumptions and terminology, which migrated from one source to another.[22] The tone of the discussion at the time was interpretative, speculative and hypothetical, and its conclusions fragmented and often mutually exclusive. The debate remained inconclusive about the theaters, missions, and types of nuclear weapons for deterring conventional aggression. The continuous call of senior Russian experts for the formulation of theory for nuclear deterrence operations demonstrates a genuine conceptual deficit and not just a lack of administrative power to translate existing theory into an actual posture.[23]

The causal mechanism underlying this approach, defined in the West as "regional nuclear deterrence" or "escalate to de-escalate" was not officially elaborated back then. However, the concept rested on the widespread premise in the Russian strategic community that "regional conventional wars would not involve values for which the adversary would tolerate the risk of even a single nuclear strike. Consequently, limited nuclear use would deter or terminate conventional hostilities,

[17]Arbatov 2010.

[18]For the first attempt, see Grin'ko and Kohan 1993.

[19]Gareev 2009.

[20]Arbatov and Dvorkin 2011.

[21]Gareev 2009, pp. 2–13; Shatokhin 2009, pp. 35–40; Modestov 2009; Protasov and Kreidin 2009; Koniakhin, and Kovalev 2009, pp. 27–31; Korobushin 2009; Muntianu and Tagirov 2011; Tagirov et al. 2009.

[22]Zagorski 2011.

[23]Sirotinin 2010; Zagorski 2011; Ruchkin 2010; Protasov and Kreidin 2009; Shushkanov and Gorbunov 2010.

without escalation to a massive nuclear exchange".[24] This was a temporary remedy, both theoretically and practically, as long as conventional military modernization was beyond Moscow's capacity. The main focus was on the nuclear dimension of deterrence, back then the only viable option in the Russian military inventory. The first variations on the non-nuclear aspects of deterrence started to appear in the discourse, but were underdeveloped. The consensus was that the military non-nuclear forms of strategic influence were beyond Russian capacity and therefore any discussion on them would be somewhat premature.[25]

In sum, during the first decade of the 21st century the publications' overall tone was one of exploration and recommendation—introducing new theory and terminology and establishing novel practices, mainly to codify the notion of escalation for the sake of de-escalation—a concept that migrated also into the operational practices of the Russian military, as annual exercises of that period demonstrated.[26] The ongoing debate produced the contours of a widely agreed theory of deterrence *à la Ruse*, which back then was essentially about the threat of nuclear escalation to prevent conventional aggression, and if deterrence should fail then to de-escalate the fighting. Still, the deterrence concept has been less coherent, monolithic, and elegant than in Western strategic studies and how many Western experts tend to represent it.

The second stage in theory development was concerned with non-nuclear deterrence. It began in the early-mid 2000s, coinciding with the conventional military modernization of the Russian armed forces, towards but mainly following the Russian operation in Georgia in 2008. The force buildup, with the focus on IT-RMA era capabilities—stand-off PGMs and C4ISR turning into the reconnaissance-strike complex—stimulated the development of deterrence theory in a wide diapason of domains from conventional to informational, both cognitive-psychological and digital-technological. As such, it reflected the growing military capabilities beyond the nuclear realm in Russia, which was rising from its geopolitical knees, modernizing its armed forces, and feeling more potent than since Soviet times, in terms of its arsenal of capabilities and repertoire of geopolitical intentions.

This period coincided with the splash of conceptual activity around the concept of hybrid warfare (HW) in the West and the compatible Russian conceptualization of the changing nature of war as new generation warfare (NGW). In essence, NGW is an amalgamation of hard and non-kinetic tools across various domains, namely the coordinated application of military, diplomatic and economic means. The ratio of nonmilitary to military measures is 4 to 1, with nonmilitary strategic competition coming under the aegis of the military. In NGW theory, regime changes brought about by externally instigated and manipulated internal protest potential is considered a type of warfare that capitalizes on indirect action, informational campaign,

[24]Adamsky 2014, pp. 91–134.

[25]Gerasimov 2013; VD 2014; Chekinov and Bogdanov 2013.

[26]Adamsky 2014.

private military organizations and the exploitation of internal protests, backed by sophisticated conventional and nuclear capabilities.[27]

Russian deterrence theory, like its Western analogue, evolved in conjunction with these developments in contemporary military-strategic thought. Theory development progressed in two main directions: the notion of "*pre-nuclear*" or *conventional* deterrence (*pred-iadernoe sderzhivanie*) and the notion of informational (cyber) deterrence,[28] in both its cognitive-psychological and digital-technological aspects. Conventional[29] or "pre-nuclear"[30] deterrence was seen as a prelude to nuclear use.[31] The concept suggests "improving credibility by increasing escalation levels, through a threat of launching long-range conventional PGMs strikes. Selective damage to the military and civilian infrastructure should signal the last warning before limited low-yield nuclear use."[32] However, given the then-slow procurement of advanced conventional munitions, experts envisioned this type of deterrence as a distant prospect and saw no non-nuclear alternative to deterring conventional aggression.[33] Believing that non-nuclear means (precision weapons, ballistic and cruise missiles) and informational (cyber) capabilities generate battlefield and deterrence effects compatible with nuclear weapons, Russian experts, more than before, emphasized deterrence as a function of non-nuclear, hard and soft instruments.

The 2014 doctrine codified ideas circulating in the Russian expert community. Non-nuclear deterrence, a complex "of foreign policy, military and nonmilitary measures aimed at preventing aggression by nonnuclear means", is the doctrine's main innovation. Within the repertoire of non-nuclear means, the doctrine refers to the use of precision conventional munitions as one of the forceful tools of strategic deterrence. Non-nuclear deterrence does not substitute for but rather complements its nuclear analogue, as part of the "forceful measures" of strategic deterrence—a system of interconnected measures of both a forceful (nuclear and non-nuclear) and non-forceful nature. This type of deterrence may include force demonstration, to prevent escalation, and even the limited use of force, as a radical measure for de-escalating hostilities.[34]

In sum, by the end of this period, and in contrast to the previous wave of conceptual activity, the discourse of the Russian experts appears to have been better

[27]Adamsky 2015, 2017a, b, 2018, 2019.

[28]Adamsky 2017a, b, pp. 46–47.

[29]Burenok and Achasov 2007; Sukhorutchenko et al. 2009; Tagirov et al. 2009.

[30]Saveliev 2009, p. 182.

[31]Varfolomeev 2011; Ruchkin 2010.

[32]Kokoshin 2009, pp. 183–186; Efimov 2006, pp. 152–155.

[33]Matvichiuk and Khriapin 2010; Bogdanov and Gorbunov 2009; Grishin and Udaltsov 2008; Korobushin 2009, pp. 14–18; Protasov and Kreidin 2009, pp. 23–26; Korobushin et al. 2009; Muntianu and Tagirov 2010, p. 69; Muntianu and Tagirov 2011, pp. 25–28.

[34]Gareev 2009.

synchronized, conceptually codified, and tightened with the actual force buildup programs, doctrine and posture.

The third and current stage of theory development has been associated with the notion of "strategic deterrence". It roughly began gathering momentum since 2014, and has involved the amalgamation of the above two endeavors into an integrated whole—the general theory of "strategic deterrence".[35] The emergence of the theory coincided with the further evolution of a cluster of ideas about the current character of war, under the rubric of NGW. Emphasizing a synthetic and systemic mixture of military and nonmilitary forms of strategic activity across several domains, and dubbed the Gerasimov doctrine by the West, strategic deterrence *à la Ruse* is about a repertoire of interrelated influence efforts across all domains in accordance with the current understanding of the nature of war in Russia. Although *strategic deterrence* is an indigenous Russian term, Western scholars offer the term *cross-domain coercion* to describe the Russian notion of a host of efforts to deter (preserve the status quo) and to compel (change the status quo) adversaries by orchestrating soft and hard instruments of power (nuclear, non-nuclear and non-military) across various domains, regionally and globally, through all stages of strategic interaction (peace, crisis, and war).[36] Apparently the term cross-domain coercion might better expresses the logic of the Russian concept of "strategic deterrence". As it features in the Russian discourse, implies also compellence, general prevention of the threat from materializing, deterrence in peacetime and the use of force during wartime to shape the battlefield by military (nuclear and non-nuclear) and non-military means. In all these cases, this is not a brute force strategy but coercion aimed at manipulating the adversary's perception and influencing its strategic behavior.

In terms of its internal logic, and in line with the earlier variations on the theme, *strategic deterrence* implies not only a demonstration of capability and resolve to use it, i.e., posture and deployments, but also the actual employment of limited force to shape the strategic behavior of the adversary, to restrain it from more aggressive moves, to halt its current course of action, to shape the strategic environment within which the interaction takes place, and also to prevent escalation or de-escalation during the actual military conflict. Thus, it spans several phases of war, and also includes efforts of strategic influence at the softest end of the continuum—such as dissuasion (*razubezhdenie*) through strategic communication (*raziasnenie pozitsii*),[37] and reflexive control efforts.

In sum, the current Russian art of deterrence is an integrated complex of non-nuclear, informational and nuclear types of influence encapsulated in a unified cross-domain program. *Strategic deterrence* harmonized the nuclear capability, without diminishing its role, with other tools of coercion, specifically within the non-nuclear and informational (cyber) domains. Statements by the political

[35]Sterlin et al. 2019; Ponomarev et al. 2019.

[36]See Adamsky 2015; Ven Bruusgaard 2016, pp. 7–26.

[37]Cite Gareev 2009.

leadership, senior military brass and doctrinal publications suggest that *strategic deterrence* is the most widely referenced umbrella term for coercion efforts. Also used are terms from the previous waves, mainly non-nuclear and conventional deterrence.[38] The debate today has become more synchronized than ever before, although there are still some incongruences and non-canonical use of terms even by officials and practitioners. This is probably because strategic deterrence is such a parsimonious umbrella term that every definition becomes possible.

9.3.3 Imprint of Strategic Culture

When the Russian style of deterrence is measured against Western strategic studies, differences in several regards stand out. However, if measured against a Russian cultural yardstick, deterrence *à la Ruse* is symptomatic of the general Russian approach to the art of strategy. The following three characteristics loom particularly large.

First, deterrence *à la Ruse* reflects a holistic approach (*kompleksnii/sistemnii podhod*) to strategy, as the Russian experts designing contemporary deterrence policy argue themselves.[39] A holistic or systemic approach stands for an all-embracing view that "grasps a big picture and describes every element of reality as being in constant interplay with others in frames of a meta-system. It views issues in different dimensions as interconnected within one generalized frame."[40] A predilection for holism is prominent throughout the Russian intellectual tradition and cognitive style in literature, religious philosophy and the sciences.[41] It has also been projected onto the culture of war, strategic style and military thought.[42] Apparently, this inclination accounts for the abovementioned broad definition of deterrence emblematic of the Russian approach, in which use of the term "deterrence" refers equally to preserving the status quo, changing the status quo, and a repertoire of intra-war coercion moves aimed at shaping the battlefield dynamic. An inclination to holism might therefore account for why the Russian discourse does not differentiate between deterrence, compellence and coercion and uses them interchangeably or under one rubric.

Second, deterrence *à la Ruse* reflects the Russian tradition of an asymmetric approach to strategy. The notion of indirect actions (*nepriamie desitvia*)—pitting your strengths against the weaknesses of the adversary—has deep, idiosyncratic roots in the Russian military tradition. The clever stratagem, operational ingenuity, addressing weaknesses and avoiding strengths—in Russian professional

[38]Sterlin et al. 2019; Ponomarev et al. 2019.

[39]Sterlin et al. 2019; Ponomarev et al. 2019.

[40]Adamsky 2017a, b.

[41]Berlin 2004; Graham 1993; Graham 1987; Gumilevskii 1953; Shapavolov 2003; Solov'ev 1988.

[42]Naveh 1997; Leitis 1951; Donnelly 1988.

terminology these are all are expressed as "military cunningness" (*voennaja hitorist'*), one of the central components of military art in the Tsarist, Soviet and Russian traditions. Military cunningness should complement, multiply or substitute for the use of force to achieve strategic results in operations.[43] Apparently, an inclination to asymmetry naturally resonates with a holistic approach to strategy, but in addition, it specifically accounts for the cross-domain modus operandi of the Russian deterrence style.

Finally, the notion of struggle (*bor'ba/protivoborstvo*), so central to the Russian style of strategy, has conditioned deterrence *à la Ruse*. Russian experts think of strategy as an uninterrupted, permanent engagement, with no division between peacetime and wartime, to be waged in the domestic and international spheres as well as on the adversary's turf. In Russian military theory, the term *struggle* has a broad meaning and refers to strategic interaction in its totality—an approach somewhat similar to the Western notion of competitive strategy in long-term competition. In terms of efforts to impose one's strategic will, the binary division between war and peace only refers to the intensity of the competition, but not its essence. Competition with the adversary is seen as protracted, occurring towards, during and following kinetic phases of interaction. The notion of struggle apparently accounts for the application of the term deterrence throughout the various stages of strategic interaction, it being used equally to refer to the prevention of a threat from materializing, deterrence in peacetime, the use of force in crisis and in wartime, and shaping the strategic environment, whether in an active or reactive mode.

9.4 Russian Approach to Deterrence: The Implications

This chapter has demonstrated that the characteristics of the Russian coercion paradigm are idiosyncratic, reflect a strong cultural imprint, and need to be analyzed within the context of Russian strategic culture. Moreover, since the Russian art of deterrence has been constantly evolving it should be understood in motion, within its intellectual history. Also, the Russian case offers an interesting illustration of a strategic community in the midst of a process of conceptual learning and conceptualizing coercion strategies—especially in an era of major military innovation and defense transformation. This is in keeping with other cases of transformation of military power in a given state, which brings with it an adjustment of deterrence models.

[43]Vorob'ev and Kiselev 2006, pp. 203–204; Lobov 2001.

The immediate implication of the uniqueness of the Russian approach relates to mirror imaging. Applying the Western terminological framework to explain Russian concepts may lead to misperceptions, if it is done without examining Russian references to each term and isolating it from the Russian ideational context, and without contrasting it with what Russians think about themselves and others. Specifically, three conceptual-operational issues outlined below might be potentially destabilizing, and as such invite separate attention.

First is the phenomenon of asymmetry in responses that emanates from the differences in strategic phobias between Russia and the collective West. Since the Kremlin is tremendously sensitive to the non-kinetic challenge of political subversion, real or imagined, it might opt for a kinetic (nuclear/conventional) response in response. It is likely to signal its capabilities and resolve in this regard. In the West, this strategic communication might appear to be groundless propaganda mixed with strategic bluff. However, if this is indeed the case, and Moscow is ready to escalate in a different domain for something that does not seem to be worthy of escalation in Western eyes, this could have a serious destabilizing potential.

Second, blurring the line between compellence and deterrence, so characteristic of the Russian style of coercion, official doctrine, theorization, and actual operational moves, blurs the line between offense and defense. This position and the strategic dynamic which it might generate is not unique to Russia's standoff with the West; as in other similar cases, it leaves significant room for subjective interpretations of the actors, producing a dynamic bordering on the classical security dilemma, and yielding the risk of, due to potential misperception and miscommunication.

Finally, it is not unlikely that contemporary Russia is cultivating the image of a faith-driven strategic actor. This utilization of religion to enhance coercion and bargaining strategies resonates with the logic driving the "madman concept" in International Relations theory and Western strategic studies. Such a stand, imagined or genuine, poses a real diagnostic challenge for the adversary. The operational challenge is how not to produce undesired escalation but at the same time craft an adequately designed strategy.

In recent years, Russian experts apparently have paid more attention than before to such issues as measuring the effectiveness of their efforts, signaling, and misperceptions. Although recent publications[44] reflect a deep and thorough exploration of the above subjects, it is unclear how cognizant Russian experts are of these peculiarities of the Russian strategic style and their possible implications for Western responses, including the possibility of crossing the culminating point of deterrence, especially under the cross-domain approach, which Russia is likely to employ.

[44]For example, see Sterlin et al. 2019, pp. 7–17; Ponomarev et al. 2019, pp. 97–99.

References

Adamsky D (2010–2019) The Culture of Military Innovation. Stanford UP (2010); Russian Nuclear Orthodoxy. Stanford UP (2019)
Adamsky D (2014) Russian Nuclear Incoherence. Journal of Strategic Studies 37.1:91–134.
Adamsky D (2015) Cross-Domain Coercion: The Current Russian Art of Strategy. IFRI, Paris
Adamsky D (2017a) From Moscow with Coercion. Journal of Strategic Studies 37.1:33-60
Adamsky D (2017b) From Israel with Deterrence, Security Studies 26.1:157-184
Arbatov A (2010) Zdravyi smysl I razoryzhenie. Rossiia v global'noi politike 4:170-180
Arbatov A, Dvorkin V (2011) Gambit or Endgame*?* Carnegie Center, Moscow
Bogdanov S A, Gorbunov V N (2009) O kharaktere vooruzhennoi bor'by'. VM 3
Berlin I (2004) The Soviet Mind. Brookings, Washington DC
Burenok V M, Achasov O B (2007) Neiadernoe sderzhivanie. VM 12
Donnelly C (1988) Red Banner. Jane's Group, London
Efimov N (2006) Politiko-Voennye Aspekty Natsional'noi Bezopsnosti Rossii. URSS, Moscow
Fenenko A (2011) Between MAD and Flexible Response. Russia in Global Affairs, 22 June 2011
Gareev M A (2009) Strategicheskoe sderzhivanie. Strategicheskaia Stabil'nost 1.46:2–13
Gerasimov V (2013) Tsennost' Nauki v Predvidinii. VPK 27 February 2013
Graham L (1987) Science, Philosophy and Human Behavior in the Soviet Union. Columbia UP, New York
Graham L (1993) Science in Russia. Cambridge UP, Cambridge
Grin'ko V L, Kohan S I (1993) Kontseptsiia sderzhivaniia: strategicheskai stabil'nsot' v sovremmenukh usloviiakh. VM 4
Grishin V P, Udaltsov S V (2008) Iadernoe sderzhi- vanie. Vestnik AVN 1
Gumilevskii L (1953) Russkie Inzhinery. Molodaia Gvardiia, Moscow
Heuser B (1988) Victory in a Nuclear War? Comparison of NATO and WTO War Aims. Contemporary European History 7.3:311–27
Hines J G, Mishulovich E M, Shull J F (1995) Soviet Intentions, 1965–1985. BMD Federal, Germantown MD
Karaganov S (2011) Preodolet' sderzhivanie. Rossiiskaia gazeta (6 April 2011)
Kokoshin A (2003a) Strategicheskoe upravlenie. ROSPEN, Moscow
Kokoshin A (2003b) Iadernye konflikty v XXI veke. Media Press
Kokoshin A (2009) Obespechenie strategicheskoi stabilnosti. URSS, Moscow
Koniakhin B A, Kovalev VI (2009) Mekhanism realizatsii strategicheskogo. Strategicheskaia Stabil'nost' 1.46:27–31
Korobushin V V (2009) Nadezhnoe strategicheskoe iadernoe sderzhivanie. Strategicheskaia Stabil'nost 46.1:14–18
Korobushin V V, Kovalev V I, Vinokurov G N (2009) Predel sokrascheniia SIaS. Vestnik AVN 28.3
Kreidin S V (1998) O problemakh global'nogo I regional'nogo sderzhivaniia. VM 5
Kreidin S V (1999) Global'noe I regional'noe sderzhivanie. VM 4
Leitis N (1951) The Operational Code of Politburo. McGraw Hill, New York
Lobov V (2001) Voennaia Khitrost. Logos, Moscow
Lupovici A (2010) The Emerging Fourth Wave of Deterrence Theory – Toward a New Research Agenda. International Studies Quarterly 54.1
Matvichiuk V V, Khriapin A L (2010) Sistema strategicheskogo sderzhivaniia. VM 1
Modestov S A (2009) Strategickeskoe sderzhivanie na teatre. Strategicheskaia Stabil'nost' 1.46
Muntianu A V, Tagirov R G (2010) Nekotorye problemnye voprosy. Strategicheskaia Stabil'nost' 53/4
Muntianu A V, Tagirov R G (2011) O nekotorukh aspektakh vlianiia globalizatsii. Strategicheskaia Stabil'nost', 54.1:25–8
Naveh S (1997) In Pursuit of Military Excellence. Routledge, London
Nezhinskii L N, Chelyshev I A (1995) O doktrinal'nykh osnovakh sovetskoi vneshnei politiki. Otechetsvennaia Istoriia 1:5–12

Paul T V, Wirtz J, Knopf J J (2009) Complex Deterrence. Chicago UP, Chicago
Payne K B (2001) The Fallacies of Cold War Deterrence and a New Direction. University of Kentucky, Lexington
Pechatnov I A (2010) Retrospektivnyi analiz evoliutzii kontsepsii sderzhivaniia. Vooruzhenie I ekonomika 9.1:11-15
Ponomarev S S, Poddubnyi V V, Polegaev V I (2019) Kriterii I pokazateli niadernogo sderzhivaniia: voennyi aspket. VM 11:97-99
Protasov A A, Kreidin S V (2009) Sistemy upravleniai voiskami. Strategicheskaia Stabil'nost' 46.1:23–6
Ruchkin V (2010) Balans interesov (28 December 2010), KZ
Saveliev A G (2009) K Novoi Redaktsii Voennoi Doktriny. URSS, Moscow
Shapavolov V F (2003) Istoki I Smysl Rossiiskoi Tsivilizatsii. Fair Press, Moscow
Shatokhin V I (2009) Iadernaia Sostavliiaiuschaia. Strategicheskaia Stabil'nsot' 1.46:35–40
Shushkanov I G, Gorbunov V N (2010) O nekotorykh aspektakh teorii I praktiki priminenia vooruzhennykh sil. VM 1:24
Sinovets P (2008) Dvulikii Ianus. Odesskii Natsional'nyi Universitet
Sirotinin ES (2010) Sderzhivanie Agressii v Kontekste Novoi Voennoi Doktriny Rossiiskoi Federatsii. VM 5
Solov'ev VS (1988) Natsional'nyi Vopros v Rossii. AST, Moscow
Sterlin A E, Protasov A A, Kreidin S V (2019) Sovremennye transfroamtsii kontseptsii I silovykh instrumentov strategicheskogo sderzhivaniia. VM 8:7-17
Sukhorutchenko V V, Zelvin A B, Sobolevskii V A (2009) Napravlenie issledovanii boevykh. VM 8
Tagirov R G, Pecahtnov I A, Burenok V M (2009) K voprosu ob opredelenii urovne. Vestnik AVN 1
Varfolomeev I (2011) Iadernaia deviatka (25 May 2011), KZ
Ven Bruusgaard K (2016) Russian Strategic Deterrence. Survival 58.4:7–26
Vorob'ev I, Kiselev V (2006) Strategiia nepriamykh desitvii. VM 9
Zagorski A (2011) Russia's Tactical Nuclear Weapons. Hamburger Beitrage

Dr. Dmitry (Dima) Adamsky Professor at the School of Government, Diplomacy and Strategy at the IDC Herzliya University, Israel. He is a visiting professor at the Faculty of Politics and Diplomacy of the Vytautas Magnus University, Lithuania. His book Russian Nuclear Orthodoxy: Religion, Politics and Strategy (Stanford University Press, 2019) won the ISA prize for the best work in the category of Religion and International Relations.

Chapter 10
An Overview of Chinese Thinking About Deterrence

Dean Cheng

Contents

Abstract All major powers undertake deterrence behaviour, as an integral part of their foreign and security policy. This includes the People's Republic of China (PRC). The PRC, however, comes from a different strategic tradition than the United States; therefore, understanding Chinese views of deterrence has become salient. This is complicated by the evolution in Chinese thinking about deterrence, as it has sought to incorporate various elements of national power.

Keywords coercion · information deterrence · space deterrence · non-military deterrence · limited deterrence

D. Cheng (✉)
Asian Studies Center, Davis Institute for National Security and Foreign Policy, The Heritage Foundation, Washington, D.C., USA
e-mail: dean.cheng@heritage.org

F. Osinga and T. Sweijs (eds.), *NL ARMS Netherlands Annual Review of Military Studies 2020*, NL ARMS, https://doi.org/10.1007/978-94-6265-419-8_10

10.1 Differing Definitions of Deterrence

The concept of deterrence, "in its most general form, … [is] simply the persuasion of one's opponent that the costs and/or risks of a given course of action he might take outweigh its benefits".[1] In this formulation, there is no presumption that deterrence as being dissuasive versus coercive. Either would be a form of deterrence. The difference between Western and Chinese thinking about deterrence, however, begins at this fundamental, conceptual level. For Western thinkers, deterrence is primarily about *dissuasion* (although there is nothing in the definition of the term that presupposes this). Thomas Schelling, for example, in his 1966 book *Arms and Influence*, defines deterrence as "the threat intended to keep an adversary from doing something".[2] This definition is echoed by other Western analysts of deterrence. John Mearsheimer, in his book *Conventional Deterrence*, notes that "deterrence, in its broadest sense, means persuading an opponent not to initiate a specific action because the perceived benefits do not justify the estimated costs and risks".[3] Schelling specifically differentiates *deterrence* from *coercion*, which he defines as "the threat intended to make an adversary do something".[4] Glenn Snyder makes the same point by noting that deterrence "is the power to *dissuade* as opposed to the power to coerce or compel".[5] Thus, Western analyses of deterrence implicitly (and even explicitly) associate deterrence with dissuasion, *and disassociate it from compellence*.[6]

The Chinese term that is most often equated with deterrence is *weishe* (威慑). The Chinese themselves translate the term as "deterrence".[7] But the attendant meanings and implications underlying the term are very different. For the Chinese, the term *weishe* embodies *both* dissuasion *and* compellence. The 2011 PLA volume on military terminology, for examples, defines a strategy of deterrence, or *weishe zhanlue*, as "a military strategy of displaying or threatening the use of armed power, in order to compel an opponent to submit".[8] This definition does not distinguish between dissuasion or compellence in the Chinese definition. Indeed, the entry notes that there are offensive deterrence strategies and defensive deterrence strategies, which would seem to represent compellence and dissuasive approaches respectively.

---

[1]George and Smoke 1974, p. 11.

[2]Schelling 1966, p. 69.

[3]Mearsheimer 1983, p. 14.

[4]Schelling 1966, p. 69.

[5]Emphasis added. Snyder 1988, p. 31.

[6]Some define coercion as encompassing deterrence and compellence. Others define compellence as encompassing deterrence and coercion. In both cases, the Western concept of deterrence primarily focuses on dissuasion. For this paper, we will use the term *compellence* to encompass the broader concept, which will include both deterrence and coercion.

[7]PLA Encyclopedia Committee 2002, p. 477.

[8]All Army Military Terminology Management Committee 2011, p. 51.

Other authoritative Chinese volumes echo this view. Generals Peng Guangqian and Yao Youzhi, in the 2005 PLA textbook *The Science of Military Strategy*, note that

> deterrence plays two basic roles: one is to dissuade the opponent from doing something through deterrence, the other is to persuade the opponent what ought to be done through deterrence, and *both* demand the opponent to submit to the deterrer's volition.[9]

Thus Peng and Yao, in essence, combine Schelling's definitions of deterrence and coercion within the Chinese term *weishe*. This combined approach also occurs in a volume authored by the PLA's National Defence University's Military Science Research Department, which attests that the purpose of deterrence is "to halt, or prevent, the other side from starting a conflict, and thus protect one's own interests from aggression. *Or, it is to shake the other side's will to resist (dikang yizhi*; 抵抗意志*), and thus seize those interests or benefits that originally would have required conflict in order to obtain them*."[10]

In the 2015 edition of *The Science of Strategy* (*zhanlue xue*; 战略学), published by the Chinese National Defence University, strategic deterrence is defined as a form of military combat whereby an adversary is coerced to "give way, compromise, or submit (*tuirang, tuoxie, huo qufu*; 退让妥协或屈服)".[11] Again, there is no distinction made between dissuasion and compellence. In essence, the available literature suggests that the Chinese do not necessarily think in terms of deterrence, as that term is employed in Western strategic literature, but in terms of *coercion*. Whether an adversary agrees to do something they would prefer *not* to do, or avoids doing something they would prefer *to* do, both fit within the Chinese term *weishe*. This term incorporates both the compellence and dissuasive aspects.

As important, Chinese decision-makers assess successful deterrence differently from their American counterparts. American discussions tend to characterize deterrence as a *goal*; in particular, there is often reference to deterring an adversary from acting in a particular domain (e.g., space, cyber). The 2010 US National Security Strategy, for example, states that the US is committed to maintaining "superior capabilities to deter and defeat adaptive enemies" and reassure friends and allies.[12] The very act of deterring one or more opponents from acting in certain domains or in certain ways is seen as serving US interests. By contrast, the Chinese view deterrence as a *means* to achieving political ends. There does not appear to be much focus on deterring or dissuading an adversary from acting in space or cyber, for example. Instead, for Chinese decision-makers, successful deterrence is ultimately a form of political activity and psychological warfare, whereby an adversary

[9]Emphasis added. Peng and Yao 2005, p. 215.

[10]Emphasis added. National Defense University Science Research Department 2004, p. 85.

[11]Xiao 2015, p. 119.

[12]Office of the President of the United States 2010, pp. 17–18.

is constrained in their actions, allowing China to achieve its goals.[13] (Although nuclear deterrence would seem to be the exception, with a general desire to avoid the use of nuclear weapons against China.) Chinese writings in turn suggest that their decision-makers will rely on more than one means in order to try and deter (and compel) an adversary. Chinese discussions of deterrence such as the various editions and versions of *Science of Strategy* and *Science of Military Strategy* consistently suggest that they will incorporate conventional, space, and information forces and actions, as well as orchestrate economic, diplomatic, and even mobilisation activities and planning, in order to force an adversary to submit. The focus is not on deterring action in one or another domain, but in securing the larger Chinese strategic objective (e.g., getting Taiwan to abandon efforts at securing independence; obtaining support for Chinese claims to the South China Sea). The act of deterrence is to help achieve a particular goal; *deterrence is not the goal itself*. As one Chinese analysis notes, the basic developmental path for Chinese deterrence is "nuclear and conventional unified; deterrence and warfighting unified; deterrence and control [of conflict] unified".[14]

Interestingly, Chinese writings suggest that there is much more attention being paid to nuclear, space, and information capabilities and their contributions to deterrence than conventional forces. In the second edition of the *PLA Encyclopedia*, released in 2007, there are several entries for different aspects of *weishe*. Not only is there an entry for the strategy of deterrence (*weishe zhanlue*; 威慑战略), but there are also entries for "nuclear deterrence (*he weishe*; 核威慑)", "space deterrence (*taikong weishe*; 太空威慑)", and "information deterrence (*xinxi weishe*; 信息威慑)".[15] Each entry includes a discussion of how deterrence in this context is viewed, not only by Chinese analysts, but foreign analysts as well. There is no entry, however, for conventional deterrence. Other Chinese writings provide additional insight into how the Chinese conceive of each of these aspects of deterrence. This paper will examine the Chinese view of these various types of deterrence individually, and what they might mean in combination.

10.2 China's Concepts of Nuclear Deterrence

Within this different Chinese perspective of deterrence, nuclear weapons occupy a particular place. The primary role of Chinese nuclear weapons is in supporting broader Chinese policies of *weishe*, in both its dissuasive and coercive aspects.[16] As Chinese leaders have noted, the mere possession of nuclear weapons compels an adversary to take them into account. Thus, as Chinese Foreign Minister Chen Yi

[13]Zhou and Wen 2004, p. 20.

[14]Academy of Military Science Military Strategy Research Office (PRC) 2013, p. 147.

[15]Editorial Committee 2007, pp. 279–284.

[16]Editorial Committee 2007, p. 4.

observed in 1962, in the midst of the "two bombs, one satellite effort," "producing atomic bombs, missiles, and supersonic aircraft would put me, the Minister of Foreign Relations, in a better position!"[17]

Nuclear deterrence is defined as the display of nuclear forces, or the threat of their employment, in order to shake and awe an adversary, or limit and constrain their military activities. It involves warning an adversary of the possible employment of nuclear weapons, either in an offensive or counter-offensive manner, and the associated destruction in order to generate psychological impacts in the target of deterrence. The expectation is that this will compel an adversary to engage in a cost-benefit analysis, and by generating fear, shake their will and cause them to abandon their goals. As the 2007 *PLA Encyclopedia* notes, successful nuclear deterrence will allow the deterring side to achieve its political or military goals.[18] According to Chinese writings, the power of nuclear weapons, coupled with their capacity for both compellence and dissuasion, means that nuclear weapons not only can deter conflict and compel adversaries, but can also serve to limit the outbreak of conflict more generally. Beginning in the 1990s, Chinese leaders noted that China's strategic deterrent forces could constrain conflicts, delay its outbreak, or limit the scale of a conflict should one nonetheless occur.[19]

According to Chinese analyses, while capabilities and will are essential elements of deterrence in peacetime, signalling one's will to employ those capabilities is vital in time of crisis.[20] Only if an adversary has no doubt that the PRC is prepared to employ its capabilities can conflict be constrained. Nuclear weapons' inherent destructiveness is a means of influencing the adversary's calculations of risk and cost, while their deployment is a concrete expression of Chinese capability. While this echoes Western concepts of deterrence, it is notable that Chinese writings explicitly note the importance of not only capability and will, but the communication of both these elements to those whom one wishes to deter. By contrast, the role of communicating capability and will is more implicit in Western writings; indeed, much of the effort in the Cold War was focused on this communications issue. It would appear that the Chinese see communications as embodying not only signalling but also credibility.

For the PRC, its approach to nuclear deterrence has focused on "limited deterrence". That is, China has sought to develop sufficient numbers of nuclear weapons to allow it to maintain a survivable second-strike force, but has not chosen to pursue a larger number typically associated with nuclear war-fighting (including counter-force targeting of an adversary's nuclear forces). China's strategic nuclear forces are mainly comprised of land-based ICBMs, and a handful of sea-based nuclear missiles. There are several dozen ICBMs, mainly the DF-31 series, and one Chinese ballistic missile submarine, whose JL-1 SLBM was comparable to the early

[17]Deng 1993, p. 60.

[18]Editorial Committee 2007, p. 282.

[19]Academy of Military Science Military Strategy Research Office (PRC) 2013, p. 142.

[20]Academy of Military Science Military Strategy Research Office (PRC) 2013, p. 174.

Polaris A2 in range. All of these are equipped with single nuclear warheads. Until 2015, the land-based missile force, both nuclear and conventional, were under the control of the Second Artillery, which was considered an "independent branch" (as opposed to a full-fledged service), with a strategic mission. A major overhaul of the People's Liberation Army at the end of 2015, however, saw the reorganization of the Second Artillery into the PLA Rocket Forces (PLARF) and its elevation to a full-fledged service. The elevation in status means that PLARF officers will be co-equal members of the staffs of each of the new war zones, alongside the ground forces, PLA Navy, PLA Air Force, and PLASSF. Indeed, a PLARF officer could, in theory, be placed in command of a war zone. The full implications of this shift are not yet clear, but it suggests that there may be a greater role for China's missile forces in any future joint campaign, both conventional and potentially nuclear. There has been some discussion of the PRC obtaining a nuclear bomber, which would give the PRC a triad such as that of the United States. It remains to be seen whether the Chinese will commit the resources necessary to build such a force.

China sees its nuclear forces as marked by several key characteristics. As noted earlier, China fields only a *limited deterrent*. This is all that necessary because, in the Chinese formulation, China adheres to a nuclear no-first use policy against states and regions that have no nuclear weapons. (This no-first use policy, however, appears to be less than absolute.) There is little indication that the PRC has engaged in either planning or acquisition to support a nuclear war-fighting strategy (including nuclear counterforce strikes against an adversary's nuclear deterrent forces). Therefore, the PRC has no requirement for a massive nuclear force. Moreover, it has a strictly "defensive" nuclear policy, where it will only use nuclear weapons in response to an adversary's aggression. Instead, within this context, the PLA's nuclear deterrent forces, the Second Artillery and its successor the PLARF, are focused on retaliatory nuclear missions. According to Chinese analyses, the PLA therefore needs to field an elite deterrent force that is credible (*ke xin*; 可信) and reliable (*ke kao*; 可靠), but does not have to be large. A credible, reliable nuclear force, coupled with the will to use it in response to an adversary's aggression, are central to China's conception of nuclear deterrence.

In order to improve its credibility, Chinese writings suggest that the PLARF will have to field a force that can weather an adversary's first strike, and possible missile defences, and still launch an effective retaliatory strike. This will entail strengthened striking power, improved survivability, and the ability to respond rapidly if and as necessary. Improvements in these areas will allow the PLARF to generate much more destructiveness should it be employed, thereby enhancing the credibility of the threat posed. Similarly, in order to enhance its reliability, the PLA is interested in improving the level of information support provided to the PLARF, including strengthening nuclear C2 capabilities, the provision of improved strategic early warning, as well as a rapid response capability.

It is important to note, however, that Chinese analyses, while not calling for nuclear counter-force targeting, do call for the ability to wage "real war (*shi zhan*; 实战)" with nuclear weapons, in addition to implementing deterrence. "Deterrence capability is based on the ability to wage real war, and the structure of deterrent

strength is indistinguishable from combat strength. Deterrent strength is embedded in real combat capability."[21] Chinese writings therefore suggest that deterrence is served by maintaining a capability of waging "real war", including mounting nuclear strikes. This view is reflected in what appears to be a concept of a "deterrence ladder", akin to an escalation ladder, as part of Chinese deterrent activities. In the PLA volume *Science of Second Artillery Campaigns*, the authors suggest that the Second Artillery (and presumably the PLA Rocket Forces) has adopted an escalatory ladder to frame their deterrence activities.[22] The rungs comprise:

- *Public opinion pressure*. The public display of Chinese nuclear missiles in the media underscores that China possesses a nuclear deterrent capability.
- *Elevating weapons readiness*. This includes increased readiness of warheads and launchers (which are seen as two separate, but related activities), as well as demonstrating launch preparations. Since Chinese nuclear warheads appear to be stored at centralized facilities, this would suggest that deploying warheads to missile units would be part of a Chinese deterrent effort.
- *Displays of actual capability*. This goes beyond public displays before the media, to include military reviews and parades; invitations to foreign attaches to inspect Chinese forces; and coverage of high level visits to forces in the field. The authors of *The Science of Second Artillery Campaigns* also suggest that mobile missiles might deploy while other nations' surveillance satellites are known to be overhead, or nuclear missile forces might be incorporated into various exercises. They also suggest simulated launches could be undertaken at this rung.
- *Manipulating tensions and creating impressions and misimpressions*. By deploying forces, emitting various signals and signatures, simulating launches, and/or raising readiness (in a demonstrable fashion), the PLA would seek to influence an adversary's calculus of the likelihood and destructiveness of a conflict.
- *Demonstration launches*. As a crisis progresses, the Chinese may decide to launch one or more missiles, in order to deter (or coerce) an adversary. These may be aimed at designated areas at sea or on land, and might involve the launch of several different types of missiles to demonstrate comprehensive readiness.
- *Demonstration launches near an adversary's forces or territory*. By engaging in test firings near an adversary's naval forces, homeland, or seized territories, the PLA would try to coerce an adversary into abandoning their ongoing activities. It is a form of indirect attack that seeks to deter or coerce.
- *Announcing the lowering of the nuclear threshold*. The PLA specifically associates this move with countering an adversary that has substantial nuclear capabilities, but also an advantage in high-technology conventional weapons. In order to counter the latter element, the Chinese leadership might announce a

[21]Academy of Military Science Military Strategy Research Office (PRC) 2013, p. 147.

[22]This section is drawn from Chinese People's Liberation Army Second Artillery 2003, pp. 281–296.

> lowering of the nuclear threshold, e.g., entertaining a nuclear response to conventional attacks against vital strategic targets in the PRC. These include nuclear facilities (including nuclear power stations); targets that could cause great loss of life such as hydroelectric facilities (presumably such as the Three Gorges Dam); the nation's capital or other major urban or economic centres. Such an adjustment might also occur if the PRC found itself in a situation where it was losing a conventional war, and was faced with a challenge to its national survival.

This array of actions underscores the Chinese belief that successful deterrence requires the PLA to be able to signal resolve—and those signals can include the employment of actual forces (as in the sixth and potentially the seventh rungs). Coupled with the incorporation of both conventional and nuclear forces under PLARF command, this would suggest that the PLA Rocket Force may envision conventional missiles as a means of warning of potential nuclear escalation. Rather than developing a nuclear counter-force capacity, the PLARF may hope to employ the same missile, with a conventional warhead, to engage in demonstrations or even attacks, as a warning of the potential for further escalation to nuclear means. For example, by employing conventional DF-21s, Chinese leaders could demonstrate the capability and reach of the missile, as well as their willingness to employ such systems. The existence of a nuclear-armed variant, perhaps within the same unit, would therefore exert deterrent pressure upon the adversary (coercive or dissuasive), whether there was an explicit threat or not.

This approach would also seem consistent with the Chinese belief in the need for tailored responses as part of deterrence efforts, including nuclear ones. As one analysis notes:

> The actual effects of nuclear deterrence are directly determined by the deterred side's awareness and understanding of nuclear deterrence information. The same type of capability and determination to apply that capability will generate different effects against different targets of deterrence, or the same target under different conditions.[23]

This suggests that the PLA's planners are trying to avoid a "cookie-cutter" approach towards deterrence. Instead, they will employ different deterrent measures against different adversaries, or even against the same adversary as conditions were to evolve.

China's deterrence efforts are further complicated because they must account for more than just the United States. Chinese leaders must also deter Russia, India, and potentially Japan. Thus, China arguably maintains more than a "minimal" deterrent's worth of nuclear weapons. It remains unclear, however, what Chinese strategic planners consider sufficient or necessary numbers of nuclear weapons to deter potential adversaries. Moreover, given the proximity of Russia, India, and Japan, Chinese nuclear planners could employ nuclear-armed medium and intermediate range ballistic missiles to effect nuclear deterrence. For the DF-21

[23]Academy of Military Science Military Strategy Research Office (PRC) 2013, p. 174.

(MRBM) and DF-26 (IRBM) missiles, Hans Kristensen and Matthew Korda assume China has 80 and 34 nuclear warheads respectively, as of 2019.[24]

10.3 Chinese Concepts of Space Deterrence

Chinese writings since at least the late 1990s have repeatedly emphasized the importance of establishing space dominance (*zhi taikong quan*; 制太空权), as part of fighting "local wars under modern, high-technology conditions", "local wars under informationised conditions", and now "informationised local wars". While the PLA is not necessarily reliant on space for its operations, its most formidable adversary, the United States, is seen as dependent upon space systems. Denying an adversary the ability to exploit space, as well as securing it for one's own use, is therefore integral to establishing space dominance. This, in turn, elevates the role of space deterrence (*kongjian weishe*; 空间威慑), which is now seen as a vital mission for the PRC's space forces. It is a relatively new task, arising in light of the rapid development of space technology, as well as the broad reliance upon space systems in support of other military functions.

Chinese writings define space deterrence as the use of space forces and capabilities to deter or coerce an opponent, preventing the outbreak of conflict, or limiting its extent should conflict occur. By displaying one's own space capabilities and demonstrating determination and will, the PLA would hope to induce doubt and fear in an opponent, so that they would either abandon their goals, or else limit the scale, intensity, and types of operations. It is important to note that space deterrence is not aimed solely, or even necessarily, at deterring actions in space, but rather, in conjunction with nuclear, conventional, and informational deterrence capabilities and activities, influence an opponent's overall perceptions and activities.

In the Chinese view, space deterrence has several unique characteristics.[25] One is *its broad impact* (*quan fangwei xing*; 全方位性). Effective space deterrence will affect not only space forces but terrestrial forces and operations as well. This reinforces the point that, from the Chinese perspective, "space deterrence" is not about deterring adversaries from acting in space, but exploiting space-related systems to achieve certain political and military aims (largely on Earth). Related to this is the assessment that *space deterrence is unified* or *integrated* (*yiti xing*; 一体性). This is a reflection of the unified nature of space capabilities, which includes military, civilian, and commercial space systems, and which encompasses systems in orbit, terrestrial tracking and control facilities, and associated data links. Successful space deterrence will employ a variety of means, including land, sea, and air-based systems as well as space-based capabilities, and will include both

[24]Kristensen and Korda 2019.

[25]Chinese Military Encyclopedia 2007, pp. 280–281.

offensive and defensive operations. Finally, implementing space deterrence must take into account *its comprehensive nature* (*zonghe xing*; 综合性). Space strength touches on a nation's economic, financial, scientific, as well as military capabilities. Space deterrence therefore reflects, in part, a nation's economic and scientific sophistication; that is, a country cannot have a strong space deterrent if it is economically and scientifically weak. At the same time, since a nation's space capabilities include not only its military systems, but also its commercial and civilian assets, facilities, and personnel, space deterrence therefore must include these elements as well.

PLA writings suggest that there is a perceived hierarchy of space deterrence actions. Although states may signal their broad pursuit of space deterrence through development of various technologies, in time of crisis or conflict, PLA teaching materials and textbooks suggest that the Chinese conceive of a "deterrence ladder" of space actions when in a crisis. This ladder goes beyond broad technological and bureaucratic developments, and involve displays of space forces and weapons; military space exercises; deployment or augmentation of space forces; and employment of space weapons.[26]

- *Displays of space forces and weapons* (*kongjian liliang xianshi*; 空间力量显示) occur in peacetime, or at the outset of a crisis. The goal is to warn an opponent, in the hopes of dissuading them from escalating a crisis or pursuing courses of action that will lead to conflict. Such displays involve the use of various forms of media to highlight one's space forces, and are ideally complemented by political and diplomatic gestures and actions, such as inviting foreign military attaches to attend weapons tests and demonstrations. An article from a leading PLA journal suggests that the space deterrence calculus includes not only military space forces but civilian systems as well.[27] Because of the steady increase in civilian space activities, and the concomitant rise in dual-use capabilities, many civilian space activities can rapidly morph into military ones. Thus, the article notes, launch of multiple satellites from one rocket and on-orbit satellite repair have military applications, and the conduct of such activities, even by civilian entities, is nonetheless a form of space deterrence.
- *Military space exercises* (*kongjian junshi yanxi*; 空间军事演习) are undertaken as a crisis escalates, if displays of space forces and weapons are insufficient to compel an opponent to alter course. They can involve actual forces or computer simulations, and are intended to demonstrate one's capabilities but also military preparations and readiness. At the same time, such exercises will also improve one's military space force readiness. Examples include ballistic missile defence tests, anti-satellite unit tests, exercises demonstrating space strike (*kongjian tuji*; 空间突击) capabilities, and displays of real-time and near-real time information support from space systems.

[26]Chang 2005; Jiang 2013.

[27]Sun and Chang 2003, p. 33.

- *Space force deployments* (*kongjian liliang bushu*; 空间力量部署) are seen as a significant escalation of space deterrent efforts. It occurs when one concludes that an opponent is engaged in preparations for war, and involves the rapid adjustment of space force deployments. As with military space exercises, this measure is not only intended to deter an opponent, but should deterrence fail, is seen as improving one's own preparations for combat. Such deployments, which may involve moving assets that are already in orbit and/or reinforcing current assets with additional platforms and systems, are intended to create local superiority of forces so that an opponent will clearly be in an inferior position. It may also involve the recall of certain space assets (e.g., space shuttles), either to preserve them from enemy action or to allow them to prepare for new missions. This may be akin to the evacuation of dependents from a region in crisis, as a signal of imminent conflict.
- The Chinese term the final step of space deterrence as "*space shock and awe strikes* (*kongjian zhenshe daji*; 空间震慑打击)". If the three previous, non-violent (or less violent) deterrent measures are insufficient, then PLA writings suggest that it may engage in punitive strikes, so as to warn an opponent that one is prepared for full-blown, comprehensive conflict in defence of the nation. Such strikes are seen as the highest, and final technique (*zuigao xingshi he zui hou shouduan*; 最高形式和最后手段) in seeking to deter and dissuade an opponent. Employing hard-kill methods, soft-kill methods, or a combination, one would attack an opponent's physical space infrastructure or data links, respectively. If this succeeds, opposing decision-makers will be psychologically shaken, and cease their activities. If it fails, an opponent's forces will nonetheless have suffered some damage and losses, facilitating the securing of space dominance in a wartime context.

It is important to note that these various space deterrence activities are unlikely to be undertaken in isolation. Rather, they will be coordinated with other, non-space activities. Indeed, several Chinese analyses note that space operations enhance other forms of deterrence, including nuclear and conventional. By providing precise information on adversary forces (e.g., location), they make nuclear attacks more effective. Space dominance can be rapidly converted into advantages for one's air, naval, and ground forces.[28] Similarly, by maintaining constant surveillance of an adversary under all conditions, one exerts a broader psychological pressure that also enhances deterrent (and coercive) efforts.

[28]Sun and Chang 2003, p. 35.

10.4 Chinese Concepts of Information Deterrence

According to Chinese analyses, the rapid advances in information technology coupled with globalization have wrought a fundamental shift in the world's socio-economic situation. We now live in the Information Age, with information being the primary currency of international power: "Outer space and information space and network and electromagnetic space have become the new main focal points for major powers interested in developing their economy and increasing their comprehensive national power. It has become the new 'high ground' for maintaining security."[29]

The growing role of information and associated technologies has led to "information deterrence" becoming a new aspect of *weishe*. That is, information itself has become an instrument of conflict, with the ability to establish "information dominance" a central focus in future wars. The ability to threaten a nation's information systems directly affects societal stability, popular livelihood, and national survival.[30] According to Chinese analyses, "information deterrence" conceptually includes deterrence in the cyber realm, but goes further, encompassing all aspects of information and information operations. "Information deterrence (*xinxi weishe*; 信息威慑)" is defined in the PLA's terminological reference volume as "a type of information operations activity in which one compels the adversary to abandon their resistance or reduce the level of resistance, through the display of information advantage or the expression of deterrent/coercive information".[31] As with other PLA writings on deterrence, the Chinese approach to information deterrence does not differentiate between a compelling and a dissuasive effect.

The 2007 edition of the *PLA Encyclopedia* defines "information deterrence" as those activities in which "threats that employ information weapons or which implement information attacks against an opponent, lead to shock and awe and constrain the adversary".[32] Interestingly, this definition notes that "information deterrence" relies in part upon warning an adversary of the serious consequences of an attack (including through demonstration), creating fears that will influence the other side's cost-benefit analysis. The purpose of information deterrence, again, is to allow the deterring side to "achieve a particular political goal (*dadao yiding de zhengzhi mubiao*; 达到一定的政治目标)", *not* to prevent the other side from acting in the information domain.

Another Chinese study guide defines it as "a national display of information advantage or the ability to employ information operations to paralyze an adversary's information systems, so as to threaten that adversary. This serves to constrain

[29]Xie 2013, p. 126.

[30]Xiao 2015, p. 123.

[31]All Army Military Terminology Management Committee 2011, p. 262.

[32]Chinese People's Liberation Army National Defense University Scientific Research Department 2007, p. 283.

the other side, as part of the deterrent/coercive goal."[33] What is clear across these various definitions is that "information deterrence", like the broader Chinese conception of deterrence in general, includes both dissuasion and coercion, and embodies the idea of deterring *through* information operations, rather than deterring operations *in* information space.

From the Chinese perspective, the importance of information in the successful conduct of warfare means that one can also employ threats against the adversary's ability to obtain and exploit information in order to deter and coerce them. Among states with roughly equivalent levels of information technology, given the widespread penetration of the Internet into all aspects of life, the potential ability to massively disrupt the adversary's entire society provides an opportunity to engage in deterrence. Indeed, on a day-to-day basis, Chinese writings suggest they believe that information deterrence is already in effect among equal players, precisely because the scale of disruption that would otherwise erupt would be enormous, while few states are confident of their ability to avoid such disruptions.[34] However, where there is a distinct imbalance in information capabilities, it is harder for the weaker side to effect information deterrence. Conversely, the side that may be weaker in terms of conventional military power but who has significant network warfare capabilities may well be able to paralyze and disrupt the more conventionally capable side, and at least impose greater costs, if not actually defeat them.[35]

In the Chinese view, the ability to successfully conduct offensive information operations is therefore the most important means of implementing information deterrence. A demonstrated capability of exploiting information to one's own end, even if not employed, will nonetheless arouse concerns in the adversary. To this end, network offensive power, the ability to conduct effective computer network attack operations is essential, as it is seen as the foundation for information deterrence.[36] This is in part because computer network attack (CNA) capabilities are relatively inexpensive, yet able to exploit a variety of means of attack, especially since computer networks now permeate so many aspects of society, the economy, and national security. Consequently, there is an unprecedented ability to employ CNA to paralyze and disrupt an adversary across much of its society. Moreover, there is a wide range of capabilities that can be employed, and a variety of vulnerabilities that can be exploited. These elements make network security difficult, both in terms of establishing counters but also establishing attribution.[37] Consequently, the implicit threat underlying information deterrence is harder to counter than conventional, nuclear, or space deterrence. Indeed, the uncertainty

[33]Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office 2005, p. 15.

[34]Academy of Military Science Military Strategy Research Office 2013, p. 196.

[35]Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office 2005, pp. 15–16.

[36]Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office 2005, p. 15.

[37]Xiao 2015, p. 123.

confronting all states even now about the ultimate effect of information operations, and especially attacks against each other's information networks, is believed to be a major factor in forestalling the occurrence of large-scale network conflict.[38] Chinese analysts seem to believe that this uncertainty creates the opportunity for robust information deterrence. As the 2013 volume of *Science of Military Strategy* notes, in order to produce an effective deterrent strength, it is necessary to not allow the adversary to accurately determine the deterring side's applicable policies, applicable forms, and compel the adversary [the target of deterrence] to constantly be guessing and feel that they are faced with hard choices.[39]

In the event of a crisis, some Chinese analysts suggest that one could remind an adversary of one's ability to plant computer viruses or that one is prepared to undertake large scale paralyzing attacks against an adversary's "finances and exchanges, energy resources, transportation, or military command systems" in order to warn them to cease and desist their resistance.[40] At a minimum, such moves are considered likely to affect the adversary's will to fight. At the same time, a clearly demonstrated ability to defend and safeguard one's information resources and systems can also serve to deter an adversary. If the adversary is unable to successfully attack one's information systems, then their ability to establish information dominance is likely to be extremely limited. In which case, their ability to establish dominance over other domains (e.g., air, space, maritime) is also likely to be very constrained, reducing their chances of successfully achieving whatever strategic objectives they might have. Under such circumstances, the adversary is likely to be deterred from initiating aggression, or may be coerced into submitting.

10.5 A Possible Information Deterrence Ladder

Given Chinese writings about deterrence activities in the space and nuclear domains, it is possible that there is a "deterrence ladder" for information operations. Chinese writings suggest that a deterrence ladder for information is indeed being explored.[41] One article by a PLA expert from the Chinese military's Academy of Military Sciences lays out such a conceptual ladder for information deterrence.[42]

---

[38]Academy of Military Science Military Strategy Research Office 2013, p. 190.

[39]Academy of Military Science Military Strategy Research Office 2013, p. 137.

[40]Liang Shenying, Sun Ying, "Pushing the Construction of Strategic Deterrence Capability, Using War to Deter War", *Xinhua Monthly* (2 November 2017).

[41]All references in this section, unless otherwise stated, are drawn from Yuan 2016.

[42]The People's Liberation Army Academy of Military Science is the leading brain trust for the PLA. It is comparable to a combination of the RAND Corporation, the US Army's Training and Doctrine Command (for the entire PLA), the Inspector General directorate, and some aspects of the Command and General Staff College (for the entire PLA).

- *Deterrence through network technology experimentation* (*wangluo kongjian jishu shiyan weishe*; 网络空间技术试验威慑). The first, basic step for information deterrence is to undertake testing and development of new technologies associated with network warfare. This includes cyber weapons, but also new offensive methods and tactics. As important, one should allow such efforts to be revealed through the media, thereby informing the rest of the world of one's capabilities. A strong foundation in information technology and training is essential. As important, because of the rapid pace of development in this field, new breakthroughs may occur at any time; uncertainty about that can also support deterrent policies.
- *Deterrence through network equipment displays and demonstrations* (*wangluo kongjian zhuangbei zhanshi weishe*; 网络空间装备展示威慑). Where the first step of information deterrence is demonstrating technological capabilities, the second step involves demonstrating a broader array of network warfare capabilities, including equipment development plans, prototype testing, and equipment production. This approach will deliberately reveal to an adversary China's overall capabilities (rather than individual pieces of equipment or programs), as well as demonstrate that they are part of a broader, integrated development effort. Yuan Yi specifically mentions the publication of white papers (such as the Chinese defence white paper), newspaper and magazine articles, and other official releases of information.
- *Deterrence through network operational exercises* (*wangluo kongjian zuozhan yanxi weishe*; 网络空间作战演习威慑). Simply displaying network capabilities, and discussing them, may not deter a potential adversary. The next rung on the Chinese information deterrence ladder is therefore to undertake operational exercises. This can involve forces deploying and operating in a real environment or a simulated one. The article suggests that public exercises involving forces in the field are typically defensive, while more offensive operations are undertaken in simulated environments, such as national cyber test ranges. Yuan Yi specifically mentions the American "Schriever" space wargames as an example of how the United States displays and develops network warfare capabilities and signals its resolve to employ them.
- *Deterrence through actual network operations* (*wangluo kongjian zuozhan xingdong weishe*; 网络空间作战行动威慑). In both the nuclear and space contexts, the highest level of deterrent action is the actual employment of nuclear and space capabilities respectively, intended to signal an adversary the critical nature of the situation, and to demonstrate resolve. As important, employment of such weapons can affect the initial campaign, if the target is sufficiently valuable. Chinese writings suggest a similar mind-set may exist for information deterrence, i.e., that the highest rung would be the employment of actual network warfare capabilities against an adversary's systems. This might involve a direct attack against key adversary networks, in order to pre-empt an enemy attack, or in response to an adversary's probe, as retaliation (and a demonstration of capability). Yuan Yi suggests a more psychological focus, such as disrupting email networks, generating a flood of text messages, and

> attacks against the power grid. Another Chinese analyst argues that successful information deterrence requires the implementation of "key point, planned, strong, multiple revisit, sustained deterrent/coercive information attacks. This will cause the adversary to have lowered self-confidence, shaken will, altered determination, so as to achieve the goal of winning without fighting."[43]

It is important to keep in mind that such information deterrent activities would not be occurring in isolation, but would be coordinated with a host of comparable activities. These would involve not only military forces (e.g., naval exercises, space exercises), but also diplomatic and political pronouncements, economic measures, etc. This is especially likely to be the case at the higher rungs on the ladder. At the same time, however, because China confronts a variety of potential adversaries, its leaders must constantly strive to engage in multilateral deterrence. Therefore, the Chinese leadership may not necessarily engage only in deterrent activities against, say, the United States or Japan, even in the midst of a crisis with those states. Heightened operations or limited offensive information operations, in the deterrent context, may be undertaken against third parties, both in order to demonstrate capability and resolve against the main target, but also to signal those third parties (and others) that China has sufficient capability to degrade them as well.

10.6 Other Chinese Deterrence Activities

Chinese analysts note the growing role of space, and information deterrent activities, which combine with more traditional nuclear and conventional deterrence to offer a wider variety of deterrent techniques.[44] Chinese writings suggest, though, that they see many other capabilities as providing even more means for effecting *weishe* (i.e., both compellence and dissuasion). One Chinese article, for example, enumerates a number of means of developing strategic deterrent techniques (*zhanlue weishe shouduan*; 战略威慑手段). These include not only developing strong overall military capabilities, fielding sufficient nuclear forces, and undertaking certain types of military activities, but it also notes the role of public diplomacy and public opinion; strategic psychological warfare; and improving military preparations.[45] Military diplomacy and propaganda work, for example, improves China's deterrent capacity, by expanding and improving China's and the PLA's international image.[46]

[43]Yibing 2011.
[44]Xiao 2008.
[45]Zhang 2004, pp. 33–34.
[46]Wang 2015, p. 13.

10.6.1 Mobilisation

An important contributor to deterrence, in the Chinese view, is mobilisation. The Chinese military defines "national defence mobilisation (*guofang dongyuan*; 国防动员)" as those steps undertaken by the government to convert some or all of various sectors from a peacetime footing to a wartime one, in response to conflict, national security threats, or crises. Mobilisation encompasses the preparations, planning, organization, and implementation of armed forces mobilisation, national economic mobilisation, political mobilisation, militia mobilisation, science and technology mobilisation, equipment mobilisation.[47] Chinese analysts see national defence mobilisation as a vital strategic option, allowing the nation to cope with threats while still allowing the national development focus to be on non-military aspects.[48] In addition, however, in the context of deterrence, they see the act of mobilising as exerting a deterrent effect. The implementation of "national defence mobilisation is the expression of a nation's will and its interests".[49] As important, because of civil-military integration and the melding or fusion of civilian and military power (*junmin ronghe*; 军民融合), mobilisation is essential in order to supplement a nation's combat power.

Actual mobilisation of a nation can deter adversaries by demonstrating both Chinese will and the ability of the PRC to expand and increase its actual capability.[50] A decision to mobilise converts a portion of China's potential military capability into actual military forces and strength. This is likely to cause an adversary to reassess the situation and recalculate the likely costs and benefits of their course of action. By shifting the balance of power, and potentially raising both costs and risks, the adversary may be deterred. Moreover, given the costs associated with mobilisation, the willingness to nonetheless accept that burden demonstrates China's will and resolve.

Similarly, Chinese analysts argue that public announcements of mobilisation, and mobilisation exercises, also have a deterrent effect. This is in part consistent with the Chinese emphasis that successful deterrence requires not only capability and will, but communicating those aspects to the target of deterrence. Indeed, the passage of the Chinese National Defence Mobilisation Law in 2010 is seen as part of this public messaging, "demonstrating the will to defend national security" in the face of existing threats.[51]Through public pronouncement of mobilisation orders, Chinese analysts believe that one may be able to induce shock and awe in the other

[47]All Army Military Terminology Management Committee 2011.

[48]Chinese People's Liberation Army National Defense University Scientific Research Department 2007, p. 13.

[49]Ren 2010, p. 14.

[50]Ren 2008, p. 227; Peng and Yao 2001, p. 51.

[51]Hu and Huang 2010, pp. 3–4.

side, causing them to be deterred (or coerced).[52] Mobilisation exercises can have a similar effect. They improve the organization and planning of mobilisation; a more effective mobilisation structure contributes to deterring an adversary. In addition, such exercises publicly display China's ability to mobilize, thereby further influencing the adversary, and helps achieve the goal of mobilisation deterrence (*dongyuan weishe*; 动员威慑).[53]

10.6.2 Conventional Deterrence

The available Chinese literature does not tend to focus on conventional deterrence. In a different volume of the PLA Encyclopedia, for example, there is discussion of conventional deterrence, but it is not broken out as a distinct form, unlike nuclear or space deterrence. Instead, it is mentioned, in terms of large conventional force deployments, alongside deterrence with nuclear and missile forces, as a means of deterring foreign aggression.[54] More discussion is accorded conventional deterrence in the 2015 edition of the *Science of Strategy* (amounting to one paragraph). This volume notes that conventional deterrence lost utility in the early days of the Nuclear Age, but has since been revived, in part due to the effectiveness of high-technology, long-range weapons. Conventional deterrence is described as controllable, and relatively low risk, generally not leading to large-scale destruction as with nuclear weapons, and therefore more likely to achieve political goals.[55] As the Chinese are discussing *weishe*, this description would suggest that the focus is as much on conventional compellence as on conventional deterrence in the Western sense.

Indeed, this would align with the 2013 *Science of Military Strategy*, which notes that conventional forces that have demonstrated an ability to defeat enemies can create deterrent effects. The authors note that the US-led 2003 Iraq War, where the US military rapidly defeated its adversary, sued real war to expand the effects of deterrence, while deterrence (weishe) effectively strengthened real war effectiveness.

> It was a paragon of linking deterrence and real war. As conventional weapons' killing power is constantly increasing, real war actions generate deterrent effects. Inevitably, this will make potential adversaries undergo sustained deterrent impacts.[56]

[52]Ren 2010, p. 79.

[53]Xu and Wang 2010, pp. 2–3.

[54]Editorial Committee 2007, p. 247.

[55]Xiao 2015, p. 12.

[56]Academy of Military Science 2013, p. 138.

This discussion also highlights that, from the Chinese perspective, conventional deterrence is not simply about having technical capabilities, but demonstrated effectiveness of one's conventional forces.

10.6.3 Non-military Deterrence Activities

While this paper focuses on actions by the Chinese military and national security establishment to effect deterrence, as the Chinese have expanded their economy and other instruments of national power, their ability to influence other peoples' calculations has grown. They have more instruments of influence, including economic, financial, diplomatic, as well as military. Because of the reach of the Chinese government and the Chinese Communist Party, the PRC is able to undertake not only a whole of government approach towards deterrence (including coercion), but a whole of society approach to deterrence and compellence. This approach almost certainly incorporates tourism, trade, investment, and political warfare (including the "three warfares"), as well as more traditional military and diplomatic tools. China has increasingly used trade as a tool of deterrence (in the compellence sense). In 2010, a Chinese fishing boat rammed two Japanese Coast Guard vessels. After the captain was taken into custody, Japanese authorities indicated they were planning on trying him. After strident Chinese protests, the Japanese government released the captain without trial. Nonetheless, the PRC decided to suspend exports of rare earth minerals to Japan. This led to some disruptions in Japanese supply chains, but also drew attention to China's dominant position in the rare earths market. It remains unclear what the purpose of the embargo was intended to serve, but it is likely that it was intended to coerce Japan and prevent it from pushing its claims to the Senkakus.

China has also weaponized its tourist trade. The burgeoning Chinese economy has led to a massive growth in the number of Chinese tourists and tour groups worldwide. But Beijing has actively discouraged tourists visiting countries with which it has disputes, seeking to coerce these states into a more amenable political line. In 2012, tensions between China and the Philippines flared when both sides laid claim to Scarborough Shoal in the northern reaches of the South China Sea. (It is not part of the Spratly island grouping.) China subsequently issued a travel advisory about the Philippines, and began to discourage its tourists from visiting.[57] This affected many Philippine resorts and even led to cancelled flights. The ban was only lifted after the more conciliatory Rodrigo Duterte was elected in 2016.[58] Other examples involve Taiwan and South Korea. Since 2016 the number of Chinese

[57] Al-Jazeera 2012.

[58] Almendral 2014.

tourists to Taiwan has dropped precipitously since the sweeping electoral victories of the pro-independence Democratic Progressive Party (DPP) in that year.[59] Beijing's efforts to persuade Seoul to suspend the deployment of the THAAD missile defence system has included discouragement of tourist groups from visiting the ROK. Reports that China may officially order tour organizers to cancel visits caused the South Korean stock market to fall 1.1 percent.[60]

While such moves are economic, they nonetheless would seem to fit the broad Chinese conception of *weishe*. They are intended to compel an adversary to submit to the Chinese will. As important, they are a means of achieving a Chinese political goal, without requiring the use of force—and "causing the enemy to submit without fighting" is part of the Chinese definition of *weishe*. Just because these efforts do not include a military component should not remove them from our analysis of Chinese concepts of deterrence, or more accurately, compellence.

10.7 Deterrence by Punishment or Denial (?)

A major focus of Western discussions of deterrence has been the difference between "deterrence by punishment" versus "deterrence by denial". Deterrence by punishment involves the threat of inflicting more pain or imposing more costs than the adversary would be able to gain from their action. Deterrence by punishment can include escalation, both horizontal and vertical. Deterrence by denial, on the other hand, seeks to deter an adversary by denying them any advantage from the action that is trying to be deterred. Deterrence by denial is typically associated with the ability to defend a given target or likely objective. A military which can block an adversary's ability to gain territory, for example, through successful defence is engaging in deterrence by denial.[61] The Chinese literature thus far reviewed does not provide any indications of a comparable discussion in Chinese writings. There is little indication of a specific terminological differentiation, which has preoccupied so much of Western literature.

Chinese writings seem to suggest that both deterrence by denial and by punishment are embodied in *weishe*, since there is discussion of both imposing higher costs on an adversary and on preventing adversaries from achieving their goals. This is consistent with the focus of *weishe*. It is on achieving a particular end, be it dissuading an adversary from a given action or compelling them to perform an action. Whether the desired goal is achieved by threatening punishment or by denying them gains matters less than that the adversary conforms to the deterring power. In this regard, the Chinese approach would seem much more pragmatic and

[59]Smith 2016.

[60]Reuters 2017.

[61]For further Western discussions of "deterrence by denial" and "deterrence by punishment", see Snyder 1960; Mazarr et al. 2018.

effects-oriented. This also suggests that the Chinese will employ both methods, i.e., deterrence by denial and deterrence by coercion, in order to compel an adversary to submit. In the 2013 Science of Strategy, for example, the success of deterrence rests upon the reality of combat power (which would suggest deterrence by denial), the ability to retaliate credibly (which would suggest deterrence by punishment), and the decisiveness of the deterrent actions undertaken.[62]

Further complicating Western analyses is the convergence between "deterrence" and warfighting. At the top of the Chinese conception of deterrence ladders for nuclear weapons, space capabilities, and information operations is the convergence between *weishe* and "real war (*shizhan*; 实战)". In the various Chinese writings, there is a consistent view that, at that last rung, one will hopefully persuade an adversary to back down based on the demonstration of will and capability. Should that fail, however, then successful implementation of that last rung will improve one's military situation (e.g., by gaining the initiative or neutralizing a key adversary asset). This linkage raises real questions about Chinese views of crisis stability and crisis management. However, it would seem that, from the Chinese perspective, the potential for loss of crisis control may serve to enhance deterrence. If that is their viewpoint, this would seem to align with the Western concept of "deterrence by denial".

On the other hand, another common element in the various deterrence ladders is the idea of revealing new capabilities or new forces. Such revelations, coupled with shifting or altered force deployments, enhances deterrence because it complicates an adversary's planning and targeting. The utility of surprise for enhancing deterrence is specifically noted in the 2013 Science of Strategy, which notes that not only new forces and technologies, but new concepts and doctrine can cause an adversary's assessment of the military balance to be "even less certain, effectively scrambling the adversary's original strategic preparations, elevating the credibility of deterrence".[63] This would seem to be a version of "deterrence by punishment". This array of discussions suggests that it is not an issue of cognizance; that is, Chinese thinkers are not ignorant of the difference between "deterrence by denial" and "deterrence by punishment", but that this difference does not necessarily have significant meaning in the Chinese strategic context.

10.8 Conclusion

China's strategic culture is several thousand years old. It developed within a very different milieu from that of the West. China has long been the dominant hegemon of the Asian continent, unrivalled in a way that has not existed in the West since the

[62]Academy of Military Science 2013, pp. 152–153.

[63]Academy of Military Science 2013, p. 150.

Roman Empire. Not surprisingly, then, it has developed a different conception of deterrence, a product of its own circumstances.

- China's concept of deterrence includes both dissuasion and coercion. It would therefore be more accurate to say that Chinese strategic thinkers engage in compellence, rather than "deterrence".
- Chinese concepts of compellence entail the use of various forms of power, both military and non-military. In the military context, they have long thought of multi-domain deterrence, incorporating nuclear, space, and information means. In this regard, Chinese deterrence and compellence actions do not appear to be oriented towards forestalling or preventing action in a given domain (space, cyber/information), or types of capabilities (nuclear, conventional). Rather than a goal or end, deterrence/compellence is a means to achieving a pre-determined political goal.
- Chinese compellence efforts are closely tied to their war-fighting concepts. Should the dissuasive or coercive effort appear to be failing, the final stage of compellence actions will likely overlap with war-fighting actions. The linkage itself, by raising issues of crisis stability, enhances deterrent effects, in the Chinese view.

Much of the available Chinese literature from which this is drawn was written before the massive reform of the PLA that occurred at the end of 2015. As the PLA has evolved organizationally, as well as in terms of equipment and operating range, it is likely that its views of deterrence and compellence has had to accommodate these changes. It is essential that further research be undertaken in this area. Unfortunately, the PRC has also become far less open in the intervening half-decade. Accessing Chinese materials, especially authoritative volumes such as military textbooks and teaching materials, has become far more difficult. A concerted effort, coordinated among various research organizations, should be a priority to support this research.

References

Academy of Military Science Military Strategy Research Office (PRC) (2013) The Science of Military Strategy. Military Science Publishing House, Beijing PRC, p 147

Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office (2005) Informationized Operations Theory Study Guide. Military Science Publishing House, Beijing PRC

Al-Jazeera (2012) Travel Warning Escalates China-Philippine Row (11 May 2012). http://www.aljazeera.com/news/asia-pacific/2012/05/20125109562394196.html. Accessed: 12 January 2020

All Army Military Terminology Management Committee, Academy of Military Sciences (2011) Chinese People's Liberation Army Terminology (Unabridged Volume). Military Science Publishing House, Beijing PRC, p 51

Almendral A (2014) Philippines Feels Force of China Travel Warning. http://www.bbc.com/news/world-asia-29684938. Accessed: 12 January 2020

Chang X (2005) Military Astronautics. National Defence Industries Press, Beijing PRC
Chinese People's Liberation Army National Defence University Scientific Research Department, Chinese Military Encyclopedia (2007) Military Strategy. Chinese Encyclopedia Publishing House, Beijing PRC
Chinese People's Liberation Army Second Artillery (2003) The Science of Second Artillery Campaigns. PLA Publishing House, Beijing PRC
Deng L (1993) China Today: Defence Science and Technology, Vol. I. National Defence Industry Press, Beijing PRC
Editorial Committee (2007) Chinese Military Encyclopedia, 2nd edn. Military Strategy. China Encyclopedia Publishing House, Beijing PRC
George A, Smoke R (1974) Deterrence in American Foreign Policy: Theory and Practice. Columbia University Press, New York
Hu T, Huang G (2010) Study Questions and Answers for the "People's Republic of China National Defence Mobilisation Law". National Defence University Publishing House, Beijing PRC
Jiang L (2013) Space Operations Teaching Materials. Military Science Publishing House, Beijing PRC
Kristensen H M, Korda M (2019) Chinese nuclear force 2019. Bulletin of the Atomic Scientists, 75.4:171–178. https://doi.org/10.1080/00963402.2019.1628511
Liang S, Sun Y (2017) Pushing the Construction of Strategic Deterrence Capability, Using War to Deter War. Xinhua Monthly November 2:2017
Mazarr M J et al (2018) What Deters and Why: Lessons of Deterrence Theory and Practice for U.S. Army Forces and Capabilities. RAND, Santa Monica
Mearsheimer J (1983) Conventional Deterrence. Cornell University Press, Ithaca NY, p 14
National Defence University Science Research Department (2004) New Perspectives on Military Transformation: Explaining 200 New Military Concepts. PLA Press, Beijing PRC, p 85
Office of the President of the United States (2010) National Security Strategy. Government Printing Office, Washington DC, pp 17–18. https://www.hsdl.org/?view&did=24251
Peng G, Yao Y (2001) Science of Military Strategy Teaching Materials. Military Science Publishing House, Beijing PRC, p 51
Peng G, Yao Y (2005) The Science of Military Strategy. AMS Press, Beijing PRC, p 215
PLA Encyclopedia Committee (2002) Chinese Military Encyclopedia, Supplemental Volume. Academy of Military Science Publishing House, Beijing PRC, p 477
Ren M (2008) Science of National Defence Mobilisation. Military Science Publishing House, Beijing PRC, p 227
Ren M (2010) Theories of National Power Mobilisation. Military Science Publishing House, Beijing PRC, p 14
Reuters (2017) South Korean Stocks Fall on Fears of Chinese Tourism Ban. http://www.voanews.com/a/south-korean-stocks-chinese-anger-thaad/3748022.html. Accessed: 18 January 2020
Schelling T (1966) Arms and Influence. Yale University Press, New Haven CT, p 69
Smith N (2016) China Is Using Tourism to Hit Taiwan Where It Really Hurts. http://time.com/4574290/china-taiwan-tourism-tourists/. Accessed: 18 January 2020
Snyder G (1960) Deterrence and power. Journal of Conflict Resolution (International), vol. 4(2), pp 163–178
Snyder G (1988) Deterrence and Defence. In: Art R (ed) The Use of Force. University Press of America, New York, p 31
Sun H, Chang J (2003) A New Shape of Military Deterrence—Space Deterrence. Military Art 10:33
Wang B (2015) Research on the Military's Foreign Propaganda Work. National Defence University Press, Beijing PRC, p 13
Xiao MGY (2008) Major Power Military Theory Innovation Amidst the New Global Military Transformation. Military Art 2:all
Xiao T (2015) The Science of Strategy. National Defence University Publishing House, Beijing PRC, p 119

Xie X (2013) National Security Strategy Teaching Materials. Military Science Publishing House, Beijing PRC, p 126
Xu J, Wang Y (2010) National Defence Mobilisation Exercises: Organization and Implementation. Liberation Army Publishing House, Beijing PRC, pp 2–3
Yibing J (2011) The Use of Information Deterrence and Joint Operations in Battle. Journal of Xi'an Politics Institute, 24(5), p 32
Yuan Y (2016) AMS Expert Discloses Network Space Deterrence. http://news.xinhuanet.com/mil/2016-01/06/c_128599390.htm. Accessed: 20 January 2020
Zhang P (2004) How to Develop Strategic Deterrence Techniques. Military Art 2:33–34
Zhou P, Wen E (2004) Developing the Theory of Strategic Deterrence with Chinese Characteristics. China Military Science 3:20

Dean Cheng is The Heritage Foundation's research fellow on Chinese political and security affairs. Having worked for SAIC and the Center for Naval Analyses, Cheng has written extensively on China's military doctrine, technological implications of its space program and "dual use" issues associated with the communist nation's industrial and scientific infrastructure.

Chapter 11
Japanese Concepts of Deterrence

Nori Katagiri

Contents

Abstract Japan has consistently adopted a deterrence-by-denial strategy in the post-war period. Its ability to deter foreign attacks depends more heavily on its ability to deny hostility than to punish perpetrators. Japan's deterrence-by-denial posture has faced at least two major problems. One problem is the inherent limit on its ability to deter foreign attacks. This posture is more oriented toward defence-by-denial than real deterrence. Japan's national security resources and institutions are positioned to deny hostility to defend the homeland, but they are not suited to deter foreign attackers because Japan bans itself from having the ability to conduct offensive military operations—a necessary factor for deterrence by the imposition of threats. Existing restrictions on the use and threat of force stem from post-war constitutional and normative constraints that have proven anachronistic today.

Keywords Japan · Self-Defence Force · deterrence by denial · extended deterrence · internal balancing

N. Katagiri (✉)
Saint Louis University, 3750 Lindell Boulevard, St. Louis, USA
e-mail: nori.katagiri@slu.edu

F. Osinga and T. Sweijs (eds.), *NL ARMS Netherlands Annual Review of Military Studies 2020*, NL ARMS, https://doi.org/10.1007/978-94-6265-419-8_11

11.1 Introduction

In this chapter, I identify some of the most important changes and continuities in the practice of deterrence by investigating the "Japanese way of deterrence (抑止, "yokushi" in Japanese)". Specifically, I examine Japan's deterrence posture by identifying the differences between deterrence-by-denial and deterrence-by-punishment. I follow other chapters of the book in defining the terms. On the one hand, deterrence by denial (拒否的抑止, "kyohi teki yokushi" in Japanese) is the ability to deny actions and persuade the opponent that it is unlikely to attain its immediate objectives at a reasonable cost. On the other hand, deterrence by punishment (懲罰的抑止, "chobatsu teki yokushi" in Japanese) comes from efforts to coerce targets into being discouraged from doing what they would otherwise do by the threat of punishment.[1]

My argument is twofold. First, Japan has consistently adopted a deterrence-by-denial strategy in the post-war period. Its ability to deter foreign attacks depends heavily on its ability to deny hostility. Japan's defence posture has in turn drawn from the combination of internal balancing and multilateral hedging strategy with the US alliance at its centre.[2] The defence posture has shaped Tokyo's preferences on operations, weapons acquisition, and joint exercises. Slow but clear changes have occurred mostly at tactical and operational levels of the denial strategy. In short, the traditional political and strategic foundation of defence policy remains firmly in place, while operational and tactical levels of defence policy get constant adjustments and upgrades in order to increase deterrent capability.

Second, Japan's deterrence-by-denial posture has faced at least two major problems. One problem is the inherent limit on its ability to deter foreign attacks. This posture is more oriented toward defence-by-denial than real deterrence. Japan's national security resources and institutions are positioned to deny hostility to defend the homeland, but they are not suited to deter foreign attackers because Japan bans itself from having the ability to conduct offensive military operations—a necessary factor for deterrence by the imposition of threats. Existing restrictions on the use and threat of force stem from post-war constitutional and normative constraints that have proven anachronistic today. This leads to the second problem in that recent changes in weapons acquisition, logistics, and combat preparedness have not significantly helped increase Japan's deterrence. These changes are so focused on equipment and technology that the overall lack of deterrence continues to hold.

I make these arguments in three steps. First, I explore the concepts of deterrence, deterrence by denial, and deterrence by punishment both in general terms and in Japanese strategic contexts. I do so by investigating how Japan's deterrence posture has developed since the end of the Cold War. Second, I explore how legal and normative restrictions on the use of force have shaped Japan's deterrence-by-denial posture. Finally, I disentangle the deterrence-by-denial posture by looking into the

[1] Preface by Osinga and Sweijs in the present volume.

[2] Katagiri 2019.

strategy of internal balancing and multilateral hedging—the two elements that characterize the "Japanese way of deterrence".

11.2 Deterrence-by-Denial and Japan's Threat Perception

In this chapter, deterrence is defined in terms of state practice to use the prospect of harm to coerce an opponent *not* to engage in unwanted behaviour. The key to deterrence is to credibly threaten the imposition of such an unbearable pain that the opponent reconsiders actions that it would otherwise take.[3] Defining deterrence this way allows us to understand Japan's deterrence efforts and make analytical distinction between deterrence by denial and deterrence by punishment. As mentioned above, deterrence by denial is the ability to deny actions and persuade the opponent that it is unlikely to attain its immediate objectives at a reasonable cost, while deterrence by punishment is based on the coercion of targets into being discouraged from doing what they would otherwise do by the threat of punishment. It consists of the threat of great harm, which will be imposed after the opponent has engaged in that behaviour. Japan's deterrence efforts represent the deterrence-by-denial through the logic of elimination; since the 1947 promulgation of the peace constitution, Japan has renounced its right to punish opponents and made it illegal to use force as a means of settling international disputes.

The Japanese meaning of the term deterrence is the same as Western concepts of deterrence. This is mostly because it was adopted from the Western literature, e.g. Thomas Schelling's *Arms and Influence* and Patrick Morgan's *Deterrence*,[4] according to Shuichiro Iwata, professor at the National Defence Academy.[5] 'Deterrence' first showed up in Japan's 1976 National Defence Program Guidelines. Every four years the Prime Minister issues an executive order that renews these guidelines to serve as a comprehensive defence doctrine; the word and meaning of deterrence has thus remained the same. Keitaro Ushirogata of Japan's Maritime Self-Defence Force, argues that as Japan's security environment evolved in recent years, the word has been used more frequently in government policy, academic publications, and policy discourse.[6] However, change, if any, comes very slowly. It is important to keep in mind the unique strategic context in which Japan formulates its deterrence posture. The term has always been used in the context of extended deterrence and as part of the US-Japan security alliance where the United States was a senior ally and Japan junior. The concept of deterrence never made its way into an independent defence strategy in Japan. This is because Japan's defence policy in the post-war era is different from the ideal-typical form of deterrence that

[3]Schelling 1968.

[4]Morgan 1983.

[5]Iwata 2015.

[6]Ushirogata 2015, pp. 21–23.

the concept illustrates. As such, the Japanese are closer to the idea of deterrence by denial than deterrence by punishment, although the most precise term for Japan's national security policy would be "defence by denial". It is because the coercive aspect of deterrence is deemed illegal due to a set of long-standing constraints on the use of force. This also comes from the fact that Japan's deterrence-by-denial effort is based on conventional deterrence without nuclear weapons.[7] That poses a challenge for Japanese strategists; they would need to achieve deterrence-by-denial through the threat of force when the option for punishment is not available.

The deterrence by denial posture has not fundamentally changed even though its strategic environment has changed. Japan consistently used US extended deterrence as an instrument to deal with security challenges from Russia, North Korea, and China, all nuclear neighbours with sizable conventional and cyber forces. Russia remains technically at war with Japan due to disagreement of ownership on the Northern Territories/Kurile Islands. North Korea's military power inflates Japan's threat perception by way of its medium-range ballistic missiles, nuclear weapons, and cyber forces. At the same time, however, the Japanese know that these programs would serve Pyongyang's primary goal of deterrence and national survival, not to be used pre-emptively to attack Japan. The main object of Japan's deterrence-by-denial posture is China. China poses the greatest multi-domain threats to Japan, including conventional, nuclear, and cyber forces backed by abundant economic and human resources. The Japanese perceive China's power as the most prominent determinant of their foreign policy.[8] This comes in part from the fact that the core of East Asian security in the 21st century has seen two major forces shaping regional dynamics: China's growing power and the US presence along with its allies.[9] The threat environment is tense, forcing close observers of East Asian security affairs like Thomas Christensen to consider China and Japan in the state of security dilemma.[10]

In fact, Japan has signalled its intent to balance China's military power via internal balancing and US extended deterrence. The actual output, however, is limited in nature, because some of the normative constraints that I discuss on the use of force in Japan have shaped the psychology of national leaders to tone down the threat element in favour of public opinion that predominantly supports non-military missions for Self-Defence Forces. Certainly, works of deterrence scholars like Robert Jervis offer a useful insight into the growing imbalance of threat perception. That is, the rising tension between Tokyo and Beijing may be a function of a chronic misperception and spiral of uncertainty stemming from the prevalent sense of insecurity on both sides of the Sea of Japan. If any, a misperception of mutual threats may have much to do with the way the two countries have interpreted each other's actions through the historical lens and a distorted projection

[7]Mearsheimer 1985, p. 15.
[8]Oros 2017; Samuels 2008.
[9]Katagiri 2015, p. 1170.
[10]Christensen 1999.

of one another's intent, making any rational move toward deterring the other by the threats of denial sufficiently threatening to undermine the semblance of a balance of power.[11] However, Japan has also worked hard to consistently signal its willingness to manage rivalry both diplomatically and peacefully, which is in part propelled by the commitment it has made to the deterrence-by-denial posture: a strategic posture designed to discourage China from using force through the show of sufficient force to deny Beijing's effort to undermine Japan's interests. This poses the challenge of dissuading China from taking provocative actions when Japan does not have the luxury of threatening the use of force for the purpose of denial. In other words, when Tokyo must demonstrate credible resolve in the eyes of Beijing officials that it is committed to deterring Beijing, it does not have the "teeth" to substantiate the resolve.

11.3 Determinants of Japan's Deterrence Posture

In this chapter, the two main sources of Japan's deterrence posture will be explored. The factors together ensure the continuation of post-war national security policy. The most important point about the constraints is its endurance that enables the continuation of deterrence-by-denial. This posture, however, comes at a cost. That is, it has made it hard for Japan to act as a "normal state"—a concept of state that is capable of using or threatening to use force as a means of national defence. This point is consistent with the literature of Japanese security policy. Scholars have noted the recent growth of Japan's defence capability, but not deterrence. Many observers also emphasize that the increase in defensive capability has not meant that Japan has become any more militaristic or nationalistic than the past. Only a small number of Japan scholars like Harvard professor Ezra Vogel correctly argue that "it's ridiculous to assume that changes in the policy for Japanese self-defence forces mean that Japan is going down the path of militarism. The entire situation is quite different than the 1930s and 1940s and there are many institutional barriers to the militarism of that era in place."[12] The reality is that while Japan undergoes technological and logistical upgrades, the socio-political foundation of national security policy remains remarkably pacifist. In this section, I discuss the legal and normative sources of such a posture.

[11] Jervis 1982.

[12] Pastreich 2015.

11.3.1 Legal Constraints

The first determinant of deterrence-by-denial comes from the "peace" constitution of 1947 and associated laws governing the Self-Defence Force (SDF), Japan Coast Guard (JCG), and national police. The obvious issue with the constitution is its Article 9 that bans possession of offensive capability, which questions the SDF's legality and legitimacy, and consequently undermines Japan's ability to use force as a means of deterring other nations from challenging Japanese sovereignty. The constitution allows SDF to use weapons to defend the country for the purpose of self-defence but not for deterring other nations because it removes SDF's ability to attack enemy forces. Further, the constitution bans use of force unless three conditions are met: (1) presence of imminent and illegal threat to the nation, (2) lack of appropriate alternative response, and (3) a minimum necessary amount of force to be used. Yet the constitution is hardly the only legal factor. Laws that govern SDF and JCG confine the defence forces to tight legal procedures, from tactical to operational to strategic levels. The legal constraint is doubly problematic because it puts psychological discomfort on defence personnel to feel unprotected for doing their job. The absence of offensive missions in their capability is critical in at least two ways. First, it forces Japan's foremost defence treaty ally, the United States, to take responsibility for planning and, if necessary, executing all offensive missions for Japan's war. This means that, for instance, a People's Liberation Army (PLA) attack on Japan would draw the US Forces in Japan (USFJ) into war with China when SDF cannot use force in an offensive manner. This leaves the task to USFJ, which would escalate the conflict between China and the United States. Second, the absence of offensive missions in Japan allows China, North Korea, and Russia to spend more on buying offensive weapons and save resources on defensive weapons and training. This further undermines Japan's ability to deter.

The legal constraint in Japan's deterrence posture was manifested, for example, in early 2013 when an airborne Japanese anti-submarine helicopter observed a Chinese frigate sail through the disputed East China Sea. Armed with hellfire missiles, the helicopter was 28 km away when the frigate put a missile guidance system on it, an action one step short of firing a shot. While tense, nothing happened, and the Japanese helicopter left the area. Eleven days later, a 6000-ton Japanese destroyer *Yudachi* was sailing through the same sea when the 2400-ton Jiangwei II-class *Lianyungang* pointed a missile at it. *Yudachi* did nothing; it stood off for a few minutes before it sailed away. *Yudachi*'s armament—harpoons, Phalanx cannons, and torpedoes—went unused. Japan's Foreign Ministry lodged a protest, followed by Prime Minister Shinzo Abe criticizing China for violating international rules of behaviour, but he quickly sought to deescalate the crisis saying that the two nations should keep communications open and stay on the course of "strategic interdependence". Facing a direct threat in a contested ocean from the smaller frigate, why did the Japanese destroyer not take action? The answer is that this was a routine; the destroyer was not authorized to fire because the Chinese ship did not shoot first. Rules of engagement disallowed the *Yudachi*

commander from acting in self-defence. *Yudachi*'s commander, Commander Kazuhiro Kuroki, was not disciplined but commended for doing his job. That Kuroki withheld fire was no surprise; the laws have long banned pre-emption.

The legal constraint also applies to cyber operations. Japan has made significant progress over the years to beef up national critical infrastructure, which involved institutional overhaul, bureaucratic reorganization, and training of personnel in the public and private sectors. On the offense side, however, Japan has faced tremendous legal hurdles in the use of cyber force to dissuade potential attackers from acting maliciously. The constitution does not permit offensive cyber operations explicitly because it does not consider cyber-attacks an act of war, and therefore it does not extend legal authority for acting in self-defence. The penal code, a set of regulations on law enforcement and police agencies, addresses duties in a manner that is consistent with the constitution; it disallows the use of force unless (1) there is an imminent and illegal threat to the nation, (2) there is no appropriate alternative response, and (3) as long as a minimum necessary amount of force is used. Japan's use of law in cyberspace is made complicated by the legal restrictions on SDF. Only an imminent security threat would mobilize the SDF, but the "threat" is commonly understood to be physical, not digital, even though cyber-attacks are essentially constant and "immediate" at all times. Similar restrictions hamper JCG's operations. A civilian body of the Ministry of Land, Infrastructure, and Telecommunications, JCG has seen a steady rise in Chinese aggressiveness, which also has much to do with law and notoriously strict rules of engagement. The law does not allow JCG crew to, for example, board suspicious vessel, arrest members of the vessel that enter Japan's territorial sea, or use force unless and until they are fired at. JCG Law's Article 18 permits JCG crew to stop suspicious ships *if* a "crime" is about to be committed in territorial waters. If the suspicious vessel does not stop after a warning, the JCG crew are not allowed to board the vessel.[13] This creates another problem in that the law forces the crew under duress to quickly and accurately determine the illegality of the act before they respond. These restrictions as a whole challenge the confidence of JCG crew to use force.

11.3.2 Normative Constraints

The second factor consists of a set of four norms and principles of social behaviour. First is the doctrine of defensive defence, which bans offensive use of force even in wartime. It means that defensive force can only be used in the event of a foreign attack and is limited to the minimum necessary for self-defence. Since the 1970s it has informed Japan's deterrence-by-denial posture and affected weapons programs and operations. There are two problems with the doctrine. First, it keeps the government from procuring weapons that could be used in attack missions. Thus SDF

[13]Japan Coast Guard 2020.

is free of systems like aircraft carriers, attack helicopters, strategic bombers, and surface-to-surface missiles even if they are necessary to deter foreign aggression. Mid-air refuelling was banned until recently because "expeditionary" operations like that can be used to invade other countries and thus were considered offensive. The reason why Japan ended up having that capability was because airborne warning and control system (AWACS) needs mid-air refuelling to keep F15s—air-to-air combat aircrafts, which are not designed for ground attack—flying. The doctrine also indicates that once in war, Japan will not be able to move the battleground outside its soil. The war would have to be strictly a defensive war, which would generate a number of civilian casualties at home.

The second norm is the belief that SDF should devote itself to domestic humanitarian assistance and disaster relief (HA/DR) missions. This is consistent with the strong public support for SDF as a non-military force.[14] Figure 11.1 shows that between 2010 and 2018, HA/DR was the most popular SDF task. Markedly fewer respondents support the SDF for real national security missions. For example, a small number of people support the SDF's mission "toward suspicious ships and armed agents" when this is precisely what SDF and JCG are doing in the Senkaku area. Even fewer people support SDF's "response towards ballistic missile attacks" even though North Korea has fired them near Japan for years.

The third norm is based on the tradition of heavy reliance on the United States for national defence. The norm is best articulated in the late diplomat Hisahiko Akazaki's work—*What is Strategic Thought?*—in which he argues that essentially the only "strategy" Japan has is to rely on the United States.[15] This "strategy", consistent with the extended deterrence of the Cold War, has garnered a high level of public support for USFJ. Figure 11.2 shows that Japanese people have always felt "close" to the United States, much more than China, Korea, or Russia. Between 1978 and 2019, around 85% of respondents consistently favoured the combination of the alliance and the SDF for national defence. This reinforces the notion that the Japanese public sees no nation other than the United States as its security partner (Fig. 11.3).

The last norm is the domestic consensus that Japan needs no nuclear weapon of its own as long as the United States extends one through the alliance. The so-called three "non-nuclear" principles of 1967 bans the possession, manufacture, and introduction of nuclear weapons. Despite the oft-rumoured indigenous nuclear weapons capability, the Japanese have firmly rejected weaponisation. The anti-nuclear "allergy" has been firmly embedded in Japanese society. The non-nuclear norm appears to have strengthened after the 2011 triple crisis of earthquake, tsunami, and nuclear meltdown in Fukushima, forcing all civilian-use nuclear reactors to shut down across the Japanese archipelago for some time. Despite facing nuclear neighbours in China, Russia, and North Korea, Japan does not see an imminent need to go nuclear and is unlikely to see one anytime soon. As

[14]Oriki 2012.

[15]Okazaki 1983.

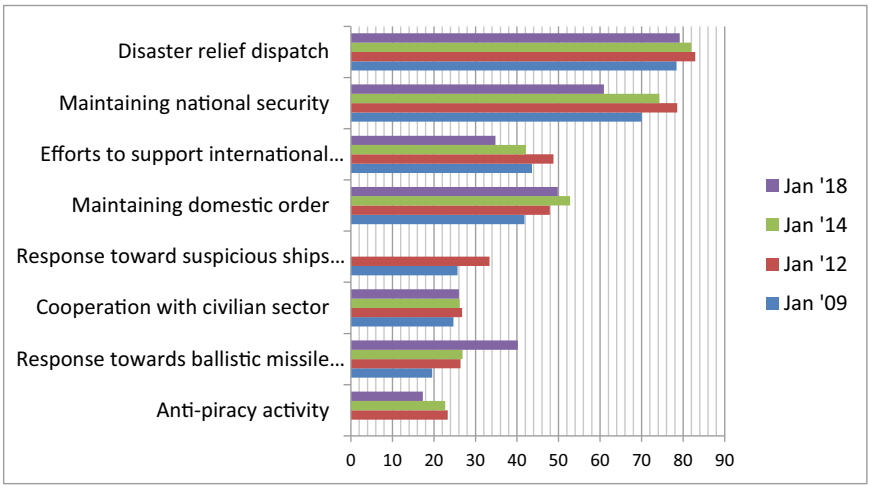

Fig. 11.1 Public expectation of SDF roles (*Source* Public Relations Office (Cabinet Office) (n.d.), p. 7)

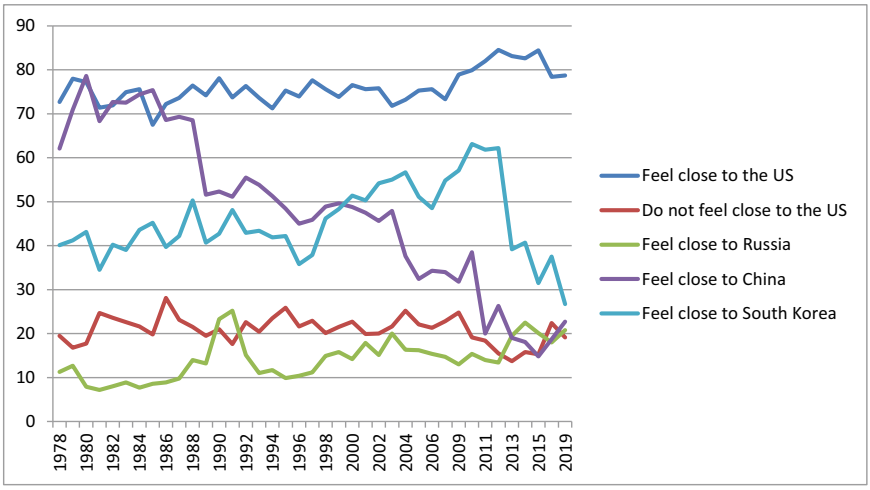

Fig. 11.2 Japanese "feeling close" to the United States and other countries (*Source* Prime Minister's Office 2019)

of April 2020, there is no Diet debate on whether Japan should go nuclear. Scholars indicate potential, but not a single lawmaker is putting forward bills. This makes Japan's deterrence-by-denial posture nuclear-free and largely dependent on conventional and cyber resources.

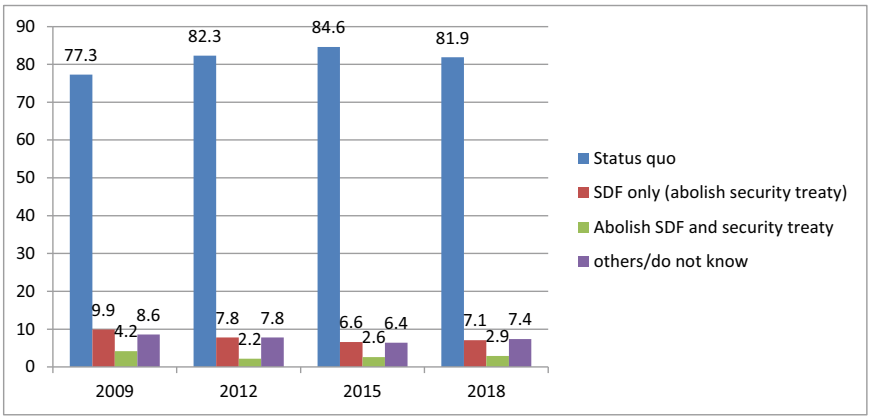

Fig. 11.3 Japanese attitude to SDF and the US alliance (*Source* Prime Minister's Office 2018)

11.4 Japan's Deterrence-by-Denial Posture

Efforts to maintain deterrence-by-denial are sustained by the combination of internal balancing and multilateral hedging with the US alliance at its centre. As part of internal balancing, Japan has increased SDF's operational flexibility by moving portions of ground forces from Hokkaido where it once anticipated Soviet attacks, toward its southwest region to confront the PLA in Japan's airspace and defend administrative control of the Senkaku islands. Japan has checked China's power by strengthening the US alliance and building security ties with partners outside, including with India and Australia. Considerable constraints remain on the use of force in a variety of security laws governing the SDF's functions, which keep Japan in appreciation of extended nuclear deterrence. This is most apparent in the government's approach toward North Korea, which combines the use of diplomatic pressure and economic sanctions designed to contain threats of nuclear weapons and ballistic missiles. Japan resists taking aggressive military missions and continues to use force in a defensive manner.[16] Despite the ongoing negotiation between Kim Jong Un and Donald Trump, the Shinzo Abe government was adamant to press Pyongyang to denuclearize itself and to return alleged Japanese abductees as a condition for rapprochement.

The other part of Japan's deterrence posture is the practice of multilateral hedging with the US alliance at its centre. The inclination toward this alliance is seen, for example, in Prime Minister Abe's determination to stick to the alliance even when things appear problematic. One defining characteristic of Abe's foreign policy was his effort to go along with Trump by making all kinds of concessions on imports of American automobiles and farm products and factory building to make

[16]Abe 2017.

more jobs for American people at the expense of Japanese taxpayers. Japan has also agreed to buy over 100 F-35 jets and several batteries for Aegis Ashore missile defence systems from the United States. Note that few in the Japanese parliament (the Diet) or the media have launched any serious resistance to these measures led by the prime minister's office and these measures were supported loyally by the Ministry of Foreign Affairs. All of this was in stark contrast to other Asian countries like China, which have confronted the United States in the ongoing trade disputes, and South Korea, whose negotiators have refused to meet the US demand to pay more for US troops stationed on Korean soil.

Multilateral hedging boosts the diplomatic aspect of Japan's deterrence-by-denial posture. It revolves around non-US countries, especially India and Australia. The involvement of these key maritime partners is what makes Japan's deterrence posture multilateral in nature. These partners, furthermore, play a part in Japan's strategy of hedging in case the alliance becomes weakened for some unexpected reasons. But the multilateral hedging strategy is nothing new. In fact, Japan began to pay a great deal of diplomatic attention to India during the administration of Prime Minister Taro Aso (2007–2008). Among other achievements he made, Aso promoted ties with India through his trademark "Arc of Freedom and Prosperity", which reinforced shared interests in democracy, freedom, and human rights. Japan and India share a common strategic interest in checking and balancing Chinese power in Asia. For India, China and Pakistan pose a powerful joint challenge because they dispute India's claims over the Kashmir region, and the Belt and Road Initiative challenges its survival and prosperity. Thus India and Japan share a sense of purpose in balancing China and maintaining the freedom of sea-lanes. India and Japan have also secured close ties with Australia (and the United States) through the "democratic security diamond (DSD)". This is critical because Australia has built its own hedging strategy to counter China's influence in the south Pacific. Japan and Australia formed the U.S.-Japan-Australia Trilateral Strategic Dialogue (TSD) in 2002 to deal with threats including North Korea's nuclear weapons and missile programs and China's power through intelligence cooperation and joint exercises.

To deter cyber-attacks, Japan is going cross domain by combining military, cyber, diplomatic, and economic means of statecraft and by making its defence system more robust. One of the best government documents that shows such a development is the 2018 National Defence Program Guidelines (NDPG). In it, the Abe administration contended that Japan considers using conventional, space, and cyber means to retaliate against an armed attack.[17] The cross-domain deterrence posture is progress in the right direction, but it comes with at least two shortcomings. First, it does not address cyber-attacks to retaliate against, therefore doing little to deter foreign cyber attackers. The other problem is that the NDPG falsely assumes that Japan would be *able* to retaliate after absorbing the first strike. Instead, the strategy should assume that the military strike would impair Japan's retaliatory

[17]The Government of Japan 2018, p. 12.

capability in a single blow. There is no denying that the NDPG represents Japan's work in progress. One important difference between cyber deterrence and the hedging strategy, however, is that the cyber dimension is mostly unilateral when the hedging strategy is multilateral by nature. The relatively cautionary stance in cyberspace has much to do with the difficulty of working together with foreign governments because of the inherently deceptive nature of cyberspace operations.

11.5 Conclusion

In this section, the three most important conclusions about Japanese concepts of deterrence will be presented. First, there are both changes and continuities in the Japanese understanding of deterrence over time. On the one hand, throughout the Cold War and today, the meaning of deterrence, denial, and punishment remain the same as that in the Western world, but the strategic and domestic environment has been different. The fundamental stance of Japanese deterrence posture—deterrence-by-denial—survives the changes in Japan's security environment characterized by the threats of Russia, North Korea, and China. This is in large part because the basic political structure of the country characterized by the legal and normative constraints on the use of force remains firmly intact. Furthermore, Japanese concepts of deterrence have continuously been used in the context of US extended deterrence and heavily toned down in terms of intensity to maintain a semblance of defence-by-denial.

Second, there have been some changes. In recent years, we have seen the word used more frequently in government policy, academic publications, and policy discourse. This has coincided with the expansion of this posture into diplomatic spheres. That is, Japan has invested heavily in garnering coalitional support to reinforce its deterrence posture by working closely with its maritime partners, such as India and Australia. At the same time, it is important to keep in mind that these changes are mostly at tactical and operational levels of deterrence and remain subordinate to the political foundation of defence policy that is characterized by the legal and normative constraints on the use of force. All this makes a highly challenging environment for the country to adopt a drastically different approach toward the strategy of deterrence. It also requires strategists in Tokyo to ensure that the current posture is well aligned with the threats they face today.

Finally, this chapter demonstrates that Japanese interpretation of deterrence presents a unique discovery in the practice of deterrence-by-denial and deterrence-by-punishment. While Japanese concepts of deterrence are drawn from the academic contribution of deterrence theorists, the actual application of the concepts is quite different. It is because the policy of deterrence must be exercised in a distinctive political and strategic setting that Japan is in in East Asia. As such, this chapter is designed to contribute to promoting the greater understanding of the *width* of deterrence concepts in the context of a growing diversity in the practice and interpretation of deterrence in global politics.

References

Abe S (2017) Solidarity against the North Korean Threat. The New York Times, 17 September 2017
Christensen T (1999) China, the U.S.-Japan Alliance, and the Security Dilemma in East Asia. International Security 23.4:49–80
Iwata S (2015) Japan's Defence Policy and Deterrence. http://www.nda.ac.jp/cc/gs/results/series/studyseries01.pdf. Accessed: 14 December 2019
Japan Coast Guard (2020) JCG Law. https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=323AC0000000028. Accessed: 27 July 2020
Jervis R (1982) Deterrence and Perception. International Security 7.3 (winter)
Katagiri N (2015) Strategy and Grand Strategy for the Future of Asia. Asian Survey 55.6
Katagiri N (2019) Shinzo Abe's Indo-Pacific Strategy: Japan's Recent Achievement and Future Direction. Asian Security
Mearsheimer J (1985) Conventional Deterrence. Cornell University Press, Ithaca
Morgan P (1983) Deterrence: A Conceptual Analysis. Sage
Oriki R (2012) The Role of Self-Defence Forces (SDF) in Responding to the Great East Japan Earthquake, The Role of the Military in Disaster Relief Operations, NIDS International Symposium on Security Affairs 2011. National Institute for Defence Studies, Tokyo
Okazaki H (1983) 戦略的思考とは何か? [What is Strategic Thought?]. Chuo Koron Shinsha, Tokyo
Oros A (2017) Japan's Security Renaissance: New Politics and Policies for the Twenty-First Century. Columbia University Press, New York
Pastreich E (2015) Interview: Ezra Vogel (29 September 2015). The Diplomat
Prime Minister's Office (2018) 日本の安全を守るための方法 [Means of Protecting Japan's Security]. https://survey.gov-online.go.jp/index-all.html. Accessed: 8 April 2020
Prime Minister's Office (2019) アメリカに対する親近感 [Psychological Distance to the United States]. https://survey.gov-online.go.jp/index-all.html. Accessed: 8 April 2020
Public Relations Office (Cabinet Office) (n.d.) Outline of "Public Opinion Survey on the Self-Defence Forces (SDF) and Defence Issue. http://www.mod.go.jp/e/d_act/others/pdf/public_opinion.pdf, p. 7.
Samuels R (2008) Securing Japan: Tokyo's Grand Strategy and the Future of East Asia. Cornell University Press, Ithaca
Schelling T (1968) Arms and Influence. Yale University Press, New Haven
The Government of Japan (2018) 2018 National Defence Program Guidelines for FY 2019 and Beyond
Ushirogata K (2015) Changes in Deterrence Concepts. Japan Maritime Self-Defence Force Command and Staff College Review 5.2:21–23

Nori Katagiri is Associate Professor of Political Science, Director of International Studies, and Director of Asian Studies at Saint Louis University. Between 2016 and 2018, he was a Visiting Research Fellow at the Air Staff College, Japan Air Self-Defense Force.

Chapter 12
Deterrence (In)stability Between India and Pakistan

Sander Ruben Aarten

Contents

Abstract Since the introduction of India's cold start and Pakistan's full spectrum deterrence doctrines, the subcontinental deterrence landscape has been characterised by strong cross-domain dynamics. In extremis, if both states adhere to the threats issued in their doctrines a Pakistan-supported militant attack on Indian soil could escalate into an all-out nuclear exchange. It is a development that has been met with great concern by many analysts for its detrimental impact on deterrence stability. Since the doctrines are believed to have become operational, at least four incidents occurred which could have sparked this cross-domain escalation spiral. And yet, crisis behaviour proved vastly different from what doctrine predicted. What does this say about deterrence stability on the subcontinent? This chapter assesses deterrence stability on the basis of perfect deterrence theory, which is argued to provide a more nuanced view of deterrence relationships than classical deterrence theory. It finds support for the stability-instability paradox and argues that deterrence is less unstable than appears at first sight. Furthermore, to fully appreciate the degree of deterrence stability, it is suggested that the factors 'context' and 'narrative' should be included into the equation.

S. R. Aarten (✉)
Netherlands Defence Academy, Breda, The Netherlands
e-mail: s.r.aarten@gmail.com

F. Osinga and T. Sweijs (eds.), *NL ARMS Netherlands Annual Review of Military Studies 2020*, NL ARMS, https://doi.org/10.1007/978-94-6265-419-8_12

Keywords Deterrence stability · India · Pakistan · Surgical strikes · Tactical nuclear weapons · cross-domain deterrence · perfect deterrence theory · classical deterrence theory · cold start · full spectrum deterrence · stability-instability paradox · Pathankot · Uri · Pulwama · Gurdaspur

12.1 Introduction

Since their inception, India and Pakistan have been at odds over Jammu and Kashmir, the Himalayan region where both countries' religious and territorial rivalry melt together into a highly flammable cocktail. In their 70-year history both countries have waged four wars (1947, 1965, 1971, 1999), experienced numerous border skirmishes, several military standoffs, and continue to exchange artillery fire across the Line of Control (LoC) regularly. Having been defeated in these wars and having lost Eastern Pakistan in one of them, Pakistan arrived at the conclusion that it could not match India with conventional means. It therefore turned to an asymmetric strategy to "bleed India through a thousand cuts" by supporting anti-Indian militant groups such as Lashkar-e-Taiba (LeT) and Jaish-e-Mohammed (JeM). Operating from behind a veil of plausible deniability, Pakistan has been using Kashmiri insurgent groups as a strategic extension of its own security forces. Since both countries' overt nuclear proliferation in 1998, India faced the daunting challenge of formulating an effective counterterrorism strategy while remaining under Pakistan's nuclear threshold. Frustrated over its inability to deter Pakistan from supporting militant groups inside India, New Delhi devised its assertive *cold start doctrine* which entails limited advances inside Pakistan by rapidly mobilising infantry and armour before Pakistan's defensive positions can be occupied. Cold start may be initiated following insurgent attacks on Indian territory that are believed to be supported by Pakistan.[1]

Even though the feasibility or even the existence of the doctrine remains hotly debated, cold start has taken root in and beyond Pakistan.[2] Pakistani strategic planners believe that the doctrine has been in effect since approximately 2013.[3] In response, Pakistan introduced its *full spectrum deterrence* (FSD) doctrine with the purpose of plugging the gap exploited by cold start. The idea behind FSD is to

[1]Shukla 2017.

[2]See Gady 2019; Ladwig 2007. Cold start is controversial in several ways; partly because of its modalities, but also because some analysts argue that India is presently unable to mount a cold start-like intervention. It is not the purpose of this chapter to delve into the question whether cold start is real or not. This chapter explores the impact of the contemporary deterrence landscape on deterrence stability. A key feature of deterrence is that the reality of a threat is in the eye of the beholder. The fact that Pakistan introduced full spectrum doctrine and tactical nuclear weapons shortly after cold start was believed to have become operational, suggests that it perceives the threat as 'real enough' to respond to it accordingly.

[3]Karl 2015.

provide Pakistan with retaliatory options that are commensurate with the intensity of the aggression it faces by linking conventional means with nuclear options on all levels—from tactical to strategic. A key component of FSD is the introduction of a tactical nuclear weapon (TNW), the Hatf IX 'Nasr' short range ballistic missile with a yield of 0.5 to 5 kilotons. The main purpose of Nasr appears to deter Indian conventional incursions into Pakistani territory as envisaged under cold start.

As a result, the subcontinental deterrence landscape has been characterised by strong cross-domain dynamics. Considering that Pakistan keeps open the option of a nuclear first-use and India adheres to a doctrine of massive retaliation, a Pakistan-supported militant attack on Indian soil could *in extremis* devolve into an all-out nuclear exchange, if both states choose to stick to the threats issued in their doctrines. This development has been met with alarmism by various scholars and analysts, calling the situation on the subcontinent highly unstable.[4] Despite this worrying development, India and Pakistan have experienced several crises which consisted of ingredients that could have sparked the cross-domain escalation spiral. Yet, in recent crises both states decided to react differently. This chapter looks into Indo-Pak crisis behaviour since 2015 to explore why India and Pakistan did not stick to their 'promised' threats and assesses what this means for deterrence stability. The chapter proceeds in three parts. First, the concept of deterrence stability is explained. After that, the course of events surrounding the militant assaults in Gurdaspur, Pathankot, Uri and Pulwama are discussed, followed by an assessment of Indo-Pak deterrence stability in the present situation.

12.2 On Deterrence Stability

To understand the concept of deterrence stability, it is necessary to first gain a basic appreciation of the underlying theoretical principles. The interconnectedness of deterrence dynamics as seen on the subcontinent fits into a stream of deterrence literature that has emerged since the late 2000s to understand this phenomenon of 'cross-domain deterrence' (CDD). CDD looks at escalation paths throughout all levels and realms of conflict. Lindsay and Gartzke define CDD as "the use of threats in one domain, or some combination of different threats, to prevent action in another domain that would change the status quo".[5] Others define it as "the use of capabilities of one type to counter threats or combinations of threats of another type in order to prevent unacceptable attacks".[6] Mallory adds that CDD entails the threat of employing asymmetric tactics to counter an adversary where it is most

[4]Joshi 2016; Jha 2016; Panda 2016a.

[5]Lindsay and Gartzke 2016.

[6]UCSD 2018.

vulnerable.[7] In this chapter, CDD will be understood simply as the use of threats in one domain to deter threats in another.

CDD is not new, but merely a widely-spread manifestation of deterrence in the contemporary security environment. Existing theories of deterrence suffice to a large degree to analyse cross-domain stability, such as perfect deterrence theory (PDT). PDT was developed by Zagare and Kilgour as a refinement of classical deterrence theory (CDT) that continues to pervade in contemporary deterrence literature.[8] In line with structural realism, classical deterrence theorists (including Jervis, Morgenthau, Waltz) see a positive monotonic relationship between balance of power and peace.[9] According to this theory, symmetry fosters stability and asymmetry leads to instability and crisis. CDT has a tendency towards overkill capabilities (cf. large nuclear stockpiles of the Cold War) because it maintains that prohibitively high costs of war are the best guarantor for deterrence stability.

PDT, like CDT, takes the cost of war as a key element for determining the degree of deterrence stability between two actors: the higher the costs the less likely an actor is going to take action first. However, unlike CDT, PDT relates the cost-benefit-calculus to an actor's satisfaction with the status quo. Furthermore, it challenges CDT's tendency towards overkill capacities by claiming that there is a minimum and maximum threshold to threat effectiveness. It recognises that a quantitative minimum is necessary to convey the threat (e.g. one nuclear weapon has limited deterrent value because it may disfunction or be taken out before its actual use), but also that inflation kicks in at some point (e.g. the added destructive threat of 50.000 vs. 10.000 nuclear weapons is relatively limited).[10] Lastly, there is a difference in the axiomatic basis. CDT assumes that conflict is always the worst possible outcome of any deterrence relationship and therefore assumes that actors have a tendency not to execute threats when challenged by the adversary. This axiom that adversaries always want to avoid conflict is logically inconsistent because it means that adversaries would never want to execute their promised threats if push came to shove.

However, if you prefer not to execute your threat, then how credible is your threat anyway? The presumption that adversaries perceive conflict as the least favourable outcome, implies a presumption that actors are not committed to their threats—which is contradictory with the entire aim of deterrence to manipulate the opponent's behaviour through the use of threats. PDT, on the other hand, argues that, depending on the subject of contestation, the adversary's 'win' could be a worse outcome than conflict. It argues that adversaries *probably* prefer to execute their promised threats. After all, for actors that are dissatisfied with the status quo, it is not unthinkable to prefer conflict to backing down.[11]

[7]Mallory 2018, p. 1.

[8]Zagare and Kilgour 2000.

[9]See Jervis 1979; Morgenthau 1948; Waltz 1979, 1981.

[10]Zagare 2004, p. 128.

[11]Quackenbusch 2006, p. 534.

Table 12.1 Differences between classical and perfect deterrence theory on the assessment of deterrence stability

Classical deterrence theory	Perfect deterrence theory
Presumptions	
Monotonic positive relationship between cost of war and prevalence of peace	Positive relationship between cost of war and prevalence of peace, although threats have minimal and maximum thresholds
Actors prefer not to execute their threats (conflict is the least-preferred outcome)	Actors *probably* prefer to execute a threat (adversary's 'win' is the least-preferred outcome)
Threats are implicitly assumed incredible	Threats are assumed as credible
Stability	
Cost of war calculus	Cost of war calculus
Parity/symmetry	Highly valued status quo
	Highly credible threats
	No incentive to execute threat in one domain to deter threats in another

(*Source* The author)

Table 12.1 captures the differences between CDT and PDT concerning the issue of stability. Deterrence is stable when the deterring actors have no incentive to initiate attack. Mutually subjective interpretations of the cost of war are central to assessing the stability in a deterrence relationship. Deterrence stability is often explained as resulting from a balance of terror, or parity, which Schelling usefully explained as follows: "[if] two powers show themselves equally capable of inflicting damage upon each other by some particular process of war, so that neither gains an advantage from its adoption and both suffer the most hideous reciprocal injuries, it is not only possible but it seems probable that neither will employ that means."[12] This idea that deterrence stability accrues from parity and the equal capability to inflict prohibitively high costs, befits classical deterrence theory.

Instability, however, is more likely to be caused by dissatisfaction than asymmetry. According to PDT, it is perfectly possible that instability emerges under conditions of power parity or even an asymmetric distribution of power that is unfavourable to the challenger. The higher the level of dissatisfaction with the status quo, the higher the costs of war an actor is willing to accept, the less stable it is. Still, a shortcoming of both PDT and CDT is that they tend to treat deterrence domains in isolation from each other. To analyse deterrence stability in cross-domain contexts it would be useful to add that stability is upheld when there is no incentive to execute a threat in one domain that may escalate to another domain.

Deterrence is stable when the actors involved feel that there is little to be gained from striking first; when the expected benefits are smaller than the expected costs. It is a matter of cost equivalence that works like a system of communicating vessels. Offsetting capabilities, such as new technologies, may affect deterrence stability.

[12]Schelling 2008, p. 19.

However, new technologies are worthless if they are not put to effective use. This is where doctrine comes in. Doctrine dictates best-practices of how to act in a given situation. India's cold start doctrine and Pakistan's full spectrum deterrence doctrine have tied together all domains and levels of conflict, leading many analysts and scholars to call the Indo-Pakistani deterrence relationship highly unstable. The next section addresses crisis behaviour during four events that occurred within the context of the contemporary deterrence landscape. These events serve as a basis to analyse the degree of instability in the contemporary Indo-Pak deterrence relationship.[13]

12.3 Events Since 2015

By and large, cold start and full spectrum deterrence came in effect in 2013. Since then, no major events emerged which could have triggered a crisis in Indo-Pak relations—until 2015. On 27 July, a cell of three LeT-militants attacked a police station in the Punjabi town of Gurdaspur, killing six civilians and one policeman. The militants were reportedly on their way to Pathankot air force base but diverted as dawn was fast approaching.[14] The attack took place only days after the prime ministers of India and Pakistan agreed to formally resume peace talks. Apart from a warning by Home Minister Singh that Islamabad should be ready for a befitting reply, the event did not escalate into a crisis.[15] Later that year Modi and Sharif met on the sidelines of the Paris climate conference, and on Christmas Day Modi paid a surprise birthday visit to Nawaz Sharif in Lahore.[16] The emerging thaw in Indo-Pak relations happened in the midst of an intensification of Indian development assistance to Afghanistan.[17] However, one week after Modi's visit to Lahore, on 2 January 2016, six militants assaulted Pathankot airbase, killing ten Indian army personnel. The attack was claimed by the United Jihad Council (UJC), a coalition of anti-Indian Kashmiri militant groups. New Delhi, sceptical about the claim because the UJC has no history of mounting attacks outside of Kashmir, suspected the involvement of LeT or JeM. A series of militant attacks on Indian diplomatic missions in Afghanistan the following two days indicates a degree of coordination that suggests the involvement of a state actor such as Pakistan's ISI, who were

[13]Joshi 2016; Jha 2016; Panda 2016a.

[14]Pendleton 2016, p. 6.

[15]India Today 2015a.

[16]India Today 2015b.

[17]India constructed Afghanistan's new Parliament Building and delivered several Mi-25 attack helicopters to the Afghan Air Force.

unhappy with the political developments.[18] India and Pakistan jointly agreed to postpone the agreed upon diplomatic talks.[19]

A few months later, on 18 September 2016, four members of JeM attacked a military camp near Uri killing 18 Indian soldiers—the highest casualty number in 20 years at that moment.[20] The attack took place three days before Nawaz Sharif addressed the UN General Assembly in which he asked the international community to speak out against Indian human rights violations and to support Kashmiri self-determination. A month before Sharif's speech, Modi gave prominent mention of Pakistan's restive Baluchistan, promising asylum to Baluch separatist leaders during his Independence Day speech. The Uri attack also happened in the midst of a spate of unrest in Indian administered Kashmir. The unrest followed the death of Burhan Wani, the 22-year old leader of an anti-Indian militant group, who was killed in a counterinsurgency operation in July that year. In a public address following the Uri attack, Modi warned Pakistan's leadership that "[…] the sacrifice of our 18 jawans will not go in vain" and promised to isolate Pakistan diplomatically.[21] India scored a diplomatic success when the SAARC summit, which was to be held in Islamabad in November that year, was cancelled after Afghanistan, Bangladesh, Bhutan, Sri Lanka and the Maldives decided not to show up (Panda 2016b). Similarly, the Crown Prince of Abu Dhabi, a country with which Pakistan maintains friendly ties, accepted an invitation to be the principal guest at the 2017 Indian Republic Day Parade.[22] China, Pakistan's 'all weather friend' reportedly indicated that it preferred a change in Pakistan's regional policies. Furthermore, Pakistan's civilian government urged the military leadership to "seek consensus on several key actions" in order to avoid further international isolation.[23] These reports suggest that the Indian effort to isolate Pakistan diplomatically have been relatively successful at the tactical level at least.

Apart from India's diplomatic efforts, the Indian army conducted 'surgical strikes' on the Pakistani side of the LoC. The strikes were not 'surgical' in the Western sense which conceptualises it as the use of precision-guided missiles with limited collateral damage.[24] A more adequate description would be 'raid' or 'SOF operation'.[25] While rare, surgical strikes are not particularly new. Due to the covert character of such operations, it is difficult to determine how many have taken place. According to some sources at least three such cross-border raids have been

[18]Sehmer 2016.
[19]BBC 2016.
[20]Snow 2016.
[21]Economic Times 2016.
[22]Kuchay 2019.
[23]Almeida 2016.
[24]Barriot and Bismuth 2008, p. 6.
[25]Gokhale 2017.

conducted during the Singh-administration.[26] Under the Modi administration, such strikes had been conducted at least once before when Indian forces crossed into Myanmar territory to attack an insurgent camp following a series of attacks in the Indian states of Nagaland and Manipur. What is different between then and now, is the publicity that surrounds these operations. Before the strikes were conducted, India is believed to have received tacit approval from the US.[27] According to New Delhi significant casualties were inflicted on the terrorists and their supporters. Islamabad, however, flatly denied that commandos crossed into its territory.

In the aftermath of the surgical strikes, cross-LoC skirmished intensified and ultimately led both sides to agree to truce in May 2018.[28] In the meantime, popular unrest in Indian-administered Kashmir remained high. In the winter of 2019, on 14 February, Adil Ahmad Darhad, an Indian national from Kashmir drove his explosive-laden car into a convoy of the Central Reserve Police Force on the Srinagar-Jammu highway, killing 44 policemen and injuring 70. The attack was claimed by JeM, which had inspired and supported the perpetrator to carry out the attack. Modi declared that India "[…] will give a befitting reply; our neighbour will not be allowed to destabilise us […] our security forces are given full freedom".[29] Similar to the Uri aftermath, India sought to isolate Pakistan diplomatically. As with any terrorist attack on Indian soil, Pakistani leaders condemned it and denied involvement. Similarly, as in previous major crises, India recalled its ambassador from Pakistan (Pakistan followed suit), revoked its MFN-status and suspended cross-border bus and train services. In addition to that, customs duties were increased with 200%, threats were made to stop the water flow to Pakistan as guaranteed under the Indus Water Treaty, and the state government of Jammu and Kashmir withdrew the security of separatist leaders.

The crisis turned kinetic as both armies traded fire along the LoC in late February. A Pakistan Army spokesperson claimed that "[Pakistan] shall dominate the escalation ladder" and gave reference to crisis meetings of the National Command Authority, which oversees Pakistan's nuclear arsenal.[30,31] As anti-Pakistan demonstrations were held across India, and keeping in mind that Indian elections would take place only weeks later, Modi may have felt the urge to act. In the early morning of 26 February, a squadron of IAF Mirage 2000s conducted airstrikes on JeM-training centres near the town of Balakot in Pakistan's Khyber-Pakhtunkhwa. It was the first time since 1971 that Indian fighters conducted an airstrike on undisputed Pakistani soil (i.e. outside of Kashmir). Pakistan responded by closing its airspace for Indian airliners and positioning tanks along the LoC in the Sialkot sector, close to the city of Jammu. It also retaliated by sending

[26]India Today 2016.
[27]Chaudhury 2018.
[28]Abi-Habib and Kumar 2018.
[29]Abi-Habib et al. 2019.
[30]ISPR 2019.
[31]Miller 2019.

JF-17s and F-16s into Indian administered Kashmir the next day. In the ensuing air battle at least one Indian MiG-21 was downed on the Pakistani side of the LoC and the pilot was taken prisoner. The following day, on 28 February, Prime Minister Imran Khan warned the Indian leadership in a televised public address about the nuclear capabilities that both countries have and called on India to show restraint and proposed to restart talks.[32] The next day Pakistan released the Indian pilot as a "gesture of peace".[33] Early March Pakistan started a crackdown against Islamist groups, detaining more than 100 individuals and putting nearly 200 madrassas under control. Around the same time the international train, the Samjhauta Express, resumed service and Indian general elections were held which Modi's BJP-party won in a landslide. In July Pakistan fully reopened its airspace to Indian companies and both ambassadors were back at their posts.

12.4 Assessment

All of the aforementioned crises were claimed or suspected to be conducted by Pakistan-supported groups. The events show a stark discrepancy between theory and practice, as is illustrated in Fig. 12.1. The doctrinally predicted escalation spiral was not set in motion even though the ingredients of its commencement—a Pakistan-supported terrorist attack on Indian soil—were present. Gurdaspur, Pathankot, Uri and Pulwama proved insufficient to trigger a cold start-like response. Following Gurdaspur and Pathankot India decided not to escalate the event into crisis, probably for want of giving the new Indo-Pak rapprochement a chance.[34] However, the cumulative pressure of these attacks combined with domestic outcry over the high number of Indian casualties in the Uri and Pulwama attacks have provoked an unprecedented reaction in New Delhi. These crises demonstrated that there is more room for conventional escalation below the nuclear threshold than doctrine predicted.

What does this say about deterrence stability when applying the stability indicators of perfect deterrence theory? It is clear that, while India is geographically relatively content with the present situation, Pakistan is displeased with the status quo in Kashmir. However, this discontentment may not automatically translate into a broadly shared vision that open conflict with India could be a cost-acceptable (or: beneficial) endeavour. A large conflict with India, which might involve nuclear first use on the part of Pakistan, would arguably leave it worse off than in the already dire present situation. Pakistan's economy is in a shambles and its relations with western countries, including the US, has been decaying over the past few years. If it

[32]Safi and Zahra-Malik 2019a.

[33]Safi and Zahra-Malik 2019b.

[34]Lalwani and Haegeland 2018 have given an excellent account of why one event escalates to the level of crisis in Indo-Pakistani relations, while others do not.

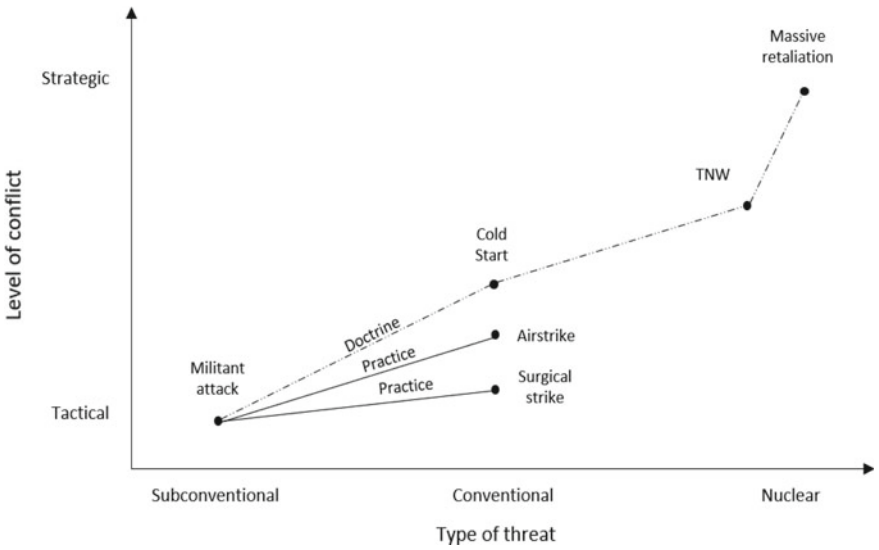

Fig. 12.1 Contemporary cross-domain deterrence dynamics in the Indo-Pak deterrence environment (*Source* The author)

initiated a nuclear first strike, as per full-spectrum deterrence in response to cold start, it may well be portrayed as an international pariah state, which makes the status quo arguably better than a 'post-TNW status quo'. In terms of threat credibility, it appears that both countries take each other's doctrines seriously. After all, despite doubts about whether India can pull off a cold start-like intervention, Pakistan took it seriously enough to come up with full-spectrum deterrence.

The fact that India regularly conducts military exercises under cold start-like conditions,[35] give further credence to this notion. We cannot be sure that India did not carry out a cold start-scripted limited air-land intervention inside Pakistani territory out of fear of crossing the nuclear threshold. But the fact that New Delhi opted for alternative ways to retaliate conventionally despite having trained formations along the Pakistani border supports the argument that Pakistan's deterrent was successful in shaping India's retaliatory response. By not operationalising cold start and TNWs the threat of nuclear escalation remained remote. Pulwama and Uri were also novel in that here was very little nuclear signalling, unlike during Kargil and the 2001–2002 Twin Peaks crisis (when India did not have a cold start doctrine up its sleeve to counter terror "attacks"). This could be either because both sides sought to steer clear from using any nuclear escalatory language in order to prevent raising tensions even further, or because the adversaries believed that the conditions

[35]Examples of these exercises include *Sindu Sudarshan-VII* (November 2019), *Vijay Prahar* (May 2018), *Mamesha Vijayee* (December 2017), *Thar Shakti* (May 2017), *Chakravyuh-II* (May 2016), *Shatrujeet* (April 2016).

for a nuclear escalation were not present. The rapid pace of escalation following Pulwama may have deterred Pakistan from stepping up the ante. If this is true, then escalation had a de-escalatory effect.

The cost of war in the nuclear realm is thus perceived as high by both India and Pakistan. These explanations all argue in favour of a degree of stability in the nuclear realm. While there are clear incentives to avoid the initiation of a threat (e.g. limited incursion inside Pakistani territory) that could lead to escalation into the nuclear realm, this incentive appears largely absent in the conventional and sub-conventional domains. Considering the ongoing insurgent attacks by organisations such as LeT and JeM, Pakistan continues to see benefit in supporting these proxies against India. New Delhi's quest to seek ways to punish and deter Pakistan-supported insurgencies, manifests in various counter-efforts below the nuclear threshold of which the surgical strikes and airstrikes are the most recent examples. This is supportive of the stability-instability paradox which holds that "despite increased tensions and severe crises, nuclear-armed adversaries will avoid a major conflict or a nuclear exchange".[36] While nuclear weapons put a cap on the risk of escalation to large scale conflict that may escalate into the nuclear realm, interstate competition shifts and intensifies on the sub-nuclear levels allowing for more low-intensity conflicts.[37]

12.5 Context and Narrative

The question, then, is: how unstable are the sub-nuclear realms? Context and narratives are important aspects to look into. As for context, India and Pakistan have been at odds over Kashmir for as long as they exist. Despite a 2003 ceasefire agreement, cross-LoC incursions of militants as well as cross-LoC shootings which include artillery shelling, have remained persistent to the present day.[38] In that context, surgical strikes may appear less destabilising than at first sight might be expected, especially because surgical strikes have been conducted under previous administrations too. The covert character, however, made that little to no information about these operations was disclosed to the public. The Indian government's overtness surrounding these strikes deviated from the norm, but was primarily intended to appease a domestic public that had grown increasingly disconcerted with the restrictive manner in which the hawkish Modi administration had acted in the previous two events (cf. no punishment following Gurdaspur and Pathankot).[39] In going overt with the surgical strikes, India failed to give incontrovertible proof of the raids' effect. Whether this was intentional or not, it allowed Pakistan to simply

[36]Krepon 2004, p. 2.
[37]Rauchhaus 2009.
[38]Jacob 2017.
[39]Haidar 2016.

deny the surgical strikes from having taken place, 'saving' its face and not having a reason to escalate the event.

The airstrikes following the Pulwama attack were a clear break with the past. For the first time in almost 50 years the IAF operated outside the Kashmiri theatre inside uncontested Pakistani territory. Moreover, escalation followed an attack that was unique in that it was JeM-supported but performed by an Indian national who had procured the explosives locally.[40] The fact that the attack was conducted by an Indian national may have made the justification of a cold start-like intervention less obvious, but it is nonetheless a development that raises concern for at least two reasons. First, it suggests that Indian administered Kashmir has an ecosystem of its own that breeds militancy, and second, it shows that attacks claimed by Pakistan-supported groups but carried out by Indian nationals would suffice to reply with the type of response as we have seen in February 2019. However, when zooming in on the narratives surrounding the airstrikes one notes a degree of de-escalatory parlance within the larger escalatory context. India called its airstrikes 'preventive' in nature and directed against 'non-military targets', while Pakistan claimed that its warplanes intentionally decided to strike uninhabited areas rather than military installations 'to send a message' and 'to avoid human loss and collateral damage'.[41] Another break with the past was Pakistan's de-escalatory behaviour. PM Khan, who can ill-afford armed conflict due to Pakistan's economic hardship and his electoral promise to establish an Islamic welfare state, urged for restraint throughout the Pulwama crisis. The limited damage that both strikes incurred, the de-escalatory parlance that both adversaries used during the airstrikes and Khan's outreach to Modi to resume talks signal that both states had little interest in escalating the conflict any further.

12.6 Conclusion

Thankfully, doctrine has proven to be a poor predictor of crisis behaviour in practice on the subcontinent. It was wrong in at least two ways. First, the cross-domain escalation spiral was not set in motion despite the occurrence of events which could have triggered it. Second, India showed that there is more room for conventional escalation than was previously assumed. This may partially be because both countries consider their respective doctrinal threats as real and credible. Certainly in the nuclear realm, the cost of war is perceived as high. The events since 2015 demonstrate that there is a shared reluctance by both sides to escalate to the nuclear realm. Efforts to offset each other are concentrated in practice on the conventional and sub-conventional realms. This is an indication that the nuclear realm is more stable than the sub-nuclear realm and demonstrates that there

[40] Abi-Habib et al. 2019.

[41] Regan and Kumar 2019.

is a clear stability-instability paradox at play. Furthermore, it could be argued that the status quo may be valued more by both sides, including Pakistan, than one might suggest. These findings all indicate that deterrence is less unstable than is assumed by many analysts and scholars.

In assessing the degree of instability in the sub-nuclear realms, it is important to take note of the strategic context and narratives that surround crisis behaviour. Surgical strikes did not deviate much from the traditional modus operandi across the LoC. While the airstrikes proved a break with the past that gives reason for concern, there was a lot of signalling that both sides were not intent on letting the situation escalate beyond limited actions. Of course, signalling commitment to not let things spiral out of control is hardly a guarantor that escalation will be limited to a certain level. As soon as conflicts erupt, events may lead a life of their own, causing a conflict to escalate to unintended larger proportions. Nonetheless, a closer look at Indo-Pak crisis behaviour showed that there are more escalation dampening mechanisms at play than appears at face value.

It is always easy to make ex post assessments. Assessments of the past may not be a confident predictor of future crisis behaviour. The Indo-Pak deterrence environment is volatile. Efforts to offset each other's capabilities may overthrow the status quo, which may or may not be nefarious to deterrence stability. The airstrikes are currently a one-off (n = 1) event and it is too early to tell whether this is exemplary for future crisis behaviour. However, considering that Pakistan has a particular interest in avoiding a conventional confrontation with India, Pakistan may well seek to plug the deterrence gap that India exploited. As India continues to seek ways to deter terrorist attacks, Pakistan may revise full spectrum deterrence in such a way that it creates an option for nuclear use after any conventional strike inside its territory. As Pakistani Lieutenant-General Tariq Khan said: "Our response should be to escalate and push the envelope of hostilities so that nuclear war is a likely outcome" on the expectation that India "simply will not go down this road" because it has more to lose.[42] If this is the case, then the threshold for nuclear escalation is lowered and the competition in risk-taking is brought to a new level again. The question is how both states will react in the next crisis. The modalities of the deterrence landscape may change profoundly as both states introduce new weapons technology and doctrines. While volatility is not the same as instability, volatility goes hand in hand with unpredictability and may be a prelude for instability following near-future changes. New weapons technology and doctrine alone, however, are not enough to make a balanced assessment of deterrence stability—these are enablers of new escalation trajectories. In making sound assessments of deterrence stability, it is at least as import to look into the strategic context and intent or propensity towards escalation as expressed through crisis narratives and actor satisfaction with the status quo, as per perfect deterrence theory.

[42]Swami 2019.

References

Abi-Habib M, Kumar H (2018) India and Pakistan agree to truce on Kashmir Border. New York Times. https://www.nytimes.com/2018/05/30/world/asia/india-pakistan-kashmir-truce.html. Accessed 22 March 2020

Abi-Habib M, Yasir S, Kumar H (2019) India Blames Pakistan for Attack in Kashmir, Promising a Response. New York Times. https://www.nytimes.com/2019/02/15/world/asia/kashmir-attack-pulwama.html. Accessed 30 December 2019

Almeida C (2016) Exclusive: Act against militants or face international isolation, civilians tell military. Dawn. https://www.dawn.com/news/1288350. Accessed 30 December 2019

Barriot C, Bismuth P (2008) Treating Victims of Weapons of Mass Destruction. Wiley, Chichester

BBC (2016) Pathankot attacks: Pakistan, India reschedule peace talks. BBC. https://www.bbc.com/news/world-asia-india-35309559. Accessed 30 December 2019

Chaudhury R C (2018) Surgical strikes: India is said to have kept America in the loop. The Economic Times. https://economictimes.indiatimes.com/news/defence/surgical-strikes-india-is-said-to-have-kept-america-in-the-loop/articleshow/54593827.cms?from=mdr. Accessed 30 December 2019

Economic Times (2016) PM Modi warns Pakistan: Uri attack will not be forgotten. The Economic Times. https://economictimes.indiatimes.com/news/politics-and-nation/pm-modi-warns-pakistan-uri-attack-will-not-be-forgotten/articleshow/54502715.cms?from=mdr. Accessed 30 December 2019

Gady F (2019) Is the Indian military capable of executing the Cold Start doctrine? The Diplomat. https://thediplomat.com/2019/01/is-the-indian-military-capable-of-executing-the-cold-start-doctrine/. Accessed 31 December 2019

Gokhale N A (2017) The Inside Story of India's 2016 'Surgical Strikes'. The Diplomat. https://thediplomat.com/2017/09/the-inside-story-of-indias-2016-surgical-strikes/. Accessed 25 March 2018

Haidar S (2016) Earlier cross-LoC strikes had different goals: former NSA. The Hindu. https://www.thehindu.com/news/national/Earlier-cross-LoC-strikes-had-different-goals-former-NSA/article15893710.ece

India Today (2015a) Gurdaspur attackers came from Pakistan, says Rajnath. India Today. https://www.indiatoday.in/india/story/gurdaspur-attackers-came-from-pakistan-says-home-minister-rajnath-singh-285513-2015-07-30. Accessed 31 December 2019

India Today (2015b) Modi's Christmas surprise: A quick stopover in Lahore to wish Happy Birthday to PM Nawaz Sharif. India Today. https://www.indiatoday.in/india/delhi/story/modi-to-meet-pakistan-pm-nawaz-sharif-in-lahore-278927-2015-12-25. Accessed 30 December 2019

India Today (2016) 4 Times Indian commandos crossed the LoC for surgical strikes: all you need to know. India Today. https://www.indiatoday.in/india/story/four-times-india-carried-out-surgical-strikes-345715-2016-10-09. Accessed 3 June 2018

ISPR (2019) Twitter post, 22 February 2019, 02:06h. https://twitter.com/OfficialDGISPR/status/1098886660354383872. Accessed 29 February 2020

Jacob H (2017) Ceasefire violations in Jammu and Kashmir: A line of Fire. United States Institute of Peace, Washington DC. https://www.usip.org/sites/default/files/PW131-Ceasefire-Violations-in-Jammu-and-Kashmir-A-Line-on-Fire.pdf. Accessed 30 December 2019

Jervis R (1979) Deterrence theory revisited. World Politics 31:289-324

Jha P (2016) Uri attack: Is India getting impatient with Delhi's strategic restraint? Hindustan Times. https://www.hindustantimes.com/india-news/why-india-is-getting-impatient-with-delhi-s-strategic-restraint/story-MutvAqKiAXWWdP8GbEdf4K.html. Accessed 11 January 2019

Joshi M (2016) Uri Attack: There Are No Military Options That Will Give India the Outcome It Wants. The Wire. https://thewire.in/diplomacy/uri-india-military-options-terror-pakistan. Accessed 11 January 2020

Karl D J (2015) India, Pakistan, and the Limits of Effective Deterrence. The Diplomat. http://thediplomat.com/2015/06/india-pakistan-and-the-limits-of-effective-deterrence/. Accessed 1 May 2016

Krepon M (2004) The Stability-Instability Paradox, Misperception, and Escalation Control. In: Krepon M, Jones R W, Haider Z (eds) South Asia, Escalation Control and the Nuclear Option in South Asia. Stimson Center, Washington DC

Kuchay B (2019) Why have Saudi Arabia, UAE failed to condemn India over Kashmir? (12 September 2019) Al Jazeera. https://www.aljazeera.com/news/2019/09/saudi-arabia-uae-failed-condemn-india-kashmir-190911112648176.html. Accessed 30 December 2019

Ladwig W C (2007) A Cold Start for Hot Wars? The Indian Army's New Limited War Doctrine. International Security 32:158–190

Lalwani S, Haegeland H (2018) Anatomy of a crisis: Explaining crisis onset in India-Pakistan relations. In: Lalwani S, Haegeland H (eds) Investigating Crises: South Asia's Lessons, Evolving Dynamics, and Trajectories. Stimson Center, Washington DC, pp 23–56

Lindsay J R, Gartzke E (2016) Cross-domain deterrence as a practical problem and a theoretical concept. http://deterrence.ucsd.edu/_files/CDD_Intro_v2.pdf. Accessed 29 February 2020

Mallory K (2018) New Challenges in Cross-Domain Deterrence. Rand Corporation, Washington DC

Miller L (2019) Calming India and Pakistan's Tit-for-Tat Escalation. International Crisis Group. https://d2071andvip0wj.cloudfront.net/1-mar-19-india-pakistan.pdf. Accessed 21 December 2019

Morgenthau H (1948) Politics among nations. Knopf, New York

Panda A (2016a) Gurdaspur, Pathankot, and Now Uri: What Are India's Options? The Diplomat. https://thediplomat.com/2016/09/gurdaspur-pathankot-and-now-uri-what-are-indias-options/. Accessed 11 January 2020

Panda A (2016b) SAARC Summit cancellation will sting Pakistan but won't prevent the next Uri or Pathankot. The Diplomat. https://thediplomat.com/2016/09/saarc-summit-cancellation-will-sting-pakistan-but-wont-prevent-the-next-uri-or-pathankot/. Accessed 30 December 2019

Pendleton H D (2016) Pathankot, India, Airbase Attack. TRADOC G-2 ACE Threats Integration

Quackenbusch S L (2006) National Missile Defense and Deterrence. Political Research Quarterly 59:533–541

Rauchhaus R (2009) Evaluating the Nuclear Peace Hypothesis - A Quantitative Approach. Journal of Conflict Resolution 53:258–277

Regan H, Kumar N (2019) Pakistan says it shot down two Indian jets as Kashmir border crisis deepens. CNN. https://edition.cnn.com/2019/02/27/india/india-pakistan-strikes-escalation-intl/index.html. Accessed 11 January 2020

Safi M, Zahra-Malik M (2019a) India demands safe return of pilot shot down by Pakistan over Kashmir. The Guardian. https://www.theguardian.com/world/2019/feb/27/pakistan-pm-imran-khan-appeals-talks-india-war-kashmir. Accessed 30 December 2019

Safi M, Zahra-Malik M (2019b) Pakistan returns Indian pilot shot down over Kashmir in 'peace gesture'. The Guardian. https://www.theguardian.com/world/2019/mar/01/pakistan-hands-back-indian-pilot-shot-down-over-kashmir-in-peace-gesture. Accessed 31 December 2019

Schelling T C (2008) Arms and influence. Yale University Press, New Haven

Sehmer A (2016) Pakistan: JeM Leader Kept Off UN Sanctions List. Terrorism Monitor 14:8. https://www.refworld.org/docid/5724df404.html. Accessed 30 December 2019

Shukla A (2017) Why General Bipin Rawat Acknowledged the Cold Start Doctrine. The Wire (20 January 2017). https://thewire.in/diplomacy/cold-start-pakistan-doctrine. Accessed 3 November 2019

Snow S (2016) 17 Indian Soldiers Killed in Kashmir: India-Pakistan Tensions Heating up. The Diplomat. https://thediplomat.com/2016/09/17-indian-soldiers-killed-in-kashmir-india-pakistan-tensions-heating-up/. Accessed 30 December 2019

Swami P (2019) Pakistan likely to be in two minds to retaliate after IAF airstrikes, India can ill-afford to lower its guard. Firstpost. https://www.firstpost.com/india/pakistan-likely-to-be-in-

two-minds-to-retaliate-after-iaf-airstrikes-india-can-ill-afford-to-lower-its-guard-6156621.html. Accessed 1 March 2020
UCSD (2018) Cross-Domain Deterrence. University of California, San Diego. http://deterrence.ucsd.edu/. Accessed 29 February 2020
Waltz K N (1979) Theory of International Politics. Random House, New York
Waltz K N (1981) The Spread of Nuclear Weapons: More May Be Better. The Adelphi Papers 21:171
Zagare F C (2004) Reconciling rationality with deterrence: A re-examination of the logical foundations of deterrence theory. Journal of Theoretical Politics 16:107–141
Zagare F C, Kilgour M D (2000) Perfect Deterrence. Cambridge University Press, Cambridge

Sander Ruben Aarten (MA) is senior policy officer at the Netherlands Defence College. He holds a master's in political science (magna cum laude) from Brussels Free University as well as a master's in strategic studies (cum laude) from the Netherlands Defence Academy. He is currently conducting Ph.D. research on deterrence and strategic stability at the Netherlands Defence Academy.

Chapter 13
Iran's Syria Strategy: The Evolution of Deterrence

Hassan Ahmadian and Payam Mohseni

Contents

Abstract Iran has been a critical player in the Syrian war since 2011, crafting a complex foreign policy and military strategy to preserve its Syrian ally. What have been the drivers of Iranian decision-making in this conflict? And how has Iranian strategy evolved over the course of the war? This chapter argues that the logic of deterrence has been fundamental not just for shaping the contours of Iran–Syria

This chapter is a revised reprint of Hassan Ahmadian and Payam Mohseni, Iran's Syria strategy: the evolution of deterrence, International Affairs 95: 2 (2019) 341–364. Reprinted with permission.

H. Ahmadian (✉)
Harvard Kennedy School, Belfer Center for Science and International Affairs, Cambridge, MA, USA
e-mail: Hassan_Ahmadian@hks.harvard.edu

H. Ahmadian
The Center for Strategic Research, University of Tehra, Tehran, Iran

P. Mohseni
Department of Government, Harvard University, Cambridge, MA, USA

F. Osinga and T. Sweijs (eds.), *NL ARMS Netherlands Annual Review of Military Studies 2020*, NL ARMS, https://doi.org/10.1007/978-94-6265-419-8_13

relations since the Islamic Revolution of 1979, but also for determining the overall trajectory of Iranian strategy in the Syrian war. The authors outline Iran's decision-making calculus and divide the country's strategy on Syria after the Arab Spring into four primary phases: (1) a 'Basij' strategy to establish local militias in Syria; (2) a regionalization strategy to incorporate transnational fighters and militias in the war effort; (3) an internationalization strategy to incorporate Russia and balance the United States; and (4) a post-ISIS deterrence strategy to balance against the United States, Turkey and Israel. Iran's Syria strategy progressively escalated in response to the possible defeat of its ally and the deterioration of its forward deterrence capacities against the United States and Israel. Today, the potential for direct inter-state conflict is rising as proxy warfare declines and Iran attempts to maintain the credibility of its forward deterrence.

Keywords proxy · Hezbollah · regionalization · internationalization · ISIS · Islamic Revolution · balancing

13.1 Introduction

Syria today stands at the crossroads of regional and international geopolitical currents. The Arab uprisings of 2010–11 and the ensuing instability that shook the Syrian regime have created a strategic battleground for regional dominance and Great Power contestation.[1] In the seventh year of the war, the conflict shows no sign of drawing to an end, but instead has entered a new stage. This phase is seeing a shift away from proxy war and an increasing risk of direct interstate clashes, with a real possibility of confrontations involving Israel, Iran, Turkey, Russia and the United States.

The partnership between Syria and Iran stretches back over four decades, and the bond between these two very different states raises an important research question for the field. What is propelling this enduring alliance in a region known for its dizzying array of constantly shifting partnerships? Many initially believed the alliance would be short-lived, tied as it had been to exigencies facing Iran and Syria during the Iran–Iraq War,[2] or that it would not be strategically significant or durable owing to 'underlying incompatibilities in their respective interests and aspirations and in the political ideologies underpinning the structure of their respective governments and societies'.[3] These ideological differences—between Syria as a secular pan-Arabist state and Iran as a theocratic pan-Islamist power—were considered too fundamental to allow for any genuine long-term partnership even over shared geopolitical interests.

[1]Vignal 2017.

[2]Hirschfeld 2014.

[3]Hunter 1993.

Nevertheless, in fact the partnership has not only endured but deepened over time. The reasons for this endurance lie largely in geopolitical factors and shared threat perceptions.[4] Iran and Syria are drawn together by their opposition to the US-led regional security order, and this alliance reflects the desire of 'middle powers' to 'defend their autonomy against intensive Western penetration of the Middle East'.[5] These shared concerns explain how Syria and Iran were able to transcend their ideological differences to work towards shared visions of regional autonomy and reduced foreign penetration of the Middle East.

In recent years, especially since 2011, Iran has demonstrated its strong commitment to its ally and has been a major player in the Syrian conflict. Iran has consistently supported the Syrian government by sending military advisers to the country, establishing transnational militias there and providing political support in the international arena. Yet many mainstream analyses, which are largely divorced from theoretical frameworks, interpret Iran's actions as expansionist,[6] reflecting an attempt to recreate the Persian Empire,[7] by means including the creation of a land bridge from the Iranian plateau to the Mediterranean Sea.[8] Others analyse Iranian behaviour through a sectarian lens, focusing on Iran as a predominant Shi'a power,[9] or on Iranian anti-Israeli ideology.[10]

Many of these accounts, however, downplay or ignore Iranian security concerns and misread Iranian behaviour owing to an inadequate understanding of Iranian threat perceptions and strategic planning. There are exceptions. Some scholars have analysed Iranian strategy in the Syrian war through the prism of Tehran's security concerns.[11] Others have framed Syrian and Iranian foreign policies as a means of increasing regime resilience at home by using 'foreign policy to acquire nationalist legitimacy from external threat'—an approach in which resistance to outside threats from actors such as the United States and Israel is used to legitimize centralization of power and popular mobilization for the regime at home.[12]

However, the limited periods covered by these works mean that they do not account for the full evolution of Iran's strategy throughout the Syrian war. In this chapter, we focus specifically on the drivers of Iranian foreign policy towards Syria over a period of decades, but especially since 2011. We argue that the most salient factor driving Iran's relationship with Syria—from the Islamic Revolution to the current Syrian conflict—has always been a strategy of deterrence. While Syria may be important for Iran for other reasons as well, such as enabling it to undertake

[4]Goodarzi 2006.

[5]Ehteshami and Hinnebusch 1997.

[6]See e.g. Champion et al. 2018.

[7]See e.g. Stavridis 2015.

[8]See Yaari 2017.

[9]For one example, see Nafi 2017.

[10]Sadjadpour 2018.

[11]Milani 2013; Hadian 2015; Ostovar 2018.

[12]Ehteshami et al. 2013.

counter-containment, the fundamental basis of the relationship is first and foremost deterrence; this can explain Iranian actions throughout the course of the Syrian war. Syria offers Iran vital strategic depth in the Arab world, allowing it manoeuvrability throughout the Levant, and provides it with a gateway to Hezbollah, enhancing Iranian deterrence of Israel. Yet, just as the development of the Iran–Syria relationship began before the formation of Hezbollah, so continued strategic cooperation between the two countries demonstrates that the relationship now represents an independent axis.

This chapter contributes to the debates on Iranian strategy and regional geopolitics by explicating the primacy that deterrence has consistently played in determining Iran's Syria strategy, as opposed to other ideological, geopolitical or sectarian factors. It draws on a rich array of primary source materials in Arabic and Persian, with key references to speeches by leaders of Iran, Syria and Hezbollah, and builds on insights and experience gained through extensive fieldwork in Iran and Lebanon. It also provides an analysis, hitherto largely absent from the field, of the stages and drivers of Iranian behaviour since the beginning of the Syrian conflict in 2011.

We begin by discussing how deterrence has underwritten the nature of Iran–Syria ties since the 1979 Islamic Revolution. We then examine the debates on Syria within Tehran at the onset of the Syrian conflict. Next, we focus on the different phases of Iranian decision-making during the war, explaining why Iran shifted from a localized strategy of supporting the Syrian regime to regionalizing and internationalizing the military coalition. Finally, we look at Iran's Syria strategy following the defeat of the Islamic State in Iraq and Syria (ISIS) and the emergence of rivalry among multiple stakeholders in the country, above all Russia, Turkey and the United States, alongside their respective allies.[13]

13.2 The Logic of the Relationship

Deterrence is the underlying logic that has bound Iran and Syria together from the beginning of the Islamic Revolution in 1979 up to the present day. Syria was the second country to formally recognize the Islamic Republic and assisted Iran during the eight-year long Iran–Iraq War (1980–1988). The Syrians also trained Iranians in ballistic missile technology, and the two countries coordinated support for non-state actors, including Hezbollah and Palestinian resistance organizations, against Israel and the United States in the Levant. Deterrence continued to be the primary driver deepening the alliance in the new century, notably after the 2003 Iraq War when the United States established a military presence in Iraq between the two countries. On the basis of their convergent interests, the relationship between Iran and Syria can be divided into three periods: first, the formative stage of cooperation in the 1980s

[13]Okyay 2017.

based on mutual threat perceptions; second, a cooling of relations as strategic incentives diverged during the Gulf War and throughout the 1990s; and third, the renewal and consolidation of the strategic alliance within what is referred to as the Axis of Resistance following the 2003 Iraq War and in a context of heightened security threats.

Deterrence implies a strategy to prevent hostile actions through shaping the cost–benefit calculations of adversaries, specifically to prove that 'the costs and/or risks of a given course of action [an adversary] might take outweigh its benefits'.[14] Deterrence theory is therefore concerned with the imprecise science of estimating an enemy's intentions and seeking to influence them.[15] Establishing credibility is foundational to the enterprise of achieving deterrence, and the primary focus of the literature therefore rests upon the various means by which states issue 'conditional threats' and demonstrate the credible 'prospect of punishment' in order to shape behaviour.[16]

Deterrence theory has largely developed in the United States and accordingly reflects western strategic thinking during the Cold War, with much less attention given to deterrence strategy as practised by countries in the developing world.[17] Accordingly, much of the literature involves a strong focus on nuclear deterrence and the noteworthy role that highly destructive weapons such as the nuclear bomb have had in determining deterrence strategy, especially during the Cold War.[18] However, other work has also focused on conventional deterrence, or deterrence undertaken with conventional weapons,[19] and there is a growing literature on asymmetric deterrence involving non-state actors.[20] Nevertheless, the field has not resolved whether the concept of deterrence is of universal application across the full range of states and non-state organizations, and is still struggling to address the general criticisms of the theory, including the claim that deterrence does not work well and is a poor strategy in practice.[21] One critical case in which deterrence actually does seem to hold, demonstrating the concept's continued relevance and significance, is that of Israel and Hezbollah since the 2006 war.[22]

Beyond the challenge posed by a dearth of theoretical work on deterrence in non-western settings, the difficulty of understanding Iranian behaviour also stems from the fact that the country's strategy is built on combined conventional and asymmetric deterrence that also incorporates the support of other state and non-state actors, all of which introduce considerable ambiguity in terms of effective

[14]George and Smoke 1974.

[15]Schelling 2008.

[16]Freedman 2004.

[17]Lieberman 2012.

[18]On nuclear deterrence, see Nye 1986.

[19]The literature on conventional deterrence includes: Huntington 1983.

[20]See e.g. Arreguín-Toft 2005.

[21]Lebow and Gross Stein 2007; Gross Stein 2009.

[22]Lieberman 2012; Sobelman 2017.

messaging, rational decision-making, and establishing credible capability without nuclear deterrence.[23] Iran's conventional deterrence capabilities are largely rooted in its domestic ballistic missile programme and its capacity to use missiles to hit regional targets, as demonstrated in strikes in Iraqi Kurdistan and on ISIS positions in Syria in September and October 2018 respectively. Iran also has asymmetrical deterrence capabilities largely through its support of regional non-state actors, such as Hezbollah in Lebanon, and also through the operational activities of the external branch of the Islamic Revolutionary Guards Corps (IRGC), the Quds Force.

In this chapter, we seek to shed light on the importance Iranian strategists give to deterrence and demonstrate how this concept shapes the country's objectives in Syria. Specifically, we argue that Iranian strategy within the Levant, including both Syria and Lebanon, should be understood as 'forward deterrence'. Here we define forward deterrence as the deployment or possession of deterrent capacity beyond one's own national borders that abut on the adversary's frontier. Iran's forward deterrence strategy has not historically involved direct forward deployment of armed forces, since its deterrence capacity is largely provided by partners and allies that are not under formal Iranian control. In other words, while Iran has a conventional deterrence strategy—as evidenced by its ballistic missile programme—in parallel it also has a forward deterrence strategy in the Levant via Syria and allied non-state actors. Syria therefore provides Iran with strategic depth in the Levant and access to Hezbollah, while Syria itself also has a combined conventional and asymmetric deterrence strategy against Israel. These are all different components of what Iran terms its 'comprehensive deterrence' (*bazdarandegi-e hame janebe*) doctrine, according to which it uses diverse and multi-layered means to defend itself from any potential aggression.

Iranian and Syrian threat perceptions have been shaped from the beginning of their relationship by a shared sense of regional isolation and a shared antiimperialist ideology.[24] The two countries forged a partnership with the practical objective of deterring regional threats from their main adversaries. These were primarily the United States, Israel, and Iraq under the regime of Saddam Hussein.[25] In particular, the Iran–Iraq War brought about a convergence of threat perceptions as Iran and Syria both perceived Iraq as a common enemy. The alliance also came at a critical juncture for Syria, which in March 1979 lost Egypt as an ally with the signature of the Camp David Accords making peace with Israel.[26] Further, Iran and Syria are both staunch supporters of the Palestinian cause: Syria was and is the home of many Palestinian groups, including the Popular Front for the Liberation of Palestine (PFLP), which has historically been headquartered in Damascus, and in the 1980s

[23]For a concise explanation of some of these challenges, see Sobelman 2017, pp. 157–62; Adler 2009; Lieberman 2012.

[24]Ehteshami and Hinnebusch 1997, pp. 88–91.

[25]Goodarzi 2006, p. 2.

[26]Ibid., p. 12.

and 1990s Syria extended support to Islamist groups including Hamas and Islamic Jihad.[27]

On the Iranian side, symbolizing the country's firm stand against Israel, the 'first Palestinian embassy in the Middle East' was opened on the grounds of the vacated Israeli mission in Tehran following the Islamic Revolution.[28] More importantly, both Syria and Iran considered their patronage of Palestinian groups as part of an effective deterrence against Israel. Joint training activities were carried out for the PFLP in Lebanon's Beqaa valley on the eve of the Arab Spring by Hezbollah, overseen by Iran, with a reported 4,000 highly trained PFLP fighters hosted in a military base in Qusayra, Lebanon.[29] For Syria, the Iranian Revolution was a godsend: Hafez al-Assad viewed the previous Israeli–Iranian alliance as representing a stranglehold over the Arab world, interpreting the Shah's support for Iraqi Kurdish insurgents as a means of bogging down Iraq and preventing it from providing support for a united Arab front against Israel.

Following the Islamic Revolution, the Iranians felt both isolated regionally and under threat from the United States, Tehran's primary adversary. This was a stark change from the pre-revolutionary period, when Iran and the United States were close allies and Iran sold oil to Israel in exchange for training its military personnel there, and Iran's notorious SAVAK intelligence services were trained by both the CIA and Israel's Mossad.[30] Revolutionary Iran's realignment away from a pro-western axis was in large part a result of significant historical grievances against the West held by Iranians, including the Anglo-Iranian oil crisis and *coup d'état* against Mohammad Mossadegh in 1953 and other significant humiliating territorial and economic concessions exacted from Iran by western powers since the nineteenth century.[31] Iran's assumption of a regionalist and anti-imperialist approach in defining its Middle Eastern priorities and threat perceptions overlapped with Hafez al-Assad's vision of rejecting the interference of extra regional powers in the domestic affairs of the region.

In parallel to developments in revolutionary Iran, Syria faced increased regional isolation for two reasons. The first was as a consequence of the Camp David Accords of 1979.[32] Despite Egypt's decision to discontinue conflict with Israel, the Syrian regime demonstrated continued populist and pan-Arab zeal, ironically alienating it from much of the Arab world. The second, a point of increasing concern for Syria, was in regard to Iraq. Syria needed to preserve its position vis-à-vis Iraq for both ideological and geopolitical reasons. As countries both ruled by Ba'athist parties that simultaneously claimed the leadership of the Arab world, they

[27]Leverett 2005, p. 12. Other groups include the paramilitary commando group Al-Sa'iqah, which was set up after the 1967 war: see Van Dam 2011, p. 67. See also Cubert 1997.

[28]Ehteshami and Hinnebusch 1997, p. 89.

[29]Leverett 2005, p. 12; Rabinovich 2008; Vallentine 2010, p. 232.

[30]Ehteshami and Hinnebusch 1997, p. 89.

[31]See e.g. Ramazani 2013.

[32]Kamil 2016.

were locked in an intense rivalry that threatened their respective domestic and regional political legitimacies and created the conditions for potential conflict.[33]

Geopolitically, Syria also sensed increased vulnerability as Iraq's influence grew regionally after the fall of the Shah and with Arab support for Iraq's efforts in the war against Iran. Accordingly, a logic of deterrence and balancing the existential Iraqi threat during the Iran–Iraq War shaped the foundation of the Iran–Syria partnership.[34] The collaboration, rooted in the 1979 Revolution, was a pragmatic strategy designed to mitigate the two countries' shared vulnerability and isolation, and to overcome the threats posed by Iraq.[35]

The third perceived shared threat was from Israel. While Hafez al-Assad was careful to try not to antagonize the United States, Syria's continued opposition towards Israel served as a wedge preventing any meaningful *rapprochement* with America, especially in the context of the pre-Arab Spring Middle East.[36] Located at the front line of the Arab–Israeli conflict and as a 'self-proclaimed' leader of Arab nationalism,[37] Syria had always considered Israel a significant threat. However, this became all the more important following the Camp David peace accords and the Israeli invasion of Lebanon in 1982, both events prompting Syria to look for a partner that could support it against a common enemy. While the Camp David peace accords deprived Syria of Egypt as an ally against Israel, Israel's invasion of Lebanon led directly to the emergence of a new partner for Syria: Hezbollah.

The important point here is that Hezbollah served as an extension of Iran's Islamic Revolution and a reflection of its anti-Zionist ideology, even though its creation was prompted by factors independent of Tehran, namely the Israeli occupation of southern Lebanon.[38] This structural opening led to an opportunity for Iran's policy of 'export[ing] the revolution' in the 1980s.[39] Accordingly, the Iranian–Syrian partnership converged behind Hezbollah against a common enemy. On top of ideological factors, Iran also considered Israel a military threat because of its close alliance with the United States. Iran thus saw in Hezbollah an opportunity to project deterrence and leverage against the United States in Lebanon, including the taking of American hostages and potentially targeting the American military presence in that country.[40] In this way Hezbollah would provide Iran with deterrent capability via its targeting of Israel and US interests in the Levant. Eventually, while the export of revolution lost primacy after the first decade of the Islamic

[33]Baram 2014.

[34]See e.g. Goodarzi 2006 and Milani 2013.

[35]Milani 2013, pp. 81–82.

[36]Landis 2010.

[37]While Syria, Iraq and Egypt, as pan-Arab republics, were all contenders for the leadership of the Arab world, the Camp David Accords in many ways removed Egypt from the contest and pitted the rivalry between the remaining two Ba'athist states, Syria and Iraq.

[38]Norton 2009; Qasim 2010.

[39]Ramazani 2001.

[40]Sick 1987.

Republic, the deterrent logic behind Iran–Hezbollah ties remained, and remains, strategically significant.

In the 1990s, the Iran–Syria partnership weakened as mutual threats diminished and the impetus for deterrence decreased. Iran pursued a more pragmatic foreign policy following the end of the Iran–Iraq War and the arrival in power of more moderate presidents, Hashemi Rafsanjani (1989–96) and the reformist Mohammad Khatami (1997–2004). Both administrations wanted to normalize Iran's regional and international standing and thus sought detente with the United States.[41]

Despite Iran's status as an anti-American revolutionary state, Rafsanjani made great efforts to invite the US oil company Conoco to do business in the country, only to be surprised by President Bill Clinton's blocking it through an executive order in March 1995, which was followed one month later by a ban on all US trade and investment with Iran. Later, Congress passed a 'sweeping sanctions bill, later signed by Clinton, to punish foreign companies that invested $40 million or more in the oil resources of Iran'.[42]

This move was all the more significant as in 1993 US exports to Iran amounted to US$1 billion and the United States was the largest purchaser of Iranian oil in the early 1990s, taking around 30 per cent of Iran's oil exports with a total value of over US$4 billion.[43] Despite the American measures, Iran pursued detente with Saudi Arabia and greatly improved its relations with the Arab states of the Persian Gulf during this period. A major meeting of the Organization of Islamic Cooperation was hosted in Tehran in 1997 and was attended by Crown Prince Abdullah and the Saudi Foreign Minister; King Fahd even donated cloth from the Ka'ba to be displayed at the summit.[44] Hezbollah also moved to normalize its relations in the domestic context of Lebanon, setting aside its more revolutionary ideals and pursuing pragmatic goals as a legitimate party in the Lebanese political scene.

Thus during these years its value for Iran and Syria declined as it gained greater autonomy and independence from its patrons. At the same time, Syria saw Iraq as less of a threat after the 1991 Gulf War, during and after which—much to Iran's dismay—it cooperated with the United States. This brought Syria closer to other Arab countries, which viewed Saddam Hussein as a common enemy after his invasion of Kuwait. Also indicative of a drift in Syrian–Iranian relations was Syria's decision to enter into negotiations with Israel in the late 1990s.[45] Thus a divergence of interests and a weakening of the logic of deterrence based on mutual threats diminished cooperation between Iran and Syria and marked a slackening of

[41]Ramazani 2001, pp. 225–228.

[42]See Gerges 1996.

[43]See Gerges 1996, p. 6; Iran's 'normalization' policy did not mean that it had given up either its revolutionary goals or its broader anti-Israel and anti-American stance in the Middle East. Rather, it sought to reach a more pragmatic position in regional affairs and largely cast aside its 'export of the revolution' policy.

[44]See Marschall 2003, pp. 142–145.

[45]Landis 2010.

the relationship during the 1990s. After 2003, however, a series of strategic reversals forced Syria closer to Iran again. With the American invasion of Iraq, a much more direct threat emerged from the United States. The establishment of a permanent and hostile US presence on the border of both countries galvanized further strategic cooperation and coalition-building in order to ensure survival. The Axis of Resistance was thus born to fend off shared threats. This became all the more important for Syria following its expulsion from Lebanon after the 2005 Cedar Revolution, which added to Damascus's sense of increased insecurity. The forces pushing Syria and Iran together culminated in the 2006 Israel–Hezbollah war, which demonstrated the potential for shared resistance and joint military effectiveness.

Thus the Iran–Syria alliance deepened as threat perceptions converged and intensified. Eventually, with the outbreak of the Syrian war in 2011, the relationship became even stronger. As the historical trend line demonstrates, the weaker Syria becomes, the more its strategic alignment with Iran advances.

13.3 Iranians Debate Syria

The Iran–Syria relationship faced its most pressing challenge with the onset of the Arab Spring. The mass protests that rocked the Arab world in 2010–11 reached Syria in March of the latter year, later than in other states of the region. Although the Syrian government employed tactics of both repression and appeasement, the protests continued unabated.[46] Faced with this growing challenge, the Iranian foreign policy establishment became embroiled in an unprecedented internal debate on its position regarding Syria, a key Iranian ally and a critical actor in the Axis of Resistance, with divergent narratives taking shape around the Syrian protests. This contrasted with Iran's immediate adoption of a clear position on the regional uprisings as a whole, which it hailed as an 'Islamic Awakening' modelled on its own revolutionary success.[47] The debate in foreign policy circles, like many others within the Islamic Republic,[48] in part reflects the relative openness to discussion of divergent policy positions among a ruling elite used to competitive elections within the framework of a hybrid political system that mixes democratic and non-democratic regime features,[49] and the factional penchant for politicizing issues for purposes of domestic gain and elite rivalry. While national security policies are generally arrived at through consensus in the Supreme National Security Council,

[46]Reforms included abolishing the emergency laws, dissolving the government and the Security Court (Amnal-Dowla), establishing a dialogue with the opposition and issuing public pardons.

[47]Mohseni 2013.

[48]For an analysis of factional differences in policy-making within the Islamic Republic, see Mohseni 2016, pp. 37–69.

[49]Gilbert and Mohseni 2011.

there is a relatively permissive approach to debate during the process of deliberation. Moreover, the Supreme Leader initially did not enforce one clear position, thus enabling different branches of government, such as the President, members of parliament, the heads of state institutions and political factions, to take divergent positions on the subject of Syria.

Two different discourses emerged within the Iranian political elite on the Syrian uprising, and these—contrary to many analyses[50]—transcended political and factional dividing lines. The first was the Arab Spring approach: a call for the support of all popular uprisings against ossified dictatorships reminiscent of Iran's struggles against the Shah. Adherents of this normative framing argued that Iran should support the legitimate demands of the Syrian people as it did those in other Arab countries, fuel the 'Islamic Awakening', and put pressure on its own ally to allow political reform. Conservative President Mahmoud Ahmadinejad, for example, supported this approach, claiming that 'we should not pay more costs in Syria because the time of Bashar Assad is over'.[51] In a controversial speech, Hashemi Rafsanjani, the moderate head of Iran's Expediency Council, took a similar position, criticizing the Syrian regime and highlighting the atrocities committed against the Syrian people.[52]

Within the Arab Spring framework, others took a more recent episode as their frame of reference for assessing the Syrian protests. The green movement protests following the 2009 elections and the alleged fraud leading to the re-election of Ahmadinejad had produced the largest mass protests since the 1979 Revolution. Many viewed the Arab Spring protests as mirroring their recent struggle. As Mir Hossein Mousavi, the reformist presidential candidate and a leader of the green movement, stated: 'The starting point of what we are now witnessing on the streets of Tunis, Sanaa, Cairo, Alexandria, and Suez can be undoubtedly traced back to . . . when people took to the streets of Tehran in the millions shouting "Where is my vote?"'[53]

The second narrative framed the uprising through a geopolitical lens and focused on the impact of the Syrian crisis on the regional balance of power. This narrative treated the Syrian uprising as a foreign plan to overthrow a key ally on the front line of the Axis of Resistance and thus tilt the balance of power against Iran.[54] This was supposedly an attempt to offset the gains Iran had made in particular since the 2003 Iraq War, the 2006 Israeli–Hezbollah war and the toppling in 2011 of pro-US secular dictatorships in Egypt, Tunisia and Yemen that had been hostile towards Iran. From this perspective, fomenters of the Syrian crisis were aiming to roll back Iranian gains and cripple Iran's deterrent capabilities against Israel and the United

[50]Milani 2013.

[51]Tabnak 2018.

[52]Rafsanjani, however, later denied his statements, saying that his words were misinterpreted. For the sound recording and video of his speech, see Jahannews 2013.

[53]Kurzman 2012.

[54]ISNA 2018.

States. On this view, the potential collapse of Assad and the loss of its main Arab ally would have been a critical blow to Iran's regional interests. Many Iranian strategists deemed it necessary to take active measures to counter this threat. Among them was Brigadier-General Hossein Hamidani, the commanding IRGC general in Syria, who in urging this course referred to Saudi offers of support to Damascus if it cut ties with Iran in exchange.[55] General Qasim Sulaymani, head of the IRGC Quds Force, pointed to Riyadh's unsuccessful attempts at turning Assad against Iran, claiming that King Abdullah told Assad that 'Lebanon is yours' if he were to abandon Iran.[56] Assad later confirmed these offers in a public interview.[57] An analysis published on Ayatollah Ali Khamenei's website also illustrates this position: Westerners considered the Syrian opposition as an opportunity to limit Hezbollah and cut relations between Iran and Syria, and they tried to eliminate the contact between Iran and Syria and destroy Iran's supportive bridge to Hezbollah through the toppling of Bashar Assad, thus putting Hezbollah under pressure.[58]

In explaining Iran's support for the Syrian regime later in the conflict, Sulaymani pointed to the fact that Syria had been the only Arab country to stand by Iran during the Iran–Iraq War when all other Arab countries opposed Tehran.[59] He added that if Iran had not entered the conflict, 'ISIS and the al-Nusra Front would have established a government in Syria and . . . dominated the region.'[60] He further alluded to Syria's anti-Israel position: In the face of all the countries that established private or public contacts with the Zionist regime, only one country, Syria, was willing to sacrifice its security and all of its territory for Muslims. And even during the time of President Bill Clinton when the issue of peace between Syria and the Zionist regime was supposed to be resolved in Paris, Hafez Assad went to Paris but did not attend the morning session and was not present at the negotiation because he knew what the impact of Syria's compromising over the steadfastness of the Resistance front against Israel was and as a result he thwarted it.[61]

While this anti-Israeli stance might be perceived as catering to domestic audiences in Iran or even aimed at appealing to widespread anti-Israeli sentiments in the region, in reality Iran has worked extensively to counter Israel on the ground. Evidence of this can be seen in Iran's logistical support for Hezbollah from its inception in 1982, when it fought against the Israeli occupation of Lebanon, and during later significant crises such as the Israeli–Hezbollah war of 2006. It can also be seen in Iran's backing of Hamas (especially its military wing) in Palestine, and

[55]Al-Alam 2016.

[56]ISNA 2016.

[57]Al-Alam 2018.

[58]Office for the Preservation and Propagation of the Works of Grand Ayatollah Seyyed Ali Khamenei 2011.

[59]ISNA 2016.

[60]ISNA 2016.

[61]ISNA 2016. Another perspective places the onus on Israel, arguing Ehud Barak allowed negotiations to fail. See Landis 2010, pp. 66–67.

its support of Palestinian Islamic Jihad, as well as other geopolitical alliances aimed at countering Israeli threats, including, of course, its 40-year-old alliance with Syria which has been defined by its emphasis on forward deterrence against Israel.

According to this view, Tehran could not turn a blind eye to the regional push against Assad as Iran considered itself the party under threat in Syria. A prominent Iranian cleric made the claim that 'if we lose Syria, we will not be able to preserve Tehran'.[62] The reformist Rear-Admiral Ali Shamkhani, who currently heads Iran's Supreme National Security Council, claimed that Iranian involvement in Syria prevented the crisis from spilling over into Iran.[63] Over time, this perspective has been reasserted both by Iran and by its allies in the region. Referring to Iranian soldiers killed in Syria and Iraq, the Supreme Leader declared in early 2016 that Iranians who departed to fight ISIS 'went to battle an enemy that would have entered the country if they had not fought them [abroad] . . . [otherwise] we would have had to battle them here in Kermanshah and Hamedan and the rest of Iran's provinces'.[64] Along similar lines, Hassan Nasrallah, the Secretary-General of Hezbollah, claimed it natural for Iranians to have been worried about the consequences of the Syrian conflict as 'war could have stretched to Tabriz, Tehran and Mashhad'.[65]

Public perceptions on Syria accordingly shifted away from the Arab Spring narrative with the emergence of 'excommunicating' or *takfiri* groups in the Syrian opposition, especially after the advance of ISIS deep into Iraqi territory. The empowerment of radical *takfiri* groups condemning Shi'a Muslims as infidels did much to undermine sympathy among Iranians for the Syrian opposition. Secular Iranians resented the emergence of conservative Islamists, while the more religious Iranians saw their fears that the uprising was a foreign plot against the Shi'a and Iran confirmed. Therefore, the radicalization and 'takfirization' of the Syrian opposition greatly undermined the Arab Spring narrative among the Iranian populace.

13.4 The Evolution of Iranian Strategy after the Arab Spring

While the two framings of the Syrian situation were highly contested in Tehran during the first six months of the uprising, it was the geopolitical framing that eventually gained traction with the elite. A clear shift in that direction, in reaction to regional and international developments, can be traced to the end of summer 2011.

---

[62]Asr Iran 2013.

[63]Fars News 2014.

[64]Office for the Preservation and Propagation of the Works of Grand Ayatollah Seyyed Ali Khamenei 2016.

[65]Al-Mayadeen 2018.

On 18 August, President Barack Obama declared for the first time that 'the time has come for President Assad to step aside'.[66] The Iranians interpreted this statement as marking a new phase in the Syrian crisis in which the United States and its allies were embarking on an interventionist policy of seeking regime change in Damascus.[67] While the Iranians were always opposed to an interventionist American role in the region and suspected the United States wanted to re-shape the Middle East through regime change policies directed at adversarial states, they now inferred that the United States had turned its gaze on Syria and was preparing to make a concerted effort to bring down Assad, thereby seriously undermining Iran's forward deterrence posture. This Iranian perception was strengthened by the Saudi withdrawal of its ambassador to Syria, at the same time as Obama's declaration, followed immediately by similar withdrawals on the part of Kuwait and Bahrain (Qatar had done the same a month earlier). It was precisely at this time that Rafsanjani made an important claim regarding these new developments: 'Now the United States and the West in general and a number of Arab countries have basically declared war on Syria and ears are waiting by the moment for the rumble of missiles and bombs.'[68]

Given that most of these Arab countries took a reactionary approach to the Arab Spring, particularly to the protests in Bahrain and Yemen, their support for the Syrian protesters was interpreted in Tehran as a geopolitical move—not one that could be framed according to the Arab Spring narrative. In particular, the Saudi shift on Syria was considered to mirror the new US policy stance of applying increasing pressure on Damascus, with a senior Saudi official claiming that 'the King knows that other than the collapse of the Islamic Republic itself, nothing would weaken Iran more than losing Syria'.[69] In addition, Turkish Foreign Minister Ahmet Davutoğlu issued the country's 'final word' to Assad on 15 August 2011, and on 28 August President Abdullah Gul declared that Turkey had 'lost confidence' in the Assad regime.[70] Turkish dialogue with Syria ended at this time.[71] The Syrian opposition was also largely anti-Iranian and explicitly declared its intention to change the political alignment of Syria and, consequently, the geopolitical map of the Middle East. The opposition protests included anti-Iranian chants and slogans, such as 'no Hezbollah, no Iran' and the burning of Iranian and Hezbollah flags.[72] Saudi Arabia, in particular, as one of Iran's main rivals in the region, was

[66]Phillips 2011.
[67]Author's interview with Iranian official, Tehran, June 2013.
[68]Jahannews 2013.
[69]Hannah 2011.
[70]Barnard 2011.
[71]Author's interview with Turkish diplomat, Istanbul, May 2017
[72]Al-Mayadeen 2016.

among the main sponsors of many Salafi militant groups, with extensive reports of its founding and organizing groups such as Jaysh al-Islam.[73]

Riyadh's objective was to overthrow Assad and thus deliver a major setback for Iran. Moreover, Burhan Ghalioun, the leader of the Syrian National Council, Syria's main opposition group at the time, declared that 'the current relationship between Syria and Iran is abnormal . . . There will be no special relationship with Iran [i.e. after the toppling of Assad]'.[74] He also stressed that the change in relations would have an impact not only on Iran but on its allies as well: 'As our relations with Iran change, so too will our relationship with Hezbollah. Hezbollah after the fall of the Syrian regime will not be the same.'[75] Iranians saw these developments, taken together, as a serious sign that significant geopolitical factors were now formally in play, shaping the course of the Syrian conflict. The war was no longer about the Syrian people, domestic reforms or human rights, but solely about geopolitical interests. In a meeting with Turkish President Recep Tayyip Erdogan in March 2012, Khamenei stressed Iran's strong opposition to any US plans in Syria, stating that 'the Islamic Republic of Iran will defend Syria because of its support for the Line [i.e. Axis] of Resistance in the face of the Zionist regime and strongly disagrees with any intervention of outside forces in the internal affairs of Syria'.[76]

Initially, Iran's support for Syria was limited to political and economic assistance along with international support through institutions such as the UN.[77] At the same time, however, it distanced itself from the Assad regime rhetorically and criticized the use of force against protesters, to appease the Iranian public. These mixed reactions indicated that the Iranian establishment's initial assessment of the Syrian conflict was largely optimistic: protests had broken out relatively late, and the Syrian regime's anti-Israeli position and independence from US influence were thought to endow Assad with greater legitimacy than some other rulers. Anticipating that modest reforms would secure the Syrian regime, Iranian support was relatively unobtrusive and decidedly non-military. As faith in Assad's political survival weakened over time, however, Iran decided that the only way out was through coalition-building. The important point here is that Iran's overarching forward deterrence strategy was threatened in Syria. In response to these threats, it resorted to a series of practical military strategies which were aimed at preserving that deterrence, each of which can be studied as a separate phenomenon in its own right. We accordingly divide Iran's Syria strategy into four phases: (1) a 'Basij' strategy of establishing local militias in Syria; (2) a regionalization strategy of incorporating transnational fighters and militias in the war effort; (3) an internationalization strategy aimed at drawing in Russia and balancing the United States;

[73]Black 2013.

[74]Wall Street Journal 2011.

[75]Syria opposition leader interview transcript.

[76]Office for the Preservation and Propagation of the Works of Grand Ayatollah Seyyed Ali Khamenei 2012.

[77]Young Journalist Club 2016.

and (4) a post-ISIS deterrence strategy to balance against the United States, Turkey and Israel. Through these four phases Iran's Syria strategy has progressively escalated in response to the possible defeat of its ally and the deterioration of its forward deterrence posture through Syria and Hezbollah against Israel. Today, the potential for direct interstate conflict is increasing as proxy warfare declines and Iran attempts to maintain the credibility of its forward deterrence capacity.

13.4.1 Phase 1: Iran's Basij Strategy

As noted above, President Obama's declaration of August 2011 and Iran's regional rivals' increased backing of rebel forces initiated a shift in Tehran's strategy towards Syria. As an international anti-Assad coalition emerged, Iran's belief that the Syrians could themselves control the situation with minimal support was significantly weakened. It therefore became clear to Tehran that Iran needed to reformulate and upgrade its strategy to block its rivals' advances in Syria. At this time, Iran's principal move was to advise the Syrian government to create local militias, with the twin aims of safeguarding significant religious and political sites on the one hand and training the Syrian military and security forces for an asymmetric war scenario on the other. Both efforts were spearheaded by the IRGC. In his personal memoir, published after his death in Syria, General Hamidani described Iran's initial involvement as advisory and as a response to the Syrian request for assistance with the immediate objectives of defending religious shrines and fighting opposition forces.[78] Training started in late 2011, only months after the perceived start of a wider regional campaign against the Syrian regime. It was not until the summer of 2012 that General Mohammad Ali Jafaari, head of the IRGC, admitted a Quds Force presence in Syria.[79]

The Basij model, which comprises a bottom-up mobilization of volunteer fighters into paramilitary formations, developed out of Iran's experience in the post-revolutionary period and in the Iran–Iraq War.[80] Iran's own Basij model was replicated in Syria as the 'People's Popular Committees' (al-Lijan al-Sha'biyah), which by the end of 2012 had merged into the new 'National Defence Forces' (Quwat al-Difa al-Watani). Iran has consistently sought to export the Basij model to other countries, including Lebanon, Iraq and Yemen. The war created the opportunity for Iran to pursue the same strategy in Syria. Cultural Basij centres were established in 14 Syrian provinces, with Hamidani claiming that 'those centres were active even in provinces under the occupation of al-Nusra'.[81]

[78] Al-Alam 2016.
[79] ISNA 2012.
[80] Mohseni and Kalout 2017.
[81] Tabnak 2015.

According to the IRGC Deputy Head of the Basij, Mohammad Hussein Sepehr, 'the greatest service that General Hamidani did for the Resistance Front was the creation of the popular Basij [in Syria] . . . composed of our Alawite and Sunni brothers'.[82] Moreover, Jafaari claimed that 'if it were not for the emergence of the popular Basij in Syria, this country would have been divided into several parts and today we would not have the country of Syria'.[83] Likewise, in an interview with the Iranian Al-Alam TV, Assad confirmed that 'in addition to advisers, there are groups of Iranian volunteers who came to Syria to fight and they are commanded by advisers and as a result Iran fought in Syria . . . however, not even one official Iranian military force is in Syria'.[84]

In contrast to analyses exaggerating the costs of Iran's involvement in Syria,[85] we argue that this military mobilization strategy served as a very cheap and effective way to enhance Syria's security.[86] Moreover, by strengthening local allied militias, Iran prepared for the possibility of territorial fragmentation in Syria. Iran's support for militias was thus a rational and limited contingency plan to provide for the event of Assad's downfall. It would have given Iran coercive capacity to shape the post-Assad distribution of territory and spheres of influence, especially with regard to littoral Alawite heartlands and regions populated by religious minorities. In short, Iran's Basij strategy aimed to shore up support for its struggling ally and to cut its own losses.

13.4.2 Phase 2: Iran's Regionalization Strategy

While the militias were critical in providing the manpower and organizational capacity to enable the Syrian regime to undertake its military operations,[87] it was still not a sufficient strategy on its own to preserve Assad's power, since the recruits were localized in Syria alone. The Syrian government still experienced reversals on the battlefield and was vulnerable to decisive setbacks, forcing Iran to reconsider its precise strategy. Tehran thus decided to pursue a regionalization strategy, expanding the scope and breadth of the Basij approach through regional coalition-building with both traditional allies such as Hezbollah and newly formed transnational militias willing to fight in Syria. This would not only bolster allied

[82]Tasnim Basij-i mardumi dar Suriyih yadgar-i mandigar-i Abu Vahab [Syria's popular Basij is a legacy of Abu Wahab] http://tn.ai/1539492. Author's translation.

[83]Al-Alam 2017.

[84]Al-Alam 2018.

[85]Juneau 2018.

[86]This perception has been confirmed by multiple Iranian officials in author interviews in Tehran between 2015 and 2017.

[87]Khaddour 2016.

militias' experience, ideology and strength but would also add support to the local militias already operating on the ground.

Hezbollah entered the Syrian conflict from Lebanon in several stages, beginning in 2013. In a speech regarding Hezbollah's initial intervention in Syria, Nasrallah argued that Hezbollah was reacting to geopolitical developments and that it was 'the last party to intervene'. He alluded to the importance of protecting 'a front [the Axis of Resistance] that the world wants to destroy . . . targeted by an American, Israeli, *takfiri* project'.[88]

Hezbollah moved into the border regions of Syria and Lebanon to prevent the infiltration and shelling of Lebanese territory by the armed opposition positioned around the Syrian city of Al Qusayr and to protect Lebanese villages in that region.[89] Perhaps even more importantly, the fall of Al Qusayr and its peripheral region would have enabled al-Nusra to cut Damascus off from resupply routes via Latakia. Tehran needed Hezbollah's assistance in retaking the city as the Syrian Arab Army and its Iranian allies were not able to do so alone. The battle of Al Qusayr marked a turning point, as it was the first major military victory by the Syrian regime and its allies. Beyond the border regions, Hezbollah also positioned itself at the Holy Shrine of Lady Zaynab and established a foothold in Damascus.[90]

It also advanced deep within Syrian territory to fight opposition combatants—securing Syrian territories bordering Lebanon from Al Qusayr across the border in northern Lebanon to Zabadani in the south.[91] In addition to Hezbollah, Iran organized transnational forces to take part in the conflict, recruiting and training fighters from Pakistan, Afghanistan and elsewhere in the Arab world—many of whom were motivated by religious and ideological loyalties to volunteer for the defence of the holy shrines. These recruits came to be known as the Fatimiyoon and Zaynabiyoon Brigades—parallel to developments happening within Iraq and the formation of the Hashd al-Shaabi (the Popular Basij). Iran has praised and promoted these fighters and defenders of the shrines (*modafe'een haram*), and has encouraged the production of music videos and documentaries about them.[92]

Since much of the discourse and many of the symbols used in this process were explicitly Shi'a, Iran's strategy could be perceived as sectarian. However, the Iranian propagation and framing of the conflict, which is itself another avenue. There is no clear information on the precise date and timings of this intervention. According to Hezbollah, however, the Al Qusayr battle marked the beginning.

---

[88]Nasrallah Hassan 13 June 2013.

[89]Ibid.

[90]Ibid.

[91]From the Iranian perspective, there was no significant distinction between the Syrian opposition and the takfiris, as both aimed to weaken the Axis of Resistance through armed opposition to the Syrian state. As such, Iran considered them all to be terrorists.

[92]See e.g. the documentary Fatih-i dilha [The conqueror of hearts], directed by Sa'id Zari' Suhayli (Channel Three of Islamic Republic of Iran Broadcasting, 2015); and the music video 'Ali Akbar Ghalich, Ayna al-Fatimiyun? [Where are the Fatimiyoon?], directed by Umid Rahbaran (Mu'asisih-ye Farhangi-ye Hunari-ye Masaf-i Iraniyan, 2015).

For research, this should be seen in a more sophisticated light. Iranian narratives and policies have been simultaneously Shi'a-driven and cross-confessional, as Iranians have actively worked to integrate religious minorities, such as Christians and Druze, and even Sunnis, into the militias.[93] The results of these attempts can be seen in the Druze militias of Saraya al-Tawheed and Ammar bin Yasir Battalion, the Christian militias of Nusur az-Zawba'a and Sootoro, and the Sunni militia of Liwa al-Quds, in addition to the majority Sunni Syrian Arab Army. Iran clearly propagated the message of a threat to the Shi'a community and the need for the Shi'a to mobilize in self-defence, including the defence of holy spaces such as the shrines, while also portraying itself as the protector of religious minorities endangered by radical Wahhabi jihadists. This behaviour represents 'sectarian identity without sectarian ideology',[94] with an emphasis on a strong Shi'a identity, but not a sectarian ideology calling for the exclusion or genocide of those belonging to other sects (as espoused by many radical Wahhabi armed groups). This explains in part why Iran and its allies have been able to acquire the support of Christians and religious minorities in the war effort.

The regionalization of the Iranian coalition alongside allies like Hezbollah allowed Iran to ensure its forward deterrence capacity in the event of Assad's fall, and to carve out a sphere of influence in Syria. Eventually, however, Iran chose to go even further to mitigate its vulnerabilities and guard against the potential failure of the regionalization strategy, by internationalizing its coalition in close cooperation with Russia.

13.4.3 Phase 3: Iran's Internationalization Strategy

Though the regionalization of the Basij strategy proved effective in keeping Assad in power in parts of Syria, Iran still felt uncertain about the final outcome and therefore looked for other ways of ensuring victory for the regime.[95] On the one hand, ISIS had advanced deep into Syrian and Iraqi territory, approaching Iranian borders. On the other hand, the Syrian Arab Army had suffered a string of military defeats from March to June 2015.[96] As a result of these developments, the Syrian regime lost the entire province of Idlib in the north and Busra al-Sham in the south to the opposition and parts of Hama and Homs provinces to ISIS.[97] The loss of Idlib, in particular, meant that al-Nusra and its allies were positioned to overwhelm Latakia, a move which Iran and its allies, including Hezbollah, did not believe they

[93]Mohseni and Kalout 2017.

[94]Mohseni and Kalout 2017.

[95]Author's interview with an Iranian diplomat, Tehran, May 2016.

[96]Al-Masdar (20 June 2015) Asbab haza'im al-Asad al-'askariya [The reasons for Assad's military defeats].

[97]Sweid 2015.

could stop. Worried about the negative developments on the ground, Iran reached out to the Russians, who had just as much to fear as the Iranians in the loss of Latakia and the victory of the al-Nusra Front in Damascus, marking the beginning of a new, internationalizing phase in Iranian strategy.

This internationalization strategy was based on three main factors. First, Assad was failing to win the war, and the rise of ISIS contributed to the perception of an existential threat to his regime. ISIS declared its caliphate in June 2014, stretching from the suburbs of Aleppo and Syria's borders with Lebanon in the west to Jalula and Sa'dia close to the Iranian and Iraqi borders in the east. Meanwhile, Syrian opposition forces were advancing in many areas all around the country, further demonstrating the serious threat posed to the Assad regime. It was obvious for Iran that a change of strategy was needed to overcome the Syrian impasse.

Second, Iran believed it needed to balance advances in US and Turkish positions within Syria that had been made in part as a consequence of the war against ISIS. Russian backing would allow Syrian troops and their allies on the ground to push back against opposition forces, including the US-backed Syrian Democratic Forces (SDF). The US had gained entry into the Syrian conflict and the fight against ISIS through its Kurdish allies. With a heavy footprint in Iraq, the United States decided to fight ISIS by supporting the Kurdish forces on the ground in Syria, where it lacked a commensurate presence of its own. Iran also wanted to balance the air power of the United States, which was providing air cover to its allies.

While its regional and local allies could assist with military operations on the ground, Iran lacked strong outside forces to balance the United States in the air. The third factor concerned domestic Iranian politics following the signing of the Iranian nuclear deal (Joint Comprehensive Plan of Action, JCPOA) in 2015, when Iranian conservatives sought to balance the successful outreach to the West under the administration of the moderate President Rouhani by engaging more closely with Russia against the United States and EU. Their goal was to prevent Iran from moving too close to a western orbit.[98]

Achieving Russian participation in the war was considered the key to all three issues. Initially, Iranian–Russian cooperation took place through intelligence-sharing and political cooperation. In the shadow of the western intervention in Libya, Russia was wary of US plans for regime change in Syria, and played a key role in the UN National Security Council to shelter Syria, including after Syria's alleged use of chemical weapons in 2013. More substantive Russian involvement was inaugurated with its military intervention in September 2015. Sulaymani was rumoured to have travelled personally to Moscow several times to discuss the feasibility and planning of the operation beforehand.[99] The resulting Russian intervention changed all the calculations in the Syrian conflict and solidified Assad's position.

[98]Mohseni 2015, pp. 1–7.

[99]Bassam 2015.

13.4.4 Phase 4: Post-ISIS Balancing

Iran announced the defeat of ISIS with General Sulaymani's congratulatory letter to the Supreme Leader on 21 November 2017, marking a new stage in its Syria strategy.[100] In this letter, Sulaymani also expressed gratitude for the decisive role played by Hezbollah, the Hashd al-Shaabi and local and transnational fighters in the victory. Ayatollah Khamenei, in his official letter responding to Sulaymani, stated that the victory represented not just the defeat of ISIS but also 'a heavier blow to the malicious policies [of conspiring actors] that . . . aimed to destroy the anti-Israeli Resistance and weaken independent states'.[101] He continued: 'I emphasize that we should not be oblivious to the conspiracies of the enemy. Those who plotted this evil conspiracy with such heavy investment will not sit by idly; they will try to conspire in another region or in another form.'

Iran suspects the 'plotting' powers to be colluding with ISIS in order to fragment Syria. Foreign Minister Mohammad Javad Zarif has claimed that the United States seeks to divide Syria[102]—an unacceptable outcome for Iran that would undermine its forward deterrence posture. While ISIS has lost the vast majority of its territorial holdings, its re-emergence cannot be ruled out: a spokesman for the US Department of Defense warned of an ISIS 'resurgence' in April 2018.[103] The terror group has apparently smuggled US$400 million out of its territories to spread across legitimate revenue-generating businesses in the Middle East including extensive money-laundering enterprises in Iraq itself.[104] More importantly, a Pentagon study published in the summer of 2018 reported that between 20,000 and 30,000 ISIS fighters remain across Iraq and Syria and continue to carry out shock hit-and-run terror campaigns.[105]

Like Obama, US President Donald Trump has been somewhat ambiguous on the American role in Syria, vacillating between military strikes on the country and statements of a desire to withdraw US forces from it. In actuality, Trump's Syria policy is driven by two important objectives: the belief in a larger regional push-back campaign against Iran, and the desire to preserve some American presence on the ground in Syria so that the United States can be part of a post-war deal and exert leverage in negotiations with Iran, the Syrian government and Russia.

While the war against ISIS focused the attention of most regional and international actors on a unified target, attention is now more fragmented, with increased peripheral rivalry and friction between the key stakeholders in Syria coming to the

[100]Office for the Preservation and Propagation of the Works of Grand Ayatollah Seyyed Ali Khamenei 2017a, b.

[101]Office for the Preservation and Propagation of the Works of Grand Ayatollah Seyyed Ali Khamenei 2017a, b.

[102]Deutsche Welle 2018a, b.

[103]US Department of Defense 2018a.

[104]Wallace and Cafarella 2018.

[105]US Department of Defense 2018b.

fore. Three main stakeholders have emerged in the Syrian conflict: first, the Kurds and the United States; second, Turkey, stretching from the western banks of the Euphrates to southern Idlib and its own borders in Hatay province; and third, the Syrian regime's own forces and allies, including Russia and Iran.

Given the territory and positions its rivals have managed to carve out within Syria, Iran is intent on balancing them and helping Assad to reconquer the entire country. The Iranians have always insisted that Syria should be maintained as a united state, seeing a Kurdish secession as threatening a regional domino effect endangering Iran's own territorial integrity. Since this sensitivity is also shared by Turkey, one of the cornerstones of the Astana peace process initiated in winter 2016 is a recognition of Syrian sovereignty and territorial integrity.[106] Similarly, Iraq opposes territorial fragmentation, especially given the threat it faces from its own autonomous Kurdish region.[107] Indeed, since 2003 Iraq has constituted a key link in Iran's Syria strategy, serving as a logistical base for Iran's support to Syria and also providing fighters to bolster Assad: Iraqi militias reported to be active in the Syrian theatre include Asa'ib Ahl al-Haq and Kata'ib Sayyid al-Shuhada, among others.[108] An exclusive Reuters report in 2012 described how Iran was alleged to be sending military supplies to Syria on a massive scale via Iraqi airspace, with Secretary of State John Kerry threatening to 'review US aid to Baghdad if it does not halt such overflights'.[109] Iraq was also host to a new intelligence-sharing centre established in Baghdad in 2015 with Iran, Russia, Syria and Hezbollah to coordinate the war effort.

Although the Syrian regime and its allies are gaining momentum on the ground, there is no guarantee that the Syrian government will regain full control of its territory, especially given the continued Turkish and US military presence in the country. Facing such a complex environment, the Iran–Syria axis is concentrating its military campaign on the territories outside the control of Damascus, with Iran having declared its plans to prioritize Idlib and Deir Ezzor in the upcoming phases of the war.[110]

Deir Ezzor has been a critical site of confrontation between the US-backed SDF and the Syrian Army and its allies. The region holds considerable strategic value as a critical land corridor abutting Iraq and the last stronghold of ISIS. As ISIS power

[106]Ministry of Foreign Affairs of the Russian Federation 18 September 2017. Although Iran and Turkey share the goal of preserving Syria's territorial integrity, from the Iranian perspective Turkey's policies are contradictory and conducive to fragmentation, calling for Assad's removal on the one hand and establishing a military presence in northern Syria at the expense of Syrian sovereignty on the other.

[107]Jüde 2017.

[108]Al-Salhy 2013.

[109]Charbonneau 2012.

[110]Mashregh News 2018.

ebbs in the region, both of the two opposing forces are anxious to monopolize control over the area, as evident in the clashes reported in Spring 2018.[111] Idlib, on the other hand, is the last stronghold of al-Nusra forces and other armed opposition fighters. The Turkish and Iran–Syria camps may face each other down in this key battleground, just as they threatened to do in Afrin in early 2018.

Beyond these two theatres, Iran will also focus on supporting the Syrian forces fighting to reconquer opposition enclaves deep inside Syria, including the south, as witnessed in the fierce battles in eastern Ghouta in Spring 2018. The Syrian Army and its allies, including Iran, have been preoccupied with preparations for these battles.

Besides these two theatres, the question of Israel is more important than ever in the post-ISIS period. Like the other main stakeholders in Syria, Iran is also pursuing deterrence towards Israel to secure its hard-fought gains. Given Iran's preoccupations in the conflict and its imperative of managing rival actors within Syria with limited resources, Tehran does not consider the pursuit of direct conflict with Israel a strategic priority.[112] That said, it is certainly seeking to safeguard its forward deterrence vis-à-vis Israel, which Sulaymani described in January 2018 as an aggressive actor 'with 300 nuclear warheads' and a doctrine of 'pre-emptive strikes'.[113]

The first half of 2018 had seen significant tensions between Israel and Iran within Syria. Immediately after the rocket barrage on Israeli positions in the Golan in early May, Israel again attacked Syria, claiming to have hit all Iranian installations throughout the country. While Iran has largely remained silent on these developments, in a major speech following this episode Hassan Nasrallah declared that 'the missile attack in the Golan established a new phase and the enemy [Israel] must make new calculations on Syria'.[114] Syria and its allies have re-established deterrent capacities against Israel, and the cost of Israeli attacks in Syria has been raised.

This represents a clear shift in Nasrallah's position on the rules of engagement with Israel. At the beginning of 2018 he had stated: 'The circumstances impact the rules of engagement. For example, in Syria there may be a strike against one of our targets, and sometimes some of our targets are hit, but we do not retaliate [immediately].'[115] By May, however, this ambiguous stance had been abandoned, with references to 'a new phase' requiring 'new calculations' by Israel.[116] Not long after that, Shamkhani said in an interview that 'Israel should not attack our forces in Syria' and that 'Syria and its allies will not allow the blood of its martyrs to be

[111]Middle East Eye 2018.

[112]See Mohseni and Ahmadian 2018; Ahmadian 2018.

[113]Deutsche Welle 2018a, b.

[114]Nasrallah 2018.

[115]Al-Mayadeen 2018.

[116]Nasrallah 2018.

wasted, and Israel understands this very well'.[117] These actions on the part of Syria and its allies should be evaluated in terms of deterrence. In the same speech in May 2018, Nasrallah referred explicitly to the role of the Resistance in establishing deterrence on the Golan Heights, stating that 'what happened in the occupied Golan is one form of response to the Zionist attacks on Syria and those in Syria, whether it be the people, the Syrian Army, or its allies'.[118] Hezbollah and Iran, in other words, would retaliate if attacked.

He emphasized that the establishment of the Resistance on the Golan was both 'a right' and 'a choice', and added that 'an international source told Israel that if it expanded the response, the other missile strike would be in the heart of occupied Palestine'.[119] The Supreme Leader has also stated repeatedly that the time of 'hit and run' is over.[120] If Iran hesitates, it will suffer a high cost in terms of its reputation. The consequent risk of an escalatory cycle highlights the need for caution on all sides in Syria.

13.5 Conclusion

Iran's Syria strategy has evolved over the course of the seven long years of war. We have argued in this chapter that the logic driving Iran's relationship with Syria has been that of acquiring and securing 'forward deterrence'. Progressively escalating in response to Tehran's sense of new threats and vulnerabilities, Iranian strategy in Syria has advanced through four stages, from a phase of localized militia formation through the regionalization and then internationalization of its coalition to the current balancing strategy of the post-ISIS period.

Iran does not consider the post-ISIS period in Syria to be the final stage of the conflict. The Assad government and its allies still need to reconquer the entirety of Syrian territory, a challenging goal given the presence of the United States and Turkey within the country. As proxy warfare has largely wound down, the possibility of direct interstate conflict has increased. This is evidenced by the fact that the major arenas of conflict are now confined to Idlib and Deir Ezzor, with Turkey exercising direct control over its proxies, effectively disarming the heavy weapons of the Turkish-backed 'National Liberation Front' and establishing joint Turkish–Russian patrols in the demilitarized buffer zones.[121]

At this point, Iranian goals are shaped by the rivalry between regional and international powers as it seeks to balance them and to consolidate its hard-won

[117] Al Jazeera 2018.

[118] Nasrallah 2018.

[119] Nasrallah 2018.

[120] Office for the Preservation and Propagation of the Works of Grand Ayatollah Seyyed Ali Khamenei 2018.

[121] BBC 2018.

position. As part of this balancing, Iran considers it essential to have deterrent capacity to protect its positions within Syria from military threats, not just from the United States and Turkey's allies but also from Israel. If Israel can attack and undermine Iran within Syria, Iran's balancing capacity *vis-à-vis* the United States and Turkey would be harmed, in terms of both reputation and operational effectiveness. That, in turn, would undermine the likelihood of victory—Iran's principal objective in the Syrian war.

The future form of Iran's Syria policy will depend to a great extent on the continuing evolution of the conflict, and the deterrent value of the militias in Syria, including their role in Iran's forward deterrence posture. It is highly unlikely that the militias will be disbanded, and the question of Iran's influence and relationship with the militias after the conflict will continue to be a critically important issue. Bearing in mind the forward deterrent logic of Iran's strategy via allies, as explicated in this chapter, the continued existence of the militias will be of much higher importance for Iran than a formal Iranian presence in Syria. Iran will thus support the Syrian regime in its increasing efforts to reassert its power and sovereignty and to fully indigenize the Syrian militias once the conflict subsides.

Over the years ahead, Iran's Syria policy will also be increasingly shaped by the United States' Iran strategy. Now that President Trump has pulled the United States out of the JCPOA and decided to exert maximum pressure on Iran, the Iranian threat perception of potential escalation has increased. Consequently, Tehran feels an urgent need to demonstrate its deterrence capacity, and the value and role of Syria as part of its forward deterrence will only increase. Iran–Syria relations will therefore continue to operate at a strategic level in the years to come.

References

Adler E (2009) Deterrence in the asymmetric-warfare era. In: Paul TV, Morgan P, Wirtz J (eds) Complex deterrence: Strategy in the global age. University of Chicago Press, Chicago, pp 85–109

Ahmadian H (2018) Will Iran, Turkey jointly confront US influence east of the Euphrates? (2 October 2018)

Al Jazeera (2018) Shamkhani: al-Su'udiya rafadat hudna Ramadaniya bi-l Yaman [Shamkhani: Saudi Arabia rejected a Ramadan truce in Yemen], 26 May 2018, http://www.aljazeera.net/programs/today-interview 26 May 2018

Al-Alam (2016) Aghaz-i buhran dar Suriyih bih rivayat-i Shahid Husayn Hamidani [The start of the Syrian crisis in the words of Shahid Hussein Hamidani], 26 December 2016, http://fa.alalam.ir/news/1902728

Al-Alam (2017) Basij-i mardumi nabud, imruz kishvar bih nam-i Suriyih nadashti'im [If it were not for the popular Basij, today we would not have a country with the name Syria], 22 November 2017, http://fa.alalam.ir/news/3168086/

Al-Alam (2018) Mufajat yakshifuha al-ra'is al-Asad fi liqa khas ma Qanat al-Alam' [President Assad reveals surprises in an exclusive meeting with Al-Alam TV], 12 June 2018

Al-Mayadeen (2016) Khayar al-Darura: Hizballah fi Suriya' [Al-Mayadeen documentary, option of necessity: Hezbollah in Syria], 23 January 2016, https://www.youtube.com/watch?v=p4zVpsfdUc8. 2016-01-23

Al-Mayadeen (2018) Hiwar khas ma' al-Amin al-Am li-Hizballah al-Sayyid Hasan Nasrallah' [Exclusive interview with the Secretary General of Hezbollah Seyed Hasan Nasrollah] (3 January 2018)

Al-Salhy S (2013) Iraqi Shi'ites flock to Assad's side as sectarian split widens, 19 June 2013, https://www.reuters.com/article/us-iraq-syria-militants/iraqi-shiites-flock-to-assads-side-as-sectarian-split-widensidUSBRE95I0ZA20130619

Arreguín-Toft I (2005) How the weak win wars: a theory of asymmetric conflict. Cambridge University Press, Cambridge

Asr Iran (2013) Ra'is-i Gharargah-i Ammar: Surye ustan-i si-o-panjum ast [Leader of the Ammar Base: Syria is the 35th province] (20 January 2013). Author's translation

Baram A (2014) Ideology and power politics in Syrian–Iraqi relations, 1968–1984. In: Ma'oz M, Yaniv A (eds) Syria under Assad: domestic constraints and regional risks. Routledge, New York, pp. 125–39

Barnard A (2011) Turkish leader says he has lost confidence in Assad, 28 August 2011, https://www.nytimes.com/2011/08/29/world/middleeast/29syria.html

Bassam L (2015) How Iranian general plotted out Syrian assault in Moscow, 6 October 2015, http://www.reuters.com/article/us-mideast-crisis-syria-soleimaniinsigh-idUSKCN0S02BV20151006

BBC (2018) Syria war: rebels "withdraw heavy weapons from Idlib buffer zone", 8 October 2018, https://www.bbc.com/news/world-middle-east-45783491

Black I (2013) Syria crisis: Saudi Arabia to spend millions to train new rebel force, 7 November 2013, https://www.theguardian.com/world/2013/nov/07/syria-crisis-saudi-arabia-spend-millions-new-rebel-force

Champion M, Ferziger J, Wainer D (2018) Israel, Saudis find common cause in warning of Iran expansionism, Bloomberg.com (18 February 2018), https://www.bloomberg.com/news/articles/2018-02-18/netanyahu-in-munich-speech-urges-west-not-to-appease-iran

Charbonneau L (2012) Exclusive: western report—Iran ships arms, personnel to Syria via Iraq, 19 September 2012, https://www.reuters.com/article/us-syria-crisis-iran-iraq/exclusive-western-report-iran-shipsarms-personnel-to-syria-via-iraq-idUSBRE88I17B20120919

Cubert H (1997) The PFLP's changing role in the Middle East. Routledge, London

Deutsche Welle (2018a) Dalil-i huaur-i Iran dar Suriye va himayat az Filistiniha bih rivayat-i Qasim Sulaymani [The reason for the presence of Iran in Syria and support for the Palestinians inthe narration of Qasim Sulaymani], 19 January 2018, https://p.dw.com/p/2r9Rs. Author's translation

Deutsche Welle (2018b) Zarif: Amrika dar masir-i tajziyih-yi Suriyih gam barmidarad' [Zarif: America is moving towards fragmenting Syria], 2 February 2018, https://p.dw.com/p/2svV5

Ehteshami A, Hinnebusch R (1997) Syria and Iran: middle powers in a penetrated system. Routledge, London, pp. 88–91

Ehteshami A, Hinnebusch R, Huuhtanen H, Raunio P, Warnaar M, Zintl T (2013) Authoritarian resilience and international linkages in Iran and Syria. In: Heydemann S, Leenders R (eds) Middle East authoritarianism: governance, contestation, and regime resilience in Syria and Iran. Stanford University Press, Stanford CA, p. 223

Fars News (2014) Taqavi dar Samira khun dad ta Tihran va Isfahan va Sistan khun nadahim [Taqavi gave blood in Samarra so we wouldn't have to in Tehran, Isfahan and Sistan] (29 December 2014)

Freedman L (2004) Deterrence. Polity, Cambridge

George A L, Smoke R (1974) Deterrence in American foreign policy: theory and practice. Columbia University Press, New York, p. 11

Gerges F (1996) Washington's misguided Iran policy. Survival 38(4):5–15

Gilbert L, Mohseni P (2011) Beyond authoritarianism: the conceptualization of hybrid regimes. Studies in Comparative International Development 46:270–97

Goodarzi J (2006) Syria and Iran: diplomatic alliance and power politics in the Middle East. Tauris, London

Gross Stein J (2009) Rational deterrence against "irrational" adversaries? No common knowledge. In: Paul T V, Morgan P, Wirtz J (eds) Complex deterrence: strategy in the global age. University of Chicago Press, Chicago
Hadian N (2015) Iran debates its regional role. Atlantic Council, Washington DC
Hannah J (2011) Responding to Syria: The King's statement, the President's hesitation. Foreign Policy, 9 August 2011, http://foreignpolicy.com/2011/08/09/responding-to-syria-the-kings-statement-the-presidents-hesitation/
Hirschfeld Y (2014) The odd couple: Ba'athist Syria and Khomeini's Iran. In: Ma'oz M, Yaniv A (eds) Syria under Assad: domestic constraints and regional risks. Routledge, New York, pp 105–124
Hunter S (1993) Iran and Syria: from hostility to limited alliance. In: Amirahmadi H, Entessar N (eds) Iran and the Arab world. Macmillan, London, pp. 198–216
Huntington S (1983) Conventional deterrence and conventional retaliation in Europe. International Security 8(3):32–56
ISNA (2012) Ja'fari: hamlih-ye pishdastanih nimikunim [Jaafari: we will not undertake a pre-emptive strike], 22 August 2012, https://www.isna.ir/news/0000178343/
ISNA (2016) Sardar Qasim Sulaymani: ma bih Suriyih razmandihi naburdihim [Commander Qasim Sulaymani: we have not taken combatants to Syria], 5 October 2016, https://www.isna.ir/news/95071409366/
ISNA (2018) Hazrat-i Ayatullah Khamini'i: hamlih be Suriyih jinayat ast [Ayatollah Khamenei: attack against Syria is a crime], 14 April 2018, https://www.isna.ir/news/97012508419/
Jahannews (2013) 'Intishar-i sawt va film-i sukhanan-i Hashimi alayhe Suriyih' [Publication of the sound and film of Hashemi's words against Syria] (23 Aug. 2013)
Jüde J (2017) Contesting borders? The formation of Iraqi Kurdistan's de facto state. International Affairs 93:847–66 (4 July 2017).
Juneau T (2018) Iran's costly intervention in Syria: a pyrrhic victory. Mediterranean Politics https://www.tandfonline.com/doi/abs/10.1080/13629395.2018.1479362
Kamil M I (2016) The Camp David Accords: a testimony. Routledge, London
Khaddour K (2016) Strength in weakness: the Syrian Army's accidental resilience. Carnegie Middle East Center, Washington DC, March 2016
Kurzman C (2012) The Arab Spring: ideals of the Iranian green movement, methods of the Iranian Revolution. International Journal of Middle East Studies 441, 2012, pp. 162–165
Landis J (2010) The US–Syria relationship: a few questions. Middle East Policy 17:64
Lebow R, Gross Stein J (2007) Beyond deterrence. In: Lebow R (ed) Coercion, cooperation, and ethics in international relations. Routledge, New York
Leverett F (2005) Inheriting Syria: Bashar's trial by fire. Brookings Institution Press, Washington DC, p. 12
Lieberman E (2012) Reconceptualizing deterrence: nudging toward rationality in Middle Eastern rivalries. Routledge, Abingdon
Marschall Ch (2003) Iran's Persian Gulf policy: from Khomeini to Khatami. Routledge, London, pp 142–145
Mashregh News (2018) Khabar-i Vilayati az Ghadam-i ba'di-ye jibhi-ye muqavimat dar Suriyih [News of Velayati of the Resistance's next steps in Syria], 13 April 2018, mshrgh.ir/846482
Middle East Eye (2018) US-led jets bombed pro-Assad forces advancing on Deir Ezzor: report, 30 April 2018, http://www.middleeasteye.net/news/us-jets-bomb-pro-government-fighters-syria-operation-1276052674
Milani M (2013) Why Tehran won't abandon Assad(ism). Washington Quarterly 36:79–93
Mohseni P (2013) The Islamic Awakening: Iran's grand narrative of the Arab uprisings. Middle East Brief no. 71. Brandeis University, Waltham, MA
Mohseni P (2015) Introduction: the Russian intervention in Syria. In: Mohseni P (ed) Disrupting the chessboard: perspectives on the Russian intervention in Syria. Belfer Center, Harvard Kennedy School, Cambridge, MA, pp 1–7, October 2015

Mohseni P (2016) Factionalism, privatization, and the political economy of regime transformation. In: Brumberg D, Farhi F (eds) Power and change in Iran: politics of contention and conciliation. Indiana University Press, Bloomington, pp 37–69

Mohseni P, Ahmadian H (2018) What Iran really wants in Syria. 10 May 2018

Mohseni P, Kalout H (2017) Iran's Axis of Resistance rises, 24 January 2017, https://www.foreignaffairs.com/articles/iran/2017-01-24/irans-axis-resistance-rises

Nafi B (2017) Iran's sectarian wars must be confronted, but not with more of the same. Middle East Eye (16 March 2017), http://www.middleeasteye.net/columns/irans-sectarian-wars-must-be-confronted-not-more-same-452011045

Nasrallah H (2018) Speech, Lebanon, Al Jazeera, (14 May 2018)

Norton A R (2009) Hezbollah: a short history. Princeton University Press, Princeton

Nye J S Jr. (1986) Nuclear ethics. Simon & Schuster, New York

Office for the Preservation and Propagation of the Works of Grand Ayatollah Seyyed Ali Khamenei (2011) Amir Mohebbian, Sinariuha-ye muhtamil-i tahdid alayhe Iran' [Possible threatening scenarios against Iran], 23 October 2011, http://farsi.khamenei.ir/others-note?id=17882

Office for the Preservation and Propagation of the Works of Grand Ayatollah Seyyed Ali Khamenei (2012) Didar-i Nukhust Vazir-i Turkiye ba Rahbar-i Inghilab' [The meeting of the Turkish Prime Minister with the Leader of the Revolution], 29 March 2012, http://farsi.khamenei.ir/news-content?id=19342

Office for the Preservation and Propagation of the Works of Grand Ayatollah Seyyed Ali Khamenei (2016) Bayanat dar didar-i jam'i az khanivadih-haye shuhadaye mudafi-i haram' [Speech in the meeting with a group of families of the martyrs defending the shrine], 25 January 2016, http://farsi.khamenei.ir/speech-content?id=32186

Office for the Preservation and Propagation of the Works of Grand Ayatollah Seyyed Ali Khamenei (2017a) Namih-i Sarlashkar Qasim Sulaymani bih Rahbar-i Inqilab darbarih-ye Payan-i Saytarihye Da'ish' [Commander Qasim Sulaymani's letter to the Leader of the Revolution about the end of ISIS' dominance], 21 November 2017, http://farsi.khamenei.ir/news-content?id=38253

Office for the Preservation and Propagation of the Works of Grand Ayatollah Seyyed Ali Khamenei (2017b) Pasukh-i Rahbar-i Inqilab bih namih-ye Sarlashkar Qasim Sulaymani darbarih-ye payan-I saytarih-ye Da'ish' [The Leader of the Revolution's response to the letter of Commander Qasim Sulaymani about the end of ISIS' dominance], 21 November 2017, http://farsi.khamenei.ir/message-content?id=38249

Office for the Preservation and Propagation of the Works of Grand Ayatollah Seyyed Ali Khamenei (2018) Videoclip: Duwran-i bizan va darru tamam shodih ast [The time for hit and run is over] http://farsi.khamenei.ir/video-content?id=29939. Author's translation

Okyay A S (2017) Turkey's post-2011 approach to its Syria border and its implications for domestic politics. International Affairs 93: 829–46

Ostovar A (2018) Iran, its clients, and the future of the Middle East: the limits of religion. International Affairs 94:1237–56

Phillips M (2011) President Obama: "The future of Syria must be determined by its people, but President Bashar al-Assad is standing in their way", 18 August 2011, https://obamawhitehouse.archives.gov/blog/2011/08/18/president-obama-future-syria-must-be-determined-its-people-president-bashar-al-assad

Qasim N (2010) Hizbullah: the story from within. Saqi, London

Rabinovich I (2008) The view from Damascus: state, political community and foreign relations in twentieth-century Syria

Ramazani R K (2001) Reflections on Iran's foreign policy: defining the "national interests. In: Esposito J, Ramazani R K (eds) Iran at the Crossroads. Palgrave, New York, pp 214–17

Ramazani R K (2013) Independence without freedom: Iran's foreign policy. University of Virginia Press, Charlottesville

Sadjadpour K (2018) 'Iran's real enemy in Syria', The Atlantic, https://www.theatlantic.com/international/archive/2018/04/iran-syria-israel/558080/. (16 April 2018)

Schelling T (2008) Arms and Influence. Yale University Press, New Haven CT, p 35
Sick G (1987) Iran's quest for superpower status. Foreign Affairs 65:703
Sobelman D (2017) Learning to deter: deterrence failure and success in the Israeli-Hezbollah conflict, 2006–16. International Security 41(3):151–96.
Stavridis J (2015) What to do about an imperial Iran. Foreign Policy (30 June 2015), http://foreignpolicy.com/2015/06/30/what-to-do-about-an-imperial-iran-middle-east-persia-regional-dominance/
Sweid R (2015) Kharif jaysh al-nizam al-Suri wa rabi' al-milishiat [The fall of the Syrian state's military and the spring of the militias], Al-Araby al-Jadid, 27 May 2015
Tabnak (2015) Rivayat-i Sardar Hamidani az nahvih-ye tashkil-i Basij-i Suriyih [Commander Hamidani's narration of the formation of the Syrian Basij] (26 January 2015)
Tabnak (2018) Ifshagari-ye Maqam-i Sipah az Nazar-i Ahmadinijad Darbare-ye Asad [IRGC official exposes Ahmadinejad's opinion about Assad] (20 February 2018)
US Department of Defense (2018a) Department of Defense press briefing by Colonel Dillon via teleconference from Baghdad, Iraq, 17 April 2018, https://dod.defense.gov/News/Transcripts/Transcript-View/Article/1496008/department-of-defense-press-briefing-by-colonel-dillon-via-teleconference-from/
US Department of Defense (2018b) Lead Inspector General report to the United States Congress: Operation Inherent Resolve (OIR) and Operation Pacific Eagle-Philippines (OPE-P), 6 August 2018, https://media.defense.gov/2018/Aug/15/2001954780/-1/-1/1/FY2018_LIG_OCO_OIR3_JUN2018_508.PDF
Vallentine M (2010) Lebanon, Syria: preparations for future conflict with Israel', https://worldview.stratfor.com/article/lebanon-syria-preparations-future-conflict-israel, p 232
Van Dam N (2011) The struggle for power in Syria: politics and society under Assad and the Ba'th Party. Tauris, London, p 67
Vignal L (2017) The changing borders and borderlands of Syria in a time of conflict, International Affairs 93:809–28
Wall Street Journal (2011) Syria opposition leader interview transcript, 2 December 2011, https://www.wsj.com/articles/SB10001424052970203833104577071960384240668
Wallace B, Cafarella J (2018) ISIS's second resurgence. Institute for the Study of War, Washington DC, 2 October 2018, http://iswresearch.blogspot.com/2018/10/isiss-second-resurgence.html
Yaari E (2017) Iran's ambitions in the Levant. Foreign Affairs (1 May 2017), https://www.foreignaffairs.com/articles/iran/2017-05-01/irans-ambitions-levant
Young Journalist Club (2016) Tuwsiye-ye Sayyid Hassan Nasrallah bih Sardar Hamidani' [Sayyid Hassan Nasrallah's advice to General Hamadani], 5 October 2016, https://www.yjc.ir/00ON1j

Dr. Hassan Ahmadian is an Assistant Professor of Middle East and North Africa studies at the University of Tehran and an Associate of the Project on Shi'ism and Global Affairs at Harvard University's Weatherhead Center for International Affairs. He is also a Middle East security and politics fellow at the Center for Strategic Research in Tehran. Dr. Ahmadian received his Ph.D. in Area Studies from the University of Tehran and undertook a Postdoctoral Research Fellowship at the Iran Project, Harvard Kennedy School Belfer Center for Science and International Affairs.

Dr. Payam Mohseni is the Former Director of the Iran Project at the Harvard Kennedy School Belfer Center for Science and International Affairs. He is also a Lecturer in the Department of Government at Harvard University and a Lecturer on Islamic Studies at the Harvard Divinity School where he teaches Iranian and Middle East politics. Dr. Mohseni is also a term member of the Council on Foreign Relations (CFR) in New York.

Part III
Deterrence of Non-State Actors

Chapter 14
Deterring Violent Non-state Actors

Eitan Shamir

Contents

Abstract The chapter examines the relevance and applicability of deterrence to violent non-state actors (VNSAs). VNSAs have become important players in the international system. Traditional deterrence theory and practice has limited utility against VNSAs due to their different characteristics to those of states that makes them less susceptive to deterrence strategies. Deterrence theory and practice has had to evolve and adapt to address these special traits of VNSAs. The chapter presents this conceptual evolution and the means and methods developed to deter VNSAs, highlighting both their advantages and shortfalls. It explains why states choose deterrence, even if not perfect, over other strategies. The Israeli case study then demonstrates how a state employs deterrence in relation to several VNSAs with diverse characteristics, levels of threat, political objectives, and military capability. The case study shows how Israel is designing a portfolio of deterrent strategies

E. Shamir (✉)
Political Science Department, The Begin Sadat Center for Strategic Studies (BESA Center), Bar Ilan University, Ramat Gan, Israel
e-mail: eitanshamir10@gmail.com

F. Osinga and T. Sweijs (eds.), *NL ARMS Netherlands Annual Review of Military Studies 2020*, NL ARMS, https://doi.org/10.1007/978-94-6265-419-8_14

tailored to each challenge, demonstrating a degree of deterrence flexibility that the state can apply. The chapter concludes that, while the option of deterring VNSAs is not ideal, it does offer a viable strategy for decision makers compared with a number of lesser alternatives.

Keywords Violent Non-State Actors (VNSAs) · Cumulative Deterrence · Tailored Deterrence · Israel · Hamas · Hizballah · ISIS · Al-Qaeda · Terrorism · Political Violence

14.1 Introduction: The Nature of the Problem

This chapter addresses the relevance and applicability of deterrence to violent non-state actors (VNSAs) and explores three questions in that regard: To what extent is deterrence effective on VNSAs? Which types of deterrence are more effective? What can we learn from historical experience in relation to VNSA deterrence? The answers to these questions are not merely theoretical but may also help policy makers decide whether and how to deter VNSAs. After a brief discussion of the general issue, the chapter explains the rise of VNSAs and explores various concepts of deterrence with regard to them, how these have evolved, and how they translate into practice. It then identifies some of the key principles for deterring VNSAs through an analysis of Israel's approach to Hamas and Hezbollah. The chapter concludes with a discussion of key lessons from deterring VNSAs for the broader theory and practice of deterrence.

VNSAs are defined here as either local or transnational organizations that challenge the established national or international political order and use organized violence in pursuit of their agenda. These organizations and their activities are normally considered illegal by both international organizations and most countries, with the exception of those states who openly support VNSAs that advance their own interests. VNSAs pursue organized political violence, such as terror and guerrilla warfare, in conjunction with other forms of political activities, such as diplomacy, information campaigns and (often criminal) economic activity, in order to finance their activities.

Most of the literature on addressing VNSAs falls under the category of "deterrence versus terrorism" and its findings are also relevant here. The concept of the VNSA allows for a broader perspective that encompasses organizations of various type and level of sophistication ranging from *ad hoc* bands of pirates in Somalia under a local warlord to Hizballah in Lebanon, which runs a state within a state and has military capabilities beyond those of many nations.[1]

[1]Thomas et al. 2005, pp. 9–10. On the general phenomena of VNSA; Mulaj 2010.

14.2 VNSAs in the International System: From Nuisance Level to Global Threat

In recent decades, VNSAs have substantially increased in number, sophistication and capability, becoming important strategic actors. Whether war is in a general decline is hotly debated within academic circles. Those who agree that war is in decline argue that the main causes for it are nuclear peace, the influence of international organizations and norms, the rising cost and destructiveness of wars, globalization and world interconnectivity, and the greater number of liberal democracies.[2] What is agreed is that, since the end of the Second World War and increasingly so following the end of the Cold War, there has been a sharp decline in state-on-state war, for the above reasons. Instead, at least one participant in most violent conflicts is a VNSA[3] and, in the major violent conflicts since the beginning of the twenty-first century, at least one player has been a VNSA. According to one inventory on the subject, all eight major conflicts have involved VNSAs, whether civil wars, insurgency situations, or conflicts involving groups acting as proxies for foreign state players.[4]

An important factor allowing VNSAs to thrive is the phenomenon of weak and/or failed states and the growing number of ungoverned regions in which terror groups, guerrillas, and criminal bands—singly or in various combinations—operate freely in the vacuum left by the state.[5] The US Fund for Peace think tank's Fragile State Index includes many countries—such as Afghanistan, Iraq, Libya, Nigeria, Pakistan, Somalia, Syria and Yemen—that serve as hubs for transnational terror and crime.[6] Even though these regions do not all pose the same degree of security risk, failed states generate terrorism, weapons proliferation, crime, energy insecurity, and regional instability that endangers international security.[7] One study likens the rise of VNSAs to past historical periods where weak and crumbling empires allowed "barbarians" to rise up and challenge them. Similarly, so the argument goes, contemporary VNSAs such as ISIS, Al-Qaeda, and the Taliban rise to power enabled

[2]Gat 2013, pp. 149–157.

[3]In fact, historically it this has always been true. However, the focus of policy makers and academic research has been on the major state-on-state wars. Since the end of the Second World War, the declining number of state-on-state wars, especially wars between great and medium powers, and the attention of policymakers and academics has turned to state-on-non-state wars. In the past, they were simply called "small wars", *guerrilla* in Spanish, *petites guerres* in French.

[4]Ray 2020.

[5]For the trend, list of countries, and definition, see: Fund for Peace nd. The working definition of a failed state I use here, following Weber, is a political entity without monopoly over the use of force, unable to enforce its sovereignty over its designed territory, and unable to deliver basic services. For this phenomenon in contemporary international relations, see Rothberg 2004.

[6]Fund for Peace nd.

[7]Stewart 2006, p. 49; Piazza 2008, p. 483.

by ungoverned spaces and the use of new technology which allows for mobility and effective use of violence.[8] This enablement is coupled with radical religious motivations that seek to undermine existing state structures and regimes. In more extreme cases, such as that of ISIS, they seek to replace present day states with different political entities based on the historical Islamic caliphate, as they see it.[9]

The fact that most contemporary violent conflicts involve VNSAs has influenced the conduct of war to such a degree that some scholars have labelled these *new wars* and argue that they are distinct from those of the past in the organization, culture, conduct, and objectives of the groups involved.[10] Van Creveld argued as early as 1991, in *On the Transformation of War*, that the nature of wars seen in previous centuries, consisting of state armies clashing on open battlefields, was fundamentally changing.[11] British General Rupert Smith—whose long career spanned the transition from the Cold War to "the War on Terror" following 9/11—later argued that wars as we knew them between developed modern states, industrialized wars, "no longer exist". Instead, what we experience now are "wars among the people", meaning that state militaries have to confront elusive VNSAs embedded within the population as opposed to well-defined state militaries distinct from the populous.[12]

VNSAs are generally not as resource-rich or well organized as states and so conflict is asymmetric. The aim of avoiding the impact of the enemy's main strengths is as old as the history of warfare itself, the weaker side opting for an indirect strategy of attrition instead of open pitched battles that lead to decisive results.[13] The ostensibly weaker side choosing to operate in difficult terrain, such as dense jungles or mountains, to offset the stronger side's advantages. More recently, VNSAs have opted to operate within dense urban environments that serve as cover for them.[14]

The "Revolution in Military Affairs (RMA)" in the 1990s enabled states to harness new military technologies originally developed for state-on-state wars but adaptable to effectively fight non-state wars. The main impact of these technologies is in their surveillance and detection capabilities which facilitate subsequent remote precision strikes that minimize casualties among one's own forces, as well as collateral damage. Using various combinations of surveillance equipment, drones, and precision missiles has become the preferred tactic of state militaries in fighting VNSAs. While developed countries have adopted these information-era technologies for warfare, the generally much poorer and less sophisticated VNSAs have developed their own parallel response, called the "O-RMA" (the other RMA) by Israeli General Itai Brun. Brun stated that O-RMA was a "loose concept that

[8]Grygiel 2018.
[9]University of Birmingham n.d..
[10]Kaldor 1999; Münkler 2005.
[11]Van Creveld 1991.
[12]Smith 2012, p. 2.
[13]Arreguin-Toft 2001; Gulsby 2010.
[14]Caforio 2008.

espoused a few key ideas and practices" based on the following components: Improving absorption capability in order to increase survivability and provide a breathing space for the 'weaker side'; creating effective deterrence in order to deter the 'stronger side' from attacking the 'weaker side' or shifting the war to more convenient areas in case this deterrent fails; and "winning the war by not losing it, while creating an attrition effect".[15]

These ideas have translated into operational principles with an emphasis on survivability (camouflage and deception, military personnel dispersal, concealment of military facilities within civilian facilities) coupled with the use of weaponry and operating methods that lead to a high number of military and civilian casualties such as suicide bombings and high-trajectory weapons. There is also an emphasis on negating the opponent's aerial supremacy through the use of both active and passive defence systems while also trying to drive the fight towards face-to-face combat where the technological edge states have is less significant. There is also great emphasis placed on propaganda.[16]

Studies have demonstrated the ability of VNSAs not only to innovate but also "to display multi-directional processes of innovation".[17] One has shown how even a localized and less sophisticated organization such as the Taliban has proven to be highly adaptable, innovative and resilient, effectively employing Improvised Explosive Devices (IEDs) and suicide bombers, all founded on O-RMA principles. The Taliban has continually refined its tactics by learning from both peers and opponents and has "clearly borrowed tactics from the war in Iraq, the Afghan civil war of the 1990s, and from Pakistani and al-Qaeda operatives".[18] Suicide bombers and IEDs are two examples of tactics developed and refined in Iraq and adopted by the Taliban for use in Afghanistan. Particularly significant innovation can be seen in the Taliban's constant attention to propaganda operations whereby they regularly seek to pre-empt US and NATO messaging on events with their own.[19]

The level of VNSAs' organizational and technological sophistication is variable, with the Shiite Lebanese Hizballah perhaps at the forefront. Supported by Iranian knowledge and materiel, the organization has evolved into a formidable component in the Lebanese political system and as a military power. Its military performance against the Israeli Defense Forces (IDF) in the 2006 Second Lebanon War was so impressive that one US analyst argued that their form of combat represented an altogether new category of "hybrid warfare" that uniquely blended regular and irregular war practices.[20] Hoffman goes on to say that "the term hybrid captures both their organization and their means" before adding:

[15]Brun 2010, p. 1.
[16]Brun 2010, pp. 549–551.
[17]Moghadam 2013, p. 467.
[18]Johnson 2013, p. 10.
[19]Johnson 2013, pp. 10, 21.
[20]Hoffman 2007a.

Hezbollah showed that it could inflict as well as take punishment. Its highly disciplined, well-trained, distributed cells contested ground and wills against a modern conventional force using an admixture of guerrilla tactics and technology in densely packed urban centers. Hezbollah's use of C–802 anti-ship cruise missiles and volleys of rockets represents a sample of what hybrid warfare might look like.[21]

To conclude, VNSAs have become formidable enemies to be reckoned with and often challenge states' authority. States are forced to choose a suitable policy and course of action on how to best cope with this challenge and minimize damages.

14.3 Why Deterring VNSAs is Challenging

There are five key factors that make VNSAs less vulnerable to deterrence than states. Firstly, there is the lack of a *clear address*, without a fully identifiable leadership governing a well-defined territory and population that is possible to communicate threats to or negotiate with.[22] While political and military systems typically feature clear and transparent hierarchies within states, this is seldom if ever the case with VNSAs, whose organization is more nebulous and command structures informal.

Secondly, and stemming from the first point, is the problem of handling communications. A major factor in the success of stable deterrence practices is the ability of both the defender and the potential attacker to communicate effectively. Whereas states have established means and protocols of communication, such as embassies and diplomatic channels on many levels, communication channels with VNSAs are much more tenuous.[23]

Thirdly, it is harder to hold VNSAs accountable for their actions than it is with states. As former U.S. Defense Secretary Rumsfeld put it, "we are fighting enemies who have no territories to defend and no treaties to honor."[24] Leaders of states, whether elected or not, are responsible for the people and property within their borders. Once these are threatened, a state's rulers must conduct careful cost-benefit analysis as to whether any particular action is worth the potential damage to their population, property, and even the regime itself. The degree to which these sorts of calculations also impose themselves on VNSAs varies but it is generally less pressing than it is for states. Fourthly, VNSAs' extremist character limits the effectiveness of deterrence. Many VNSAs have extremist ideologies and hence adopt violent methods to pursue their cause, often ready not only to take the lives of

[21]Hoffman 2007b, p. 59. Some military historians, however, argue that this is not a new phenomenon: see Murray and Mansoor 2012.

[22]Wilner 2013, p. 748; Trager and Zagorcheva 2006, pp. 87–88.

[23]Adamsky 2017, p. 176.

[24]Grygiel 2018, p. 115.

others but also to sacrifice their own if they believe it will advance it.[25] Finally, VNSAs are elusive in nature. Both leaders and operatives work underground, embedded in the population and/or transient secret locations.

14.4 Deterrence Theory and the Impact of VNSAs

Despite these five limiting factors, deterrence has been exerted against VNSAs' violent activity to partly if not entirely curtail its impact. As Trager and Arachova argue, "the claim that deterrence is ineffective against terrorist organizations is wrong."[26] This approach requires transcending the traditional concepts of deterrence outlined in the introductory section of this work.[27] A whole body of literature has emerged in the wake of 9/11 and the ensuing War on Terror that argues that deterrence against VNSAs can be effective,[28] but that the new strategic challenges involved require new concepts of that deterrence.[29]

Thomas Rid argues that the classic Cold War deterrence concepts of *absolute and specific deterrence* are not relevant for VNSAs. He instead suggests that it is much more useful to borrow the terms *restrictive deterrence* and *general deterrence* from criminological theory. While *absolute deterrence* applies when a potential aggressor has contemplated offensive action at least once and has been deterred completely in each instance, *specific deterrence* is designed for a single target with a relatively clear message given as form retaliation would take. *General deterrence*, refers to the deterrence of potential aggressors who have never experienced punitive consequences. *Restrictive deterrence*, by contrast, applies when an aggressor attempts to minimize the risk of punishment or its severity by restricting the quantity and/or quality of offensives. Thus, Rid offers the following analysis to explain why deterring VNSAs is more akin to deterring crime:

During the Cold War, deterrence was absolute and specific. Deterrence was specific in the sense that it was designed for only one recipient with a relatively clear message of what retaliation would look like…. The use of strategic nuclear weapons needed to be absolutely avoided in order for deterrence to work…. When the goal is deterring nuclear war, one single instance of deterrence failure would equal an existential catastrophe for several nations; when the goal is deterring political violence, one single instance of deterrence failure may equal merely a data point in a larger series of events…. If deterrence works successfully, the rate of

[25]Pape 2006.

[26]Trager and Zagorcheva 2006, p. 88.

[27]"Deterrence refers to the practice, the process or the situation in which one state relies on the prospect of harm to persuade an opponent not to engage in certain specified behavior." See the Preface to the present volume by Osinga and Sweijs.

[28]Trager and Zagorcheva 2006, p. 88; Wilner 2013, p. 743.

[29]Schmitt and Shanker 2011, p. 5.

violence in a certain area or jurisdiction will go down or level out, but it will rarely go to zero. In short, restrictive general deterrence is the rule.[30]

Research on deterring political violence forms the bulk of what is called the "fourth wave" in deterrence studies that emerged after the end of the Cold War and the rise of threats from VNSAs.[31] This new type of deterrence research focused on tackling non-state actors and the asymmetric threats they pose as cyber-warriors, pirates, and terrorists.[32]

14.5 Why States Choose to Deter VNSAs

Conflicts with VNSAs tend to be chronic and attritional in character. There are few strategic options states can pursue to win a conflict over a VNSA. A state can persuade the VNSA that diplomacy would benefit it more than violence. When there is such a will to compromise, some groups transition towards a political process and abandon violence as an instrument to advance their policy objectives. Such was the case with the Irish Republican Army (IRA) and Fatah, the dominant group in the Palestinian Liberation Organization (PLO) which, under the leadership of Mahmoud Abbas ("Abu Mazen"), decided to focus on diplomacy rather than violence.[33]

Another option for the state is to concede. Issues that may have seemed vital may no longer be so after much blood and treasure has been lost with no end to the conflict in sight. The state may thus choose to cut its losses, while the VNSA construes it a victory. This scenario is relevant when the conflict is not existential for the state involved as was the case with the British leaving Palestine in 1948, the Americans (and the French before them) quitting Vietnam in 1973, and the US and NATO forces rolling back from Afghanistan at the moment.[34]

Annihilation of the VNSA enemy is another option or neutralizing or killing enough of its leadership and personnel to render it operationally incapable. Such was the case with Sri Lanka's offensive against the Tamil Tigers in 2009 and Peru's against the Shining Path in 2013.[35] But sometimes, none of these options seem either attractive and/or feasible. Withdrawing is not always an option for some states where the conflict takes place on their own soil or the attacks are directed at the home front, such as with the United States and Al-Qaeda. Conversely, pursuing total defeat of the VNSA can cost too much blood and treasure and present great risks for political legitimacy and domestic popularity if the VNSA refuses to

[30]Rid 2012, p. 127.
[31]Knopf 2010.
[32]Wilner and Wenger 2012; Stein 2012; McMillan 2005; Harvey and Wilner 2012.
[33]Cronin 2009, pp. 35–57.
[34]Cronin 2009, pp. 73–93.
[35]Cronin 2009, pp. 115–145.

abandon violence as an instrument of policy. The remaining option for decision makers in this scenario is deterrence. It will not necessarily produce an end to the conflict, but it may allow it to be managed at an acceptable level of cost. The goal is to minimize impediments to state business.[36]

A common conceptual contradiction is what Wilner calls the "defeat-deter paradox", that is the incompatibility of the twin aims of destroying and deterring an opponent. This is so since deterrence is based on cost-benefit analysis; if the opponent feels it is going to be destroyed anyway, it cannot be deterred because it has nothing to gain by deferring its reaction.[37] Ways to overcome this paradox will be addressed in the next section; suffice it to say here that states have to be very clear about the strategies they employ and their correlative effect.

Another key point is that, with globalization and the proliferation of technology, the potential of VNSAs obtaining WMDs has become a nightmare scenario for many states. President Obama stated in 2010: "The single biggest threat to US security …would be the possibility of a terrorist organization obtaining a nuclear weapon."[38] While, according to experts, this scenario is much less plausible than it may seem to some, due to the many barriers to both obtaining and using such weapons, deterrence—even if not as robust as was the case in the Cold War—must be employed to minimize its likelihood.[39] At the moment the methods used to deter such attempts are no different to those used against any terrorist attack. These methods and their limitations will be examined in the next section.

14.6 How to Deter VNSAs: Strategic Approaches and Tactical Methods

In the previous section, I argued that the basic logic of deterrence can and should be applied to VNSAs, with some caveats. That said, deterring VNSAs requires a much more nuanced and sophisticated approach, as Jeffery Knopf has argued:

The area of greatest and most important consensus is that deterrence remains viable and relevant… Scholars also agree that the strategy is unlikely to be fool proof, but significant disagreements remain over how reliable it is likely to be with respect to different types of actors.[40]

Moreover, he argues that

…it still make sense to seek whatever leverage one can seek from the strategy [of deterrence] and while it is not possible to deter all VNSA all the time seeking

[36]Wilner 2013, p. 742.
[37]Wilner 2013, p. 742.
[38]Schmitt and Shanker 2011, p. 5.
[39]Jenkins 2012, pp. 133–134.
[40]Knopf 2010, p. 2.

ways to improve results at the margins remains important, but realistic understanding of the limits of deterrence is also necessary.[41]

In other words, states can use deterrence against VNSAs but should not expect a simple zero-sum game, as was the case with the Cold War between great powers. Employing deterrence against VNSAs has led to the development of a number of new approaches within overall deterrence theory.[42] The key questions to answer here are therefore: How has the theory evolved to cover the phenomena of VNSAs? What are the practices derived from these new ideas?

The key conceptual distinction employed with regard to VNSAs is captured in the opposing terms *deterrence by punishment* and *deterrence by denial*. Deterrence by punishment relates to a threat of great damage to an opponent should it engage in a particular behaviour. Deterrence by denial relates to convincing an opponent that it is unlikely to attain its immediate objectives at a reasonable cost to itself. When translating these concepts into practice, it becomes clear that one option, punishment, is more offensive in nature, while the other, denial, is more defensive. The threat of inflicting great harm can work effectively when a VNSA has high-value assets that can be identified and targeted. It is critical that the intent in the threat be credible and that the state has the capability to carry it out.

Leadership Targeting

The deterrer has a number of options before choosing this approach, including threats of assassinating or capturing leaders and/or key operatives. While there is an ongoing debate about the effectiveness of leadership decapitation, capable leaders are often central to a VNSA and leaders who are busy with self-preservation have less time to focus on offensive operations.[43] Recent studies have found leadership decapitation to resolve campaigns against VNSAs quicker and more positively. The intensity of a conflict is also likelier to decline following the successful removal of an enemy leader and VNSA attacks are less likely following successful leadership decapitations than after failed attempts.[44] Javier shows how successful drone attacks on leaders and operatives have impaired VNSAs' ability to operate.[45] Some of the mixed findings in the research regarding decapitation has been explained by Price, who found that leadership decapitation significantly decreases the life expectancy of terrorist groups, but that its effectiveness decreases with the maturity of the group, to a point where it may even have no effect at all.[46]

Other possible high-value targets are a VNSA's physical assets such as weapon caches, bunkers, tunnels, buildings, and training camps. Paradoxically, the more powerful a VNSA becomes, acquiring more capabilities in the process, the more

[41]Knopf 2012, p. 31.

[42]Wilner 2014, p. 448.

[43]For doubts regarding the utility of leader decapitation, see Staniland 2006; Jordan 2009; for arguments for targeted killing, see Byman 2006; Johnston 2012; and Jordan 2014.

[44]Johnston 2012.

[45]Jordan 2014, p. 25.

[46]Price 2012.

these capabilities offer targets for the deterrer in a way that becomes a "rich man's problem" for the VNSA. Some may see this as part of denial strategy, but denial relates to defensive means. Attacking capabilities serves both purposes: punishment and at least temporarily impairing the adversary's ability to carry out attacks. Israel-Hizballah deterrence relations provide a case in point. Israel attacked the organization's long-range missiles and main headquarters in the Dahiya Quarter of Beirut in 2006 and continues to issue threats to destroy the quarter again if provoked by Hizballah.[47]

MABAM

Unlike nuclear deterrence, where the emphasis is principally on the threat of force, with VNSAs there is use of actual force to serve as punishment and inhibition of future attacks. The IDF has recently intensified its practical application of this concept, naming it MABAM, a Hebrew acronym for the "operations between the wars". Ongoing covert operations are designed to destroy key assets of Israel's opponents—mainly those of Hizballah and other pro-Iranian militias—based in Syria.[48] The strategic intent is to achieve a cumulative undermining of the opponent's capabilities and thus avoid or at least postpone a much larger confrontation.[49] While these operations are still restricted in scope, they are part of a larger campaign to curb the growing threat to Israel's north, a threat which, if allowed to develop, might lead to eventual total war. More conceptually, Israel is trying to inhibit its opponents from developing specific capabilities in specific areas as opposed to letting them develop these capabilities and then deterring them from using them, as was the case in South Lebanon.

Not all VNSAs who claim to represent and defend a population are actually concerned about threats to their own people. Indeed, some organizations, such as ISIS in Raqqa and Mosul, have shown complete indifference to the fate of the population under their control, even using them as human shields. However, there are VNSAs who do rely on the support of their population and therefore have to be more sensitive toward their situation. Hizballah is one such example and Israel's "Dahiya Doctrine" presents not only a threat to the organization's military assets, but also to the fabric of the Shiite community that Hizballah, which is based in the Dahiya Quarter as well as south Lebanon close to the Israel border, vows to protect.[50] According to a 2006 UN report, 900,000 Lebanese, virtually all Shiites, fled their homes, while nearly 30,000 residential units were destroyed in the campaign.[51] Then, as now, Hizballah has to answer to its people and provide good reasons for inviting such harm to them by its actions. This is the reason behind

[47]Reut Institute 2009.

[48]Okbi 2017.

[49]IDF 2015.

[50]Khalidi 2014.

[51]United Nations n.d.

Israel's constant threats to it, communicated by senior IDF leaders, sending a clear message to Hizballah as to the cost of a war between the two.[52]

Deterrence by Denial

Deterrence by denial is based on defensive measures that necessarily involve less violence. According to Lawrence Freedman, their goal is "to control the situation sufficiently in order to deny the opponent strategic options."[53] Thus, the purpose is to foil terrorist attacks or at least reduce their impact and thereby lessen the motivation for subsequent actions.[54] The higher and more effective the barriers to attack are, the less likely it is that it will take place. Following the 9/11 attacks, the air travel industry implemented major security reforms, supplemented with new technologies, processes, and training of personnel. The few subsequent attempts to highjack or destroy planes have been thwarted and lessons quickly learned, as with the case of foiled "shoe bomber" Richard Reid in December 2001. Since that incident, passengers are often required to remove their shoes for further inspection when passing through airport security. Deterrence by denial includes a wide range of measures: an increased security presence on the streets and at borders and barriers; increased public awareness raising of terrorist threats; and deployment of technologies that help intelligence agencies monitor individuals, such as those for facial recognition and monitoring social media. Some of these measures can foil attacks in their embryo phase, taking pre-emptive action against key individuals and confiscating weapons material.

Another non-military means to curb a VNSA's operational ability is targeting its economic resources, especially its cash flow. A VNSA's operations and programs are often heavily dependent on its financial resources that originate from sponsoring states, individual contributions, or proceeds from crime, such as drug smuggling and human trafficking. As a result, VNSAs engage in extensive money laundering operations.[55] Sanctions against sponsors, whether states or individuals, and the freezing or confiscating of bank assets can help curb VNSAs' freedom to operate.

Deligitimization

Curbing VNSA activity through the battle of narratives offers another avenue. Although an aspect of denial strategy, its growing importance in today's world of social media has persuaded Wilner to label it separately as *deterrence by delegitimization*.[56] This is accomplished by undermining a VNSA's legitimacy as the defender of this or that faith or ideology, showing its leaders to be corrupt or not genuinely caring about the people they purport to represent.

[52]Nachmias 2018.

[53]Freedman 2004, p. 37.

[54]Trager and Zagorcheva 2006, p. 106.

[55]Cox 2011.

[56]Wilner 2014, p. 449.

Intrawar Deterrence

Another strategy is *narrow deterrence*, which aims to limit VNSAs' activities by deterring the deployment of certain types of weaponry or campaign conduct, such as chemical warfare, using specific threats of devastating retribution.[57] This approach relates to Alex Wilner's concept of *intrawar deterrence*. Like its Cold War inter-state predecessor, *intrawar deterrence* sees it as feasible to deter particular aspects of a militant group's behaviour while simultaneously engaging in military operations geared toward their ultimate destruction.[58] This allows one to overcome the "defeat-deter paradox" already mentioned.[59]

Triadic Deterrence

Another approach is to limit VNSAs' activity through *indirect deterrence*, or *triadic coercion*, putting pressure on the state that is either sponsoring or harbouring the VNSAs.[60] This can be in form of diplomatic and/or economic sanctions or even direct military threats. Turkey used military threats against Syria in 1998, for example, massing troops on the Syrian border and threatening to start a war should Damascus continue to provide a safe haven for the Kurdish PKK and its leader. During the first half of the 1950s, Israel conducted punitive raids against Jordanian and Egyptian military targets for allowing and encouraging the Palestinian *Fedayeen* to make cross-border raids against Israel. During 2018, the Indian Army entered Pakistan-administered Kashmir, retaliating against the Pakistani military for harbouring militant Islamic groups such as Jaish-e-Mohammed.

Cumulative Deterrence

Deterring NVSAs often requires the use of calibrated force to signal one's intentions to other side. The underlying assumptions behind this are different from those of classical nuclear deterrence. In the latter, the use of force is seen as a total failure of deterrence. As Rid puts it: "the first common assumption [regarding deterrence] is theoretical: that the role of deterrence is to avoid all adversarial offensive action, and that once force is used, deterrence has failed."[61] The concept of *cumulative deterrence* implies that deterring VNSAs requires an assortment of measures of both the punishment and denial types, both the use and the threat of attacks to various degrees of escalation. It is an approach that recognizes that results will not be immediate but longer term. Cumulative deterrence theory sees deterrence not for binary, either-or outcomes. Deterrence is created but also gradually deteriorates and so must be constantly renewed in order to be maintained. It is based on the simultaneous use of threats and military force over the course of an extended conflict. The response to attacks should be immediate, certain, and the amount of

[57]Freedman 2004, pp. 32–33.
[58]Wilner 2014, pp. 449–450.
[59]Wilner 2013, p. 74.
[60]Knopf 2012, pp. 33–34; Pearlman and Atzili 2018.
[61]Rid 2012, p. 125.

force properly calibrated to that attack.[62] Long campaigns against VNSAs, Almog writes:

> …would build on victories achieved over the short, medium, and long terms that gradually wear down the enemy. It would involve a multi-layered, highly orchestrated effort to inflict the greatest damage possible on the terrorists and their weapon systems, infrastructure, support networks, financial flows, and other means of support.[63]

During the Second Palestinian Intifada (2000–2005), Israel faced continual waves of suicide bomb attacks from various Palestinian organizations and employed a mixture of deterrence by both punishment and denial against the main organization leading the attacks, Yasser Arafat's PLO.[64] Offensive measures, such as assassinating operatives, were carried out in conjunction with denial measures such as armed guards on public buildings, the construction of a security barrier, surveillance of suspects, and the disruption of the suicide bomb "production line". The key to success here was intelligence, both traditional human intelligence and more technologically based approaches. The strategic aim was not annihilation of the adversary, but rather shaping and moderating its behaviour over time and shifting its strategic goals away from direct conflict and toward political settlement.[65]

Tailored Deterrence

We have observed that deterring VNSAs probably requires more nuanced methods than deterring states. In practice, states have to smartly combine measures against VNSAs, the exact mix being dependent on the deterrer's capabilities and objectives, the general context, and the nature of the VNSA's challenge. To remain effective, the deterrer must adapt its measures to changing circumstances, especially as the VNSA develops effective countermeasures for its vulnerabilities. If VNSAs are different from states and approaches to them must be bespoke, one needs to understand each VNSA's hierarchy of values and vulnerabilities to know in each case areas to target. Each VNSA needs to be studied in terms of specific vulnerabilities and how they are adapted over time. This is the idea of *tailored deterrence*, defined as "tailored in character and emphasis to address … fundamental differences in the perceptions and resulting decision calculus of specific adversaries in specific circumstances".[66] This requires broader knowledge than operational intelligence: It requires a deep understanding of the VNSA's values and beliefs.

The art of deterring VNSAs is a complex one, with no single concept or approach providing a comprehensive answer. To effectively deter VNSAs, states need to employ an ever-evolving mix of concepts, to understand their adversaries,

[62]Rid 2012, pp. 139–141.
[63]Almog 2004, p 6.
[64]Wilner 2013, pp. 758–759.
[65]Almog 2004, p. 9.
[66]Lantis 2009, p. 470.

and to master the practices required by each different approach. The next section examines Israel's experience in relation to three different VNSAs. Unable to defeat them, Israel has employed cumulative deterrence but has also tailored its approach to each VNSA specifically.

14.7 Tailored Deterrence: Israel's Deterrence Relations with Hamas and Hizballah

Israel's Experience

Israel has long and varied experience of confronting VNSAs with the use of deterrence always a major part of its strategy to curb the threat posed. The Israeli experience thus provides for a rich case study on the different aspects of deterring VNSAs, as Adamsky has pointed out:

> Traditionally, the Israeli case has been a natural choice of inquiry for experts dealing with nonnuclear deterrence and intra-war coercion. The literature turned to the Israeli experience because of the unparalleled pool of empirical evidence that offered a unique data set enabling the testing of conventional deterrence postulates. Due to an uninterrupted utilization of this strategy, the Israeli case still enables the refinement of insights for both deterrence theory and policy.[67]

Jews living in the Ottoman provinces that later became Israel were often targets of attacks by Arab neighbours prior to the inception of Zionism. These attacks were initiated for economic gain (theft) or religious reasons. After the British recognition of the Jewish right to self-determination (1917), foiling the future establishment of a Jewish state became a further reason to attack the Jews. The initial reactions to Arab attacks were by and large defensive, such as hiring guards to defend village perimeters. The Zionist leader Jabotinsky presented his metaphor of the "Iron Wall" as early as 1923.[68] Jabotinsky argued that the basic asymmetry of the two communities' size ruled out a decisive "once and for all" Jewish defeat of the Arabs. Therefore, the Jews' only chance of survival was to thwart attacks by the Arabs until the latter gave up and settled for co-existence. Though the terms were not yet coined, Jabotinsky was laying the foundation for a strategy based on deterrence by denial and cumulative deterrence. From the mid-1930s onwards, military leaders such as Yitzhak Sadeh, a former Red Army officer and founder of the Palmach (Striking Companies) and Orde Charles Wingate, a British military officer expert in irregular warfare who established the SNS (Special Night Squads), promoted Jewish military activism in the form of punitive raids against the Arab irregulars.

Israel's defence doctrine in the 1950s divided the Arab threat into two: The "fundamental threat" of a high-intensity war with Arab state militaries and the "routine threat" of continuous, low-intensity, small-scale, irregular warfare against

[67] Adamsky 2017, p. 159.

[68] Jabotinsky 1923.

military and civilian targets to wear down Jewish resolve to remain in Israel. While the focus of this paper is not on the high intensity threat, it suffices to say that conventional deterrence serves as a foundational concept in Israel's military doctrine to counter both of these threats.[69]

While the focus of Israel's security community in its first five decades was on the high intensity threat due to its existential menace, they also continuously countered various forms of attack by Palestinian VNSAs. These have continued in many forms, such as cross-border raids, rocket attacks, the planting of mines and explosives, the hijacking of civilian buses and airplanes and, latterly, suicide bombings against civilian and military targets. Israel's countermeasures have included a mixture of both denial and punishment deterrence. Denial measures have included border barriers and patrols, enhancing civilian awareness and training. Deterrence by punishment has been carried out through special units and detailed intelligence that has enabled operations against headquarters, training bases, and weapons caches, as well as the assassination of leaders.

While the end of the twentieth century saw a lower probability of a military attack by Arab states, it also witnessed a dramatic rise in the threat from three VNSAs: The Gaza-based Palestinian Hamas, the Lebanese Shiite Hizballah, and the West Bank Palestinian Fatah organization. Israel's disengagement from Lebanon in 2000 and Gaza in 2005 left voids that resulted in Hizballah becoming the most powerful organization in Lebanon and Hamas the *de facto* ruler of Gaza. During the Second Palestinian Intifada, Fatah also led a violent campaign against Israel, but since Abbas became PLO chairman in 2004, he has conducted a policy of non-violence.

Both Hizballah and Hamas are state sponsored. Iran militarily supports Hizballah and, to a lesser extent, the Sunni Hamas; Hamas, however, also enjoys economic and diplomatic support from Sunni states such as Turkey and Qatar. Both VNSAs seek to sustain the conflict with Israel despite Israel's disengagement from Lebanon and Gaza, their stated goal being "the liberation of Palestine". Meanwhile a delicate deterrence balance is maintained, disrupted by occasional spikes in violent exchanges.

Despite many similarities between the two VNSAs, Israel's deterrence approach has proved to be, thus far, much more stably pursued in the case of Hizballah than that of Hamas. With the former, there has only been one sustained period of violent escalation (2006), whereas there have been three major episodes of clashes (2008, 2012, 2014 and other minor ones in between) with the latter. The two are similar in certain respects, but important differences exist that influence Israel's deterrence strategy.

Tailored Deterrence Towards Hizballah

Hizballah can be described as a "state within a state". Its two main sources of power, Iranian patronage and the support of the largest ethnic-religious community

[69]Hecht and Shamir 2016, p. 123.

in Lebanon, the Shia, are also its two main sources of vulnerability. The Shia community is concentrated in three main areas of Lebanon and so it is possible to focus retaliatory action on such areas. Iran, the main investor in Hizballah capabilities, wants to retain Hizballah as a deterrent against potential Israeli operations against its nuclear facilities. Following the Israeli withdrawal from Lebanon, Hizballah has continually provoked Israel mainly in order to maintain its image as the leader of the "resistance".

In July 2006, in response to the killing and abduction of its soldiers, Israel launched an all-out attack on Hizballah. The result was massive destruction and loss of life in Shiite Hizballah areas. Iran was also unhappy with Hizballah wasting Iranian resources in, from its perspective, a pointless war. Hizballah's achievements in the war in fact boosted its reputation for holding its own against the mighty IDF and being able to strike inside Israel, but the price it paid for that was high. Hizballah leader Hassan Nasrallah, in an apologetic statement, subsequently admitted that he would not have ordered the abductions had he known the price.[70]

Since 2006, quiet has been almost continuously maintained on the Israeli-Lebanese border. Hizballah's military capabilities in general and ability to strike Israel's home front in particular have increased dramatically, but so too have Israel's. The price of any future war would be substantial for either side and this has led to a stable mutual deterrence relationship.[71]

Tailored Deterrence Towards Hamas

Hamas is militarily much weaker and Gaza's socio-economic situation dire. Paradoxically, it is this position of weakness that has allowed Hamas to continue attacking Israel. Hamas was founded as a religious movement for the welfare and education of poor Palestinians, adding political and armed activity against the Fatah-dominated PLO and Israel only in 1987. Hamas's declared long-term goals are to replace Fatah as the leader of the Palestinian people and to destroy Israel.

Fatah has dominated the Palestinian Authority (PA) since the latter was established, but increasingly Palestinians perceive it as detached from them and self-indulgent, leading to increasing support for Hamas. In January 2006, Hamas won a majority in the parliamentary elections and formed a government. This led to Fatah more-and-more violently resisting Hamas's democratic assumption of power, which led to a summer 2007 split of the PA into two entities: Gaza ruled by Hamas and the West Bank ruled by Fatah. Each entity behaves towards Israel distinctively and Israel responds to each distinctively too.

Since Israel withdrew completely from Gaza, its rulers behave as if it were a state. Israel also treats Hamas as it would treat any government. Regardless of who initiates any terrorist attack from Gaza into Israel, Israel holds Hamas responsible for it and retaliates against it, demanding it hold other smaller organizations in check. Whenever the frequency and/or severity of attacks from Gaza reaches a

[70]Nasrallah 2006.

[71]Sobelman 2017.

certain point, a phenomenon termed "deterrence erosion" in Israel's strategic parlance, Israel moves into "escalate to deescalate" mode by launching larger-scale military operations with the stated objective of "restoring deterrence", success being measured by the consequent reduction in attacks emanating from Gaza.[72] This series of operations—"Summer Rains" (June–November 2006), "Hot Winter" (February 2008), "Cast Lead" (December 2008), "Defensive Pillar" (November 2012) and "Protective Edge" (Summer 2014), all colloquially termed "mowing the grass" but officially "deterrence operations"—has indeed gradually reduced the frequency and severity of such attacks.[73]

However, Israel's limited objectives in these operations are defined by a lack of more optimal alternatives. Israel does not wish to reconquer Gaza and govern its population. Destroying Hamas's military power and ability to govern would create a vacuum to be filled with other, less tamed organizations that would necessitate continuous direct Israeli action.[74] Understanding Israel's reluctance to destroy it and the point at which Israel will decide to escalate its response is what both enables and determines Hamas's freedom of action to attack Israel or to allow other groups to do so. The price it pays in relation to Israel's response must be acceptable, however. Thus in November 2012, Hamas did not want an escalation and quickly sought a compromise with Israel to end Operation Defensive Pillar. However, in the summer of 2014 Hamas needed an escalation to improve its dramatically deteriorating financial situation as a result of a series of actions by Iran, the PA and Egypt which had prevented it from paying its employees and funding other activities critical to its governance. Hamas hoped that it could force conciliatory responses from Israel if it sustained combat over a lengthy period and was willing to pay a much higher price in casualties from such a lengthy, intensive war.[75]

Within Hamas there is constant debate about the cost of maintaining public support for its aggressive policy towards Israel. On the one hand, the consistently dire economic situation, the level of civilian casualties, and the damage to property are deemed useful for Hamas's propaganda campaign against Israel. On the other, Hamas must be careful not to create a popular backlash against its regime. This creates a measure of deterrence for Hamas and enables Israel to provide succour, directly (and indirectly via Egypt and Qatar), in return for fewer attacks.

A much lower intensity of attacks on Israel is evidence of the cumulative success of Israel's strategy. So too is Hamas's response to Israel's escalated attacks on its rival group in Gaza, the Palestinian Islamic Jihad. In November 2019, after a number of rocket attacks by this group and departing from its policy of targeting Hamas for every terrorist attack emanating from Gaza, Israel focused its military action on Islamic Jihad in a two-day exchange of rockets and bombs (Operation

[72]Shamir and Hecht 2014, p. 83.

[73]Inbar and Shamir 2014; Adamsky 2017, p. 169.

[74]Shamir and Hecht 2014, p. 83.

[75]Shamir and Hecht 2014, pp. 82–83.

Black Belt). Hamas, also deviating from its past policy, did not join the fray, despite being called a traitor by other groups in Gaza.

In the West Bank, Israeli policy is different. Palestinian terrorist attacks there are less well-organized and the vast majority also less deadly (being mostly petrol-bombs thrown at passing Israeli cars). Israeli forces are also more embedded within the local population and able to operate directly against terrorists.[76] However, the phenomenon of deterrence is apparent in that Fatah (and the PLO) which governs the PA prefers not to openly engage in attacks on Israel. Indeed its military often assists Israel in preventing attacks or apprehending attackers.

Table 14.1 summarizes the differences between the two organizations and various strategic approaches tailored by Israel in its efforts to deter offensive actions.

14.7.1 Israel's Experience

14.8 Case Study Analysis

The Israeli case study demonstrates that in relations between state and VNSA there are cases where either side may lack the capacity and/or will, despite its ideology and rhetoric, to annihilate the other. In these cases, deterrence becomes a useful strategy that allows for co-existence and lowers the level of violence. The form of the deterrence and its sustainability depend on structural variables as well as context across case and time. Thus, the IDF intelligence community constantly maps and monitors its various adversaries' weak points and prepares what it calls "maps of pain" to inform Israel's threats to each.[77]

The more organized and developed a VNSA is, the more it acquires valuable assets over time. As it becomes responsible for territories and the people within them, it adopts state-like behaviour. However, different geopolitical aspects (such as sponsors and alliances, the stability of VNSA and its rule), as well as historical circumstances, long and short-term objectives, ideology and religion, all shape different models of deterrence. This explains why Israel's deterrence relations with Hamas are so different from those it has with Hizballah and Fatah.

[76]Israeli Security Agency n.d..

[77]Frisch 2017.

Table 14.1 Israel's deterrence relationship with VNSAs: main characteristics (*Source* The author)

VNSA	Dimension	Key characteristics	Strategy employed
Hizballah, Lebanon	Political organization Sponsor(s) Military strength Objectives	State within a state Iran Highly developed Competing interests: (Lebanese, Iranian, resistance to Israel) Will to act against Israel if ordered to by Iran	Mutual deterrence; Agreed red lines; Use of aggressive rhetoric, demonstration of capabilities; Covert military operations in Syria outside the "agreed area"
Hamas, Gaza Strip	Political organization Sponsors Military strength Objectives	"Mini state" governs defined territory, population Less committed, more diverse: Iran, then Egypt, then, Turkey and Qatar Medium developed military capabilities Long term vision: Liberate Palestine under Hamas; short term: Leading Palestinian "resistance" to Israel Limited attacks on Israel's border villages and towns	Contain and compel; measured responses to provocation Large military in order to compel Hamas to change its behavior Israel's strategy aims to weaken but not replace Hamas Hamas provides one "address"
Fatah, West Bank (Now PA)	Political organization Sponsors Military strength Objectives	From VNSA to partially recognized state (PA) Various sponsors mainly Arab states Weak military capabilities, mainly small arms Long term: Palestinian state; Short term: International legitimacy, consolidating gains in Territories; Shift from violence to diplomacy	Israel compels and deters Fatah through economic, diplomatic means Israel's security forces cooperate with PA's official security forces; Israel retains operational freedom to act in the West Bank Conflict with PA mostly managed diplomatically, non-violently

14.9 Conclusions

Deterrence in international relations is as old as civilization itself. In the ancient world, one city was razed to the ground for others to witness and so surrender without a fight. Prisoners of war were executed, but some spared and sent to convince others to surrender without a fight so as to avoid that fate. However, it was only during the Cold War and the nuclear age that deterrence became a key strategy, probably the only possible strategy in such a world. Sophisticated deterrence theory has developed since then and has been extended to encompass state-on-state deterrence.

Following three waves of academic literature on deterrence, "fourth wave" deterrence literature evolved in the wake of 9/11 and focused on terrorism.[78] More specifically, it focused on Al-Qaeda, a transnational organization with a radical Islamist agenda originating in the Arab World.[79] As a result of their special character, VNSAs such as this presented many challenges to established deterrence theory. The theory had to evolve and so too did the practice. Unlike nuclear deterrence, it was often the case that practice fed and even led theory. Deterring VNSAs is like deterring crime and, after trial and error, successful practices have been developed and improved upon before being conceptualized as such. Some practices, such as leadership decapitation, are still controversial today.

The dynamism of deterrence *vis-à-vis* VNSAs has prompted many innovations, both practical and theoretical. The harnessing of many technologies originally intended for state-on-state war, such as attack helicopters and drones armed with precise anti-tank guided missiles to conduct leadership decapitation is just one example. The use of cyber technology, facial recognition the use of information and social media surveillance has also become paramount for this type of conflict, as the battle of narratives is key. VNSAs have also shown a remarkable ability to evolve organizationally and technologically and are often quicker to adapt and more agile than states. They are also able to develop their own concepts such as "victory through non-defeat".

There is no question that, in developing the theory of deterrence against VNSAs, the boundaries of the original concept of it is sometimes stretched to the limit. Some may even question whether what states call deterrence has become something else altogether. For example, while Israel framed its Second Lebanon War as an operation designed to strengthen its deterrence, some observers argued the operation was more simply about revenge.[80] However, it is also true that, in order to deal with VNSAs and their peculiarities, the theory and practice of deterrence will likely continue to evolve and adapt. As VNSAs remain important actors in the international system, deterrence, while imperfect, will continue to provide states with viable strategies to contain VNSAs' violent activity.

References

Adamsky D (2017) From Israel with deterrence: strategic culture, intra-war coercion and brute force. Security Studies 26.1:157–184

Almog D (2004) Cumulative deterrence and the war on terrorism. Parameters 34(4):4–19

Arreguin-Toft I (2001) How the weak win wars. International Security 26.1:93–128

Brun I (2010) While you're busy making other plans – the 'other RMA'. Journal of Strategic Studies 33.4:535–565

[78]Lupovici 2010, p. 718.

[79]Wilner 2014, p. 439.

[80]Löwenheim and Heimann 2008.

Byman D (2006) Do targeted killings work? Foreign Affairs 85.2:95–111
Caforio G (2008) The asymmetric warfare: in search of asymmetry. Management, Peace Economics and Development 7:7–23
Cox DW (2011) Introduction to money laundering deterrence. Wiley, London
Cronin AK (2009) How terrorism ends: understanding the decline and demise of terrorist campaigns. Princeton University Press, Princeton NJ
Freedman L (2004) Deterrence. Polity, Cambridge
Frisch H (2017) Hizballah and Hamas maps of pain and the required strategy
Fund for Peace (n.d.) Fragile State Index 2015. http://fsi.fundforpeace.org/rankings-2015. Accessed 4 October 2016
Fund for Peace (n.d.) Fragile and Conflict Affected States. https://fundforpeace.org/what-we-do/fragile-and-conflict-affected-states. Accessed 24 March 2020
Gat A (2013) Is war declining–and why? Journal of Peace Research 50.2:149–157
Grygiel J J (2018) Return of the barbarians: confronting non-state actors from ancient Rome to the present. Cambridge University Press, Cambridge
Gulsby S A (2010) Strategic asymmetric deception and its role in the current threat environment. Journal of Strategic Security 3.1:65–70
Harvey F, Wilner A (2012) Counter-coercion, the power of failure, and the practical limits of deterring terrorism. In: Wenger A, Wilner A (eds) Deterring terrorism: theory and practice. Stanford University Press, Redwood, CA, pp 94–114
Hecht E, Shamir E (2016) The case for Israeli ground forces. Survival 58.5:123–148
Hoffman F G (2007a) Conflict in the 21st century: the rise of hybrid wars. Potomac Institute for Policy Studies, Arlington
Hoffman FG (2007b) Preparing for hybrid wars. Marine Corps Gazette 91.3:57–61
Inbar E, Shamir E (2014) 'Mowing the grass': Israel's strategy for protracted intractable conflict. Journal of Strategic Studies 37.1:65–90
Israeli Defense Forces (2015) MABAM: IDF Chief of the General Staff, 'IDF Strategy' August 2015 [text in Hebrew]. https://www.idf.il/media/34416/strategy.pdf. Accessed 10 April 2020
Israeli Security Agency (n.d.) Monthly Reports. https://www.shabak.gov.il/english/publications/Pages/monthlyreports.aspx. Accessed 21 March 2020
Jabotinsky V Z (1923) The iron wall [text in Russian]. Razsviet 4 November 1923
Jenkins B M (2012) The terrorist perception of nuclear weapons and its implications on deterrence. In: Wenger A, Wilner A (eds) Deterring terrorism: theory and practice. Stanford University Press, Redwood CA, pp 117–135
Johnson T H (2013) Taliban adaptations and innovations. Small Wars and Insurgencies 24.1:3–27
Johnston P B (2012) Does decapitation work? Assessing the effectiveness of leadership targeting in counter-insurgency campaigns. International Security 36.4:47–79
Jordan J (2009) When heads roll: assessing the effectiveness of leadership decapitation. Security Studies 18.4:719–755
Jordan J (2014) The effectiveness of the drone campaign against Al-Qaida Central: a case study. Journal of Strategic Studies 37:4–29
Kaldor M (1999) New and old wars: organized violence in a global era. John Wiley & Sons, Hoboken NJ
Khalidi R I (2014) From the editor: the Dahiya Doctrine, proportionality, and war crimes. Journal of Palestine Studies 44.1:5–13
Knopf J W (2010) The fourth wave in deterrence research. Contemporary Security Policy 31.1:1–33
Knopf J W (2012) Terrorism and the fourth wave in deterrence research. In: Wenger A, Wilner A (eds) Deterring terrorism: theory and practice. Stanford University Press, Redwood, CA, pp 31–45
Lantis J S (2009) Strategic culture and tailored deterrence: bridging the gap between theory and practice. Contemporary Security Policy 30:3:467–485
Löwenheim O, Heimann G (2008) Revenge in international politics. Security Studies 17.4:685–724

Lupovici A (2010) The emerging fourth wave of deterrence theory: toward a new research agenda. International Studies Quarterly 54.3:705–732
McMillan J (2005) Treating terrorist groups as armed bands: the strategic implications. In: Purcell J S, Weintraub J D (eds) Topics in terrorism: toward a transatlantic consensus on the nature of the threat. Atlantic Council, Washington DC, pp 23–34
Moghadam A (2013) How al-Qaeda innovates. Security Studies 22.3:466–497
Mulaj K (2010) Violent non-state actors in world politics. Columbia University Press/Hurst, New York
Münkler H (2005) The new wars. Polity, Cambridge
Murray W, Mansoor P R (2012) Hybrid warfare: fighting complex opponents from the ancient world to the present. Cambridge University Press, Cambridge
Nachmias R (2018) Hizballah versus Northern Command Chief: Israel will collapse. https://www.ynet.co.il/articles/0,7340,L-3605238,00.html. Accessed 18 March 2020
Nasrallah H (2006) Interview on Lebanese New TV (NTV). 27 August 2006
Okbi Y, Ahronheim A (2017) Reports: Israeli aircraft struck an Iranian base outside Damascus, Jerusalem Post 2. https://www.jpost.com/Arab-Israeli-Conflict/Reports-Israeli-aircraft-struck-an-Iranian-base-outside-Damascus-515789. Accessed 24 March 2020
Pape R A (2006) Dying to win: the strategic logic of suicide terrorism. Random House, New York
Pearlman W, Atzili B (2018) Triadic coercion: Israel's targeting of states that host non-state actors. Columbia University Press, New York
Piazza J A (2008) Incubators of terror: do failed and failing states promote transnational terrorism? International Studies Quarterly 52.3:483
Price B C (2012) Targeting top terrorists: how leadership decapitation contributes to counterterrorism. International Security 36.4:9–46
Ray M (2020) Eight deadliest wars of the 21st century. https://www.britannica.com/list/8-deadliest-wars-of-the-21st-century. Accessed 18 March 2020
Reut Institute (2009) The Dahiya Doctrine (text in Hebrew). http://reut-institute.org/he/Publication.aspx?PublicationId=3672. Accessed 24 March 2020
Rid T (2012) Deterrence beyond the state: the Israeli experience. Contemporary Security Policy 33.1:124–147
Rothberg R I (2004) When states fail: causes and consequences. Princeton University Press, Princeton NJ
Schmitt E P, Shanker T (2011) Counterstrike: the untold story of America's secret campaign against al-Qaeda. Macmillan, New York
Shamir E, Hecht E (2014) Gaza 2014: Israel's attrition vs Hamas' exhaustion. Parameters 44.4:81–90
Smith R (2012) The utility of force: the art of war in the modern world. Penguin UK, London
Sobelman D (2017) Learning to deter: deterrence failure and success in the Israel-Hezbollah conflict, 2006–16. International Security 41.3:151–196
Staniland P (2006) Defeating transnational insurgencies: the best offense is a good fence. Washington Quarterly 29:21–40
Stein J G (2012) Deterring terrorists not terrorism. In: Wenger A, Wilner A (eds) Deterring terrorism: theory and practice. Stanford University Press, Redwood, CA, pp 46–66
Stewart P (2006) Weak states and global threats: fact or fiction? Washington Quarterly 29.2:49
Thomas S S et al (2005) Warlords rising: confronting violent non-state actors. Lexington Books, Oxford
Trager R F, Zagorcheva D P (2006) Deterring terrorism: it can be done. International Security 30.3:87–123
United Nations (n.d.) United Nations Environment Program Lebanon Post-Conflict Environmental Assessment. http://postconflict.unep.ch/publications.php?prog=lebanon. Accessed 18 March 2020
University of Birmingham (n.d.) Isis and a new caliphate. https://www.birmingham.ac.uk/research/perspective/isis-perspective.aspx. Accessed 18 March 2020
Van Creveld M L (1991) The transformation of war. The Free Press, New York

Wilner A (2013) Fencing in warfare: threats, punishment, and intra-war deterrence in counterterrorism. Security Studies 22.4:740–722
Wilner A (2014) Contemporary deterrence theory and counterterrorism: a bridge too far. New York University Journal of International Law and Politics 47:439–462
Wilner A, Wenger A (2012) Linking the deterrence to terrorism promises and pitfalls. In: Wenger A, Wilner A (eds) Deterring terrorism: theory and practice. Stanford University Press, Redwood, CA, pp 3–17

Dr. Eitan Shamir is an Associate Professor in the Department of Political Science at Bar Ilan University and a Research Associate with the Begin-Sadat Center for Strategic Studies (BESA). Prior to his academic position, Shamir was in charge of the National Security Doctrine Department at the Ministry of Strategic Affairs, Office of the Prime Minister (Israel). He holds a Ph.D. from the Department of War Studies at King's College London.

Chapter 15
All Deterrence Is Local: The Utility and Application of Localised Deterrence in Counterinsurgency

Martijn Kitzen and Christina van Kuijck

Contents

Abstract The deterrence of non-state actors is a relatively understudied and not particularly well-understood aspect of deterrence studies. This chapter contributes to the emerging body of knowledge on this matter by coining the idea of localised deterrence. Based on a discussion of counterinsurgency theory it is argued that tailored measures can be effectively employed for deterring violent non-state actors by targeting their relations with the local populace. Subsequently, this chapter explores theoretical as well as practical aspects of localised deterrence in order to explain how this concept can be conceptualised and operationalised to effectively deter insurgents and their supporters amongst the local populace. Ultimately, this allows us to reflect upon the concept and set an agenda for embedding localised deterrence within the wider body of deterrence studies by identifying new avenues of research.

M. Kitzen (✉)
Netherlands Defence Academy, Breda, The Netherlands
e-mail: MWM.Kitzen@mindef.nl

C. van Kuijck
Netherlands Ministry of Defence, The Hague, The Netherlands
e-mail: cia.v.kuijck@mindef.nl

F. Osinga and T. Sweijs (eds.), *NL ARMS Netherlands Annual Review of Military Studies 2020*, NL ARMS, https://doi.org/10.1007/978-94-6265-419-8_15

Keywords (Localised) deterrence · non-state actors · local population · counterinsurgency

15.1 Introduction

Deterrence has always been a crucial element in the fight against irregular opponents.[1] Due to the nature of such adversaries this application not only required deterring the actual fighters and other members of irregular groups, but also their supporters among the local populace. In colonial warfare, for example, this led to the wide-spread use of exemplary force as a means for punishing locales in which irregular adversaries thrived, while also sending a message to the opponent as well as the wider population. Gradually, however, an awareness emerged that in the long run the brutalities in which this approach typically resulted outweighed the success on the short term as the government's authority was almost continuously challenged. Moreover, especially in case of liberal democracies, the shifting of ethical, judicial and political standards rendered the use of force against the local population no longer acceptable. While all of this altered the application of deterrence in irregular warfare, practices like starvation and forced migration could be observed well into the second half of the twentieth century. In today's Western interventions such methods have been completely replaced as the emphasis lies on the use of persuasive methods for winning the support of the local population. But, how is it then possible to deter irregular opponents such as violent non-state actors that interact with and hide among the local population?

Deterrence studies first emerged during the Cold War in which the concept was crucial for maintaining a strategic balance between the two rivalling superpowers. From this background, it is fully understandable that the field has traditionally focused on interstate competition at the strategic level. More recently, however, violent non-state actors have gained an increasingly important role in the international security environment. It is not surprising, therefore, that there is a growing interest in the utility of deterrence vis-à-vis such opponents. In this regard, Chap. 14 by Shamir and Chap. 19 by Jakobsen offer valuable and much-needed insights for forwarding the understanding of the concept's application outside its traditional context. Yet, overall deterring violent non-state actors remains a relatively understudied aspect of deterrence studies. Partially, this can be ascribed to the tactical nature of this specific form of deterrence. Contrary to the classical notion, which emphasizes strategic level efforts to change the behaviour of states in the international system, the utility of deterrence against non-state actors typically involves

[1] Kitzen 2016, pp. 107–174.

'the immediate behaviour of individual people or small groups' with potentially strategic implications.[2] Wilner, among others, has repeatedly pointed at the far-reaching ramifications of this different focus for deterring extremist violence.[3] In such cases punishment and denial—the mainstays of classical deterrence—do not suffice as it is also crucial to target what the opponent believes through delegitimisation. Consequently, the cost-benefit analysis underlying the application of deterrence should take the perception of the target audience into account. Influencing the opponent requires a thorough understanding of cultural values and circumstances. A profound insight into the local context, thus, is key for successfully deterring violent non-state actors. Or in other words, in such cases all deterrence is local.

This chapter seeks to contribute to the expanding body of knowledge on the deterrence of non-state actors by focusing more closely on what we label 'localised deterrence'; i.e. the tactical application of deterrence based on the specifics of the local situation. Thus far, research in this field has mainly focused on the fight against terrorist organisations.[4] We aim to broaden this scope by discussing the localised nature of this particular form of deterrence from the perspective of counterinsurgency. The Global War on Terror and the fight against the Islamic State, after all, have demonstrated that dealing with extremist groups might not only require the implementation of a counterterrorism strategy, but also the conduct of counterinsurgency in unstable countries. Moreover, as today's violent non-state actors have become increasingly capable of interacting with populations and challenging weak governments, fighting insurgencies will remain a relevant theme in future warfare. The renewed competition for global influence among big powers, in this regard, is expected to augment this as 'grey zone tactics' might encompass the exploitation of non-state groups as proxies in order to destabilize states.[5] Our focus on counterinsurgency, thus, not only serves to widen the scope of the field, but is also prompted by the reality of modern warfare. Yet, this choice might not be obvious to all as counterinsurgency is mostly associated with 'winning the hearts and minds', which seemingly does leave little space for deterrence. As we will explain below, however, counterinsurgency as a form of irregular warfare in the first place is a highly dynamic contest between adversaries that inherently—and inevitably—involves coercion and therefore also deterrence.[6]

While we here coin the term localised deterrence, this chapter does not intend to build a theory or provide a comprehensive overview of its application. Our contribution should be considered a first attempt to introduce the concept as a distinctive object within the field and to identify new avenues for advancing the state

[2]For the distinction between strategic and tactical deterrence, see Johnson et al. 2002, pp. 12–13.

[3]Wilner 2010a, b, 2011, 2013, 2015a, b; Wenger and Wilner 2012; Long and Wilner 2014. See also Buesa and Baumert 2018; Cherney and Murphy 2019; Elbahy 2019; Lieberman 2019.

[4]Breekveldt and Kitzen 2019, p. 13.

[5]Cohen et al. 2020, p. 7.

[6]Kitzen (forthcoming).

of knowledge in the area of deterring non-state actors. To do so, we will first discuss the utility of localised deterrence in counterinsurgency from a theoretical perspective. This allows us to subsequently expand on this basis to obtain a fundamental understanding of the concept and identify germane issues with regard to its practice as well as the adjoining intricacies and challenges. Ultimately, the combined theoretical and practical insights serve to reflect upon the concept and set an agenda for expanding the body of knowledge by introducing localised deterrence as a specific subject of deterrence studies.

15.2 Explaining the Local Turn

Why does localised deterrence matter in counterinsurgency? Answering this question first requires us to clarify how the concept fits in with counterinsurgency theory. Therefore, our exploration starts with a discussion of the logic underlying counterinsurgency which will allow us to understand how localised deterrence might be used for fighting insurgencies. This section thus explains the rationale of localised deterrence as a tool of counterinsurgency.

In counterinsurgency state and non-state actors vie for control over and support of the population. As such, obtaining legitimacy is a key objective for all parties involved in this violent struggle.[7] Legitimacy is essentially understood as the acceptance and justification of authority based on social constructs, and is influenced by local culture, norms, values and beliefs.[8] Hence the importance of gaining a local understanding, as, among others, reiterated in NATO's AJP-3.4.4. *Counterinsurgency* (2016), which states that 'an effective counter-insurgent force needs to have a(n) (often hard-earned) cultural understanding as well as a more general understanding of the societal, economic and political landscape of the affected country'. Or in other words, in counterinsurgency 'societal context is king'.[9] A profound insight into the local social landscape and culture is not only pivotal for obtaining legitimacy, but also for denying support to the adversary, to influence relevant audiences on the basis of their motivations and drivers, and to obtain intelligence about the insurgents and their activities.[10] Ultimately this boils down to the fact that in counterinsurgency, a thorough understanding is imperative in order to obtain control over the target society while simultaneously preventing the opponent from doing so. Kilcullen, in this regard, has conceptualised this struggle as 'competitive control' which typically is won by the actor that manages

[7]Clayton and Thomson 2014, p. 922; Kitzen 2017; Brathwaite and Konaev 2019, p. 5. See also AJP-3.4.4, no. 203.

[8]Suchman 1995, p. 574; Hurd 1999; Reus-Smit 2007; Toros 2008; Andersen and Taylor 2008, p. 513; Beetham 2012, p. 123; Lamb 2014, p. 17; Gawthorpe 2017, pp. 841–2.

[9]Kitzen 2016, p. 544. See also Payne 2013; Schutte 2015.

[10]Jardine and Palamar 2013, p. 591; Barfield 2014; Johnson and Zellen 2014, p. 7; Patterson 2016, pp. 41, 56; Warren 2016, p. 55.

to impose a predictable, normative, ordered system 'that tells them [the people] exactly what they need to do, and not to do, in order to be safe'.[11]

Thus, both insurgents and counterinsurgents, compete to establish, enhance and maintain control over the population, denominated contested control.[12] Control, in this context, is defined as the capability of one societal agent to influence the circumstances of action of others.[13] Insurgents use various violent methods to obtain such control, including terrorism, which is characterised by the threat or use of violence to obtain publicity and spread a message of fear.[14] While terrorism is a tactic that can be employed by insurgents, insurgencies typically rely more heavily on political subversion and guerrilla warfare to exploit and address political grievances for achieving local change. Whereas terrorists do not necessarily need popular support, insurgents require the support (or at least acquiescence) of the population to win the struggle for control. Consequently, insurgencies employ hybrid strategies that not only target the state and its incumbents, but also seek to influence the relevant populace by either reaching out to the people or by imposing fear through the use of systematic terrorist attacks.[15] It is important to reiterate here that work in the field of deterring non-state actors has typically focused on terrorism and extremist organisations who seek to influence their target audiences through sustained (symbolic) violence. Whereas the labels for different types of violent non-state actors are often used interchangeably—especially by politicians, insurgencies are more complicated due to their hybrid character and their intricate interactions with the local population. Contrary to terrorists, insurgents might prefer political subversion and only employ terrorist tactics if necessary. Consequently, this chapter's adoption of the counterinsurgency perspective also serves to widen the scope of deterrence theory with regard to its application against violent non-state actors.

Counterinsurgents, on their turn, seek to obtain control through either collaboration with the population or by establishing dominance through the use or threat of force. The Western model of population-centric counterinsurgency focuses on the former and is often characterized as the 'hearts-and-minds' approach. Its emphasis lies on gaining popular support by enhancing state legitimacy through the use and creation of persuasive programmes and incentives as well as the provision of

[11]Kilcullen 2013, p. 126; Kilcullen 2016, pp. 153–154.

[12]Black 2016, pp. 11, 111, 189; Kilcullen 2013, p. 133.

[13]Giddens 1986, p. 283; Wong 2009, p. 3; Lukes 2005, pp. 21–22, 74; Kitzen 2016, p. 35.

[14]Lutz and Lutz 2010, pp. 351–352; O'Gorman 2011; Kiras 2012, pp. 234–237; Kim and Blank 2013, pp. 918–920; Kiras 2013, pp. 175–176; Bourne 2014, pp. 225, 246–247; Metz 2012a, p. 38; Mabon 2015, p. 7; Mazarr 2015, p. 62; Musgrave 2015; Bunker 2016, p. 7.

[15]For the broad discussion on the difference between insurgencies and terrorism see Schmid 2011. See also Wilner 2010b; Gross Stein 2012, p. 48; Metz 2012b; Romano 2012, pp. 246–247; Kim and Blank 2013, pp. 918–920; Moghadam et al. 2014; Unal 2016; Johnston 2018.

security.[16] The second approach, also known as the authoritarian model, seeks to establish unquestioned dominance by coercing both the enemy and the population.[17] In reality the divide between these two models is more nuanced, since they both use a mix of coercive and persuasive strategies—though the West typically focusses on persuasion, and authoritarian regimes more on coercion.[18] Additionally, the exact approach is not only influenced by regime type, but also by other factors like, for instance military culture.[19] While both models use different methods and means, they share the goal of enhancing and spreading state control.[20]

On the other hand, the authoritarian approach is problematic from a Western perspective due to its reliance upon force. The Western model itself overemphasises persuasive hearts-and-minds methods, which might be insufficient for establishing control. This is supported by the historical track record of Western counterinsurgency which proves that success is notoriously hard to achieve, as has yet again been illustrated in Iraq and Afghanistan. Moreover, today's conflicts have become even more complicated as they typically involve several types of actors with different motivations and interests. Consequently, depending on the local situation, coercion—compellence, and/or deterrence—might prove to be more effective.[21]

This inability to incorporate a broader range of methods for increasing the effectiveness of the counterinsurgency approach at the grass roots level is further enhanced by the fact that strategic decision-making almost exclusively takes place from a top-down perspective.[22] Contrastingly to counterinsurgency's localised nature, the crucial bottom-up view needed for understanding the way the local context informs people's choices, or 'strategies of survival', in a situation of violent contention is lacking.[23] This further hampers the ability to determine which tool(s) on the continuum ranging from persuasion to force (which will be dealt with below) should be employed for attaining the desired effect of enhanced control over the populace.[24] Indeed, instead of taking a top-down, outsider or *etic* perspective, effective counterinsurgency first and foremost requires a profound insight into the

[16]Katagiri 2011, pp. 170–171; Kilcullen 2013, p. 141; Kitzen 2016, pp. 34–35; Hirose et al. 2017, pp. 48–49.

[17]Kilcullen 2006; Kalyvas 2008, p. 111; Kilcullen 2013, pp. 134–141.

[18]See for example DeVore 2013; Jardine and Palamar 2013; Zhukov 2012; Larsdotter 2014; Byman 2016; Kitzen 2016, p. 35; Ucko 2016; Gawthorpe 2017.

[19]Kitzen 2012b.

[20]Byman 2016, p. 63; Ucko 2016, pp. 30–31; Asal et al. 2019, p. 1714.

[21]See for example Katagiri 2011; Kitzen 2012a; Bebber 2014, p. 206; Metz 2017; Schram 2019.

[22]Mackay et al. 2011, p. 98; Harkness and Hunzeker 2015; Gawthorpe 2017; Wong and Guggenheim 2018; Breekveldt and Kitzen (forthcoming).

[23]Migdal 1988, p. 27.

[24]Castro and Coleman 2014, p. 635; Liu and Opotow 2014, pp. 683–4; Jones 2017, p. 9; De Tray 2018, p. 37.

perception of the local population; the so-called *emic* perspective.[25] The resulting understanding serves as an underpinning for deciding upon the most effective course of action at the grass roots level. This might include deterring people from taking an active or supportive role in the insurgency as well as other measures to deter non-compliance with the government. But how does exactly such deterrence materialise?

15.3 Localised Deterrence

The local character of counterinsurgency implies that whenever deterrence is applied, this should be tailored to the specifics of the locale in which the struggle for control takes place. Hence, we have labelled this highly-specialized form localised deterrence as it can be applied against violent non-state actors that interact—either through force or persuasion—with a particular society. But how does this approach work? What exactly should be deterred and who should be deterred for that sake? Why do these actors exactly behave in an unintended way? And which methods can be employed for obtaining the desired change in behaviour? In order to conceptualise localised deterrence as a distinctive topic within deterrence studies it is pivotal that we answer these questions from a theoretical perspective as well as discuss salient facets of its operational application.

As mentioned afore, adopting an emic perspective is instrumental in understanding the local context through the eyes of the target audience. Decision-making on the basis of this information allows for customizing the cost-benefit analysis underlying the application of deterrence and thereby overcoming traditional coercion theory's universal bias which assumes that all actors will act in the same way, be it individuals or nations.[26] Equally important, a thorough emic understanding also serves to design effective measures of deterrence. In this regard, deterring an opponent or sympathiser among the population is typically achieved through a range of methods that are part of the broader coercive framework and which can be depicted in what we call the influence continuum (Fig. 15.1). As mentioned afore this continuum has force on one extreme and persuasion on the other, and typically all parties in a conflict seek to effectively influence other relevant actors through (a mix of) coercive and/or persuasive methods.[27] Whereas the former focuses on altering behaviour by depriving freedom or autonomy through (the threat of) force or other measures, the latter, for this same purpose, exploits an actor's perception of

[25]See for example Lett 1990, p. 130; Morris et al. 1999; Lune and Berg 2017, p. 108; Rossman and Rallis 2017, pp. 101–106; Bergman and Lindgren 2018; Treadwell 2018, pp. 294–5.

[26]Gross Stein 2012, pp. 53–4; Argomaniz and Vidal 2015, p. 176; Nix 2015, p. 4; Pampinella 2015, p. 519; Brathwaite and Konaev 2019, p. 11; Klinger 2019, p. 22.

[27]Kitzen 2016, pp. 93–101; Van Kuijck 2017; Perloff 2010, pp. 17–19; Ledgerwood et al. 2014, p. 533. See also Filippidou 2020a, b.

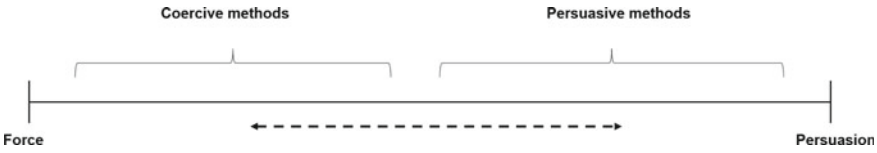

Fig. 15.1 The influence continuum (Fig. 15.1 is based upon Kitzen 2016, p. 101.)

free choice through intentional messaging.[28] As the term continuum implies, effectively influencing an actor might require to shift between coercive and persuasive methods or to employ a mix of measures in order to attain the desired effect.

Before deciding upon a method, however, effective localised deterrence first presupposes a clear purpose of what to achieve. When seeking to influence an opponent or social group, it is pivotal to determine which behaviour needs to be deterred. After all, this determines who exactly should be targeted and what specific method(s) should be employed to achieve the intended behavioural change. All of this should be based on a thorough situational awareness that results from an emic understanding of the local conflict dynamics. Such an operational approach to deterrence is described by, among others, Mackay, Rowland, Tatham and Van Kuijck who all recognise that exerting influence must be tailored to the local context.[29] For that purpose, it is pivotal to adopt a multidisciplinary method that allows for identifying triggers and circumstances of behaviour, as well as the different relevant target audiences. Of course, this serves the aim of effectively changing undesired behaviour and attaining the deterrer's goals. In order to obtain a more profound understanding of an operational approach of localised deterrence, we will now deal with its different facets, starting with the rationale of targeting specific behaviour.

15.4 What to Deter?

As aforementioned, effective deterrence requires an actor to determine which non-desired behaviour it wants to stop or which desired behaviour it wants to maintain. Often, however, goals remain vague and are not specified into relevant behaviours. In counterinsurgency, for instance, the main aim is to establish control over the population. This, typically, is translated in sub-goals like securing the people, isolating the insurgents, neutralizing the insurgent's subversive effort (while simultaneously enhancing the government's authority) and armed organization, as

[28]Powers 2007; Perloff 2010, pp. 15–19; Miller 2016.

[29]Mackay et al. 2011, 2012; Tatham 2015b; Van Kuijck 2017. The most evolved approach, in this regard is Actor and Audience Analysis (AAA, previously termed Target Audience Analysis or TAA).

well as creating unity of effort among all friendly actors involved in the campaign.[30] Although all of these objectives are relevant, they should be further specified into relevant behaviours that can be targeted. But why is it so important to focus on such specific behaviours?

Whereas traditionally the hearts-and-minds approach emphasizes attitude —'minds'—, this is a particular poor focal point for changing behaviour in circumstances of violent contention. Whilst different attitudes are a factor of consideration, they are only predictive for behaviour under specific conditions that mostly are absent in a conflict zone or do not apply to relevant behaviour.[31] Such specific behaviour itself, however, is a useful indicator that can be measured.[32] An increase in intelligence about the adversary's intents and actions received from the population, for instance, reveals much about a desired behaviour. A decrease in friendly interactions between counterinsurgents and local population, on the other hand, gives a clear indication of the rise of an undesired behaviour. Specific behaviour, therefore, offers a measurable and palpable focal point on which to act.

In the context of deterrence, the main goal would be to identify and forestall non-desired behaviour. This, consequently, should be operationalized as a SMART objective, i.e. being specific, measurable, achievable, relevant, and time-bound.[33] In a struggle for control over the population, it is crucial to determine which different behaviours from both insurgents as well as the local populace should be deterred. Whereas counterinsurgency has traditionally focused on attitudinal approaches such as bringing about a shift from impartiality towards support for the government, this has remained very much an intangible and unmeasurable objective. Focusing on behaviour overcomes this problem by first seeking to understand why the population matters. As people, among others, provide food, funding, supplies, resources, sanctuary, information and recruits to the party they support, various relevant behaviours can be distinguished.[34] Examples of non-desired behaviour include collaborating with the insurgents by taking up arms, placing IEDs (Improvised Explosive Devices), delivering food, money, or other specific resources, and withholding crucial information from the counterinsurgents. Similarly, insurgent behaviours such as murdering, maiming or raping civilians, spreading propaganda and night-letters, kidnapping of important key figures, armed robbery, theft, and

[30]See AJP-3.4.4. 2016, nr. 0404.

[31]Ajzen and Timko 1986; Olson and Zanna 1993; Courneya 1995; Glasman and Albarracín 2006. For an overview of why attitudes are poor predictors of behaviour, see Mackay et al. 2011; Payne 2013; Khalil 2014; Tatham and Le Page 2014, 2015a, b; Tatham and Giles 2015.

[32]Mackay et al. 2011, pp. 95–98, 169–170; Tatham and Le Page 2014, pp. 12–13; Paul et al. 2015a, p. 74; Petit 2019, p. 3.

[33]Paul et al. 2015a, pp. 73–78; Paul et al. 2015b, pp. 23–27.

[34]Patterson 2016, pp. 41, 49; Hirose et al. 2017, pp. 49–50; Hultquist 2017, pp. 510–511; Pechenkina and Bennett 2017; Rueda 2017, pp. 1627–8; Luttikhuis 2018; Asal et al. 2019, p. 1714; Brathwaite and Konaev 2019; Pechenkina et al. 2019, p. 546; Silverman 2019, pp 1461–2.

destruction of property can be targeted.[35] For instance, the Taliban still relies on opium, hashish trafficking, and levying taxes for their funding.[36] This would entail different behaviours under the concept of "Taliban Funding", such as poppy cultivation, the transportation of opium, and the use of smuggling routes. Looking at poppy cultivation, one needs to understand which different behaviours form this specific non-desired behaviour, which can include exchanging money for protection of the crops, buying relevant materials for growing poppy, and planting the seeds. Campaigns were conducted between 2006 and 2013 (with exaggerated reports of crop destruction and allegations of corruption) to deter the population from growing poppy and the funding of the Taliban, but the opposite happened. Instead of understanding that poor households prefer low-risk activities in the high-risk environment of Afghanistan and addressing this issue by taking into account the various behaviours, the campaign resulted in the rise of antipathic behaviour towards the government.[37]

Wilner has reiterated the importance of identifying such measurable factors like behaviour for deterring violent non-state actors.[38] Moreover, he has pointed out that with regard to the use of force, measuring the amount of violence is insufficient. Instead, assessing the type, nature, time-period and changes of violence will offer a better understanding of the behaviour involving the use of force and the way to address it. Thus, effective deterrence first and foremost requires identifying the target behaviour, which subsequently allows for identifying the relevant audience.

15.5 Whom to Deter?

Elsewhere in this volume Jakobsen states that an increasing number of actors can be potentially deterred in modern conflicts. In counterinsurgency, a myriad of actors is present. Typically, this is perceived in terms of a distinction between friendly, neutral, and hostile audiences.[39] Furthermore, active and passive supporters of both sides play a role in the violent struggle, and different categories of membership of insurgencies can be distinguished (leaders, armed elements, cadres, auxiliaries, underground, and mass base). Effective deterrence, however, requires a focus on the group(s) most relevant to the defined undesired behaviour. Hence, identification and

[35]See e.g. Johnson 2007; Dietz 2011; Clarke 2015; Glenn 2015, pp. 148–9; Patterson 2016, p. 56; Cancian 2017. See also AJP-3.4.4, nos. 0221-2, 0226, 0252-0258.

[36]See for example Norwegian Ministry of Foreign Affairs and Ministry of Defence 2016, p. 126; Financial Transactions and Reports Analysis Centre of Canada 2018.

[37]Mansfield 2017; Minoia and Pain 2017; Secure Livelihoods Research Consortium 2017.

[38]Wilner 2010b, pp. 323–324.

[39]AJP-3.4.4 2016, nos. 0219, 0229. Friendly, Hostile and Neutral audiences are mentioned throughout the entire doctrine. Other examples are sources of external support, e.g. influential individuals and criminal organisations (no. 0227) and 'other actors', such as neighbouring countries (nos. 0330-0337).

segmentation of involved actors is pivotal and should be as specifically as possible.[40] Again, it should be stressed that this depends on the target behaviour. For example, if a state seeks to deter foreign fighters from joining insurgencies, it not only needs to determine who travels to the conflict zone, but it also should identify the relevant intermediaries. The more specific the behaviour is, the more accurate the relevant target audience can be identified in order to design and implement an effective intervention strategy.

Depending on the local context relevant target audiences can be segmented in categories such as gender, country of origin, age, occupation, and socio-cultural or ethnical background. In case of the aforementioned example the target audience, for instance, consists of male and female foreign fighters aged 18–25 from Europe that travel to another country to join an insurgency, and smugglers instrumental in providing travel tickets and false passports.[41] Another illustration is provided by the identification of vulnerable groups that might be potentially tempted to actively support an insurgency with the state they live in. Boko Haram's target audience in Nigeria e.g. can be divided into, among others, illiterate minors with difficult upbringings, and unemployed young males.[42] A second real-life example of the diversity of the relevant audience is provided by of Al-Shabaab, which receives funds from different sources and groups, either voluntary or involuntary. This, among others, is illustrated by the extremist group's tactic of trading and taxing of charcoal. When seeking to deter Al-Shabaab's funding of insurgent groups, this requires not only influencing behaviour of its members, but also of truck drivers and smugglers who transport charcoal from different locations, as well as the manufacturers and labourers who produce that charcoal.[43] Identifying the relevant audiences, however, can even become more complicated in case of violent non-state actors consisting of an intricate web of interconnected networks as is the case with Al-Qaeda in the Islamic Maghreb (AQIM), which receives funds through various sources. One such source concerns a minor criminal activity involving sales of luxury vehicles through family networks and individuals in Guinea-Bissau and Mauritania. In this case, relevant audiences would include sales persons and companies of luxury vehicles, the transporters of the luxury vehicles, family members that provided transfer services in order to trace the transactions, and the high-end buyers that can afford and actually buy these luxury vehicles.[44]

Since it is often impossible to target all identified audiences, it is necessary to make sense of the different categories and prioritize them for the purpose of deterring non-desired behaviour. Therefore, relevant groups should be categorized

[40]This is an approach that comes from communication and marketing sciences, though it is also used for ethnographic purposes. See for example Kim 2014, p. 89; Cwalina et al. 2015, p. 70, 106; Drumwright and Murphy 2015, pp. 180, 186; Maison 2019, pp. 60–62, 132.

[41]See for example the Soufan Group 2015; Benmelech and Klor 2016; OSCE 2018; Cook and Vale 2019; Marone and Vidino 2019; Vale 2019.

[42]Onuoha 2014; Ewi and Salifu 2017; Adelaja et al. 2018.

[43]Fanusie and Entz 2017b; UNSC 2018; Felter et al. 2020.

[44]Ortmann 2017; Fanusie and Entz 2017a; FAFT-GIABA-GABAC 2016, pp. 23–24.

in different spheres such as the actual target audience, those reacting positively to the application of deterrence to the main audience, those reacting negatively, and those ambivalent.[45] Using the example of AQIM, the target audience consist of persons and groups that are not members of AQIM and knowingly engage in the luxury vehicles sales process to provide money to AQIM. The audience that reacts positively to the deterring 'message' is made up of persons and groups (family members, local leaders, and high-end buyers) unknowingly supporting AQIM through the luxury vehicles sales process, and who can make a difference in the behaviour of the actual target audience. AQIM members as well as those involved in transfer of funds form the audience that can react negatively to the measures applied to the main audience. The audience that is ambivalent and might even be best left alone consists of transporters of the luxury vehicles. It should be mentioned here, that this categorization remains hypothetical as any accurate classification of different audiences should be based on research from a local perspective (which is outside the scope of this contribution). This, however, does not affect the pivotal point that a thorough and as specific as possible identification of the relevant audiences is instrumental in considering how the target behaviour can be deterred.

15.6 Driving Factors for (Un)desired Behaviour

To determine how to change undesired behaviour, it is a prerequisite to learn the triggers and factor underlying that specific behaviour. As touched upon in the previous paragraph, once relevant behaviours and audiences are identified, a more profound analysis should be conducted at the local level. This encompasses in-country vetting by use of the local language(s) in order to consider as many salient issues as possible. As repeatedly echoed throughout this chapter, it is crucial to know who exactly the audiences are and how these people understand the world from their lens or perspective; behaviour can only be changed by adopting such an emic perspective. Even a seemingly relatively simple or straightforward matter like the term 'evil' or 'wrong', might be perceived completely different from the local perspective.[46]

This insight has been observed time and again in the counterinsurgency campaigns of the last two decades, but it seems very hard to learn this lesson and incorporate an emic perspective in decision-making at even the tactical level. A striking example is provided by an attempt to reduce the number of IED-strikes and American deaths through an information operations (IO)-campaign in Afghanistan.[47] Portraying US soldiers as friendly people devoted to their family

[45]See for example Mackay et al. 2011, 2012; Tatham 2015b.

[46]For an overview of the concept of 'wrong' or 'evil' from different points of view, see Martínez Jiménez 2015.

[47]Dietz 2011. See also Breekveldt and Kitzen (forthcoming).

succeeded in positively changing the local attitude towards them. Yet a change of undesired behaviour—the placing of IEDs—did not occur. An evaluation brought to light that there were two reasons for this failure. First, those placing the IEDs turned out to be extremist, whose attitude and behaviour could not be changed in this way. More important was the second finding that the IO's campaign use of images of soldiers and their families also conveyed the message that life in the US was good. Unintendedly, this prompted the people that were producing and transporting IEDs to step up their effort. Since financial reasons were a primary motivation, it turned out to be that the portrayed richness of live in the US made them want to make more money in order to immigrate to that country. Thus, contrary to the desired effect, the locals involved boosted production and transportation which resulted in an increase of IED strikes. The Americans, from their perspective, did everything right in their attempt to influence the population, the audience's perception, and specifically those involved in producing and transporting IEDs. Yet, due to a poor insight into the local perspective. it did not lead to the expected desired outcome, but far more to the opposite.

Employing effective methods of localised deterrence, thus, requires an equally localised understanding of the undesired behaviour and target audience. For that purpose, it is pivotal to adopt a multidisciplinary approach that combines insights from various academic fields (e.g. communication, anthropology, social psychology, and neuroscience) for conducting bottom-up research in order to answer the crucial questions of what, who, why, and how.[48] After all, the actual application of localised deterrence first requires a more detailed knowledge of *what* exactly is the relevant behaviour and who makes up the target audience, *why* people engage in the relevant (non-)desired behaviours, and *how* this can be changed in an holistic manner that fits the local context. These different aspects, thus, not only enhance respectively descriptive and prognostic information about the audience and targeted behaviour, but also provide an insight into which transformative and tangible method is most effective for attaining the desired behavioural change.

15.7 How to Deter?

Although that it is impossible to deal in this chapter with all different methods that can be used in localised deterrence, the influence continuum (Fig. 15.1) clearly demonstrates that methods may vary from the use of force to pure (verbal) persuasion. Moreover, depending on the local situation and more specifically the nature of the involved actors, shifting between different coercive and persuasive

[48]Mackay et al. 2011; Tatham 2015b; van Kuijck 2017 all identify the 'what, why, and how' questions. We have dissected the 'what' question as it basically comprises two fundamental elements of 'what' and 'who'.

methods or adopting a mix might be required.[49] While ultimately, a profound understanding of the local social landscape and conflict dynamics should inform the preferred method(s), this conceptual exploration benefits from distinguishing between the three main categories of audiences that shape the human terrain in which the struggle for control is fought. In this regard it is important to notice that local people's strategies of survival typically boil down to weighing sanctions and incentives in order to limit the damage suffered from the conflict and, when possible, to strengthen their position.[50] Furthermore, counterinsurgency is mostly conducted in developing countries with a so-called web-like society and hampered by a scarcity of resources. Due to this combination, effective engagement of different groups focuses at leaders and the way they seek to address the people's strategies of survival. Although, yet again, this heavily depends on the local situation, we have opted here to follow this logic since it is impossible to discuss all methods of localised deterrence. Moreover, it allows us to provide a structural oversight of methods, and to discuss the practical application of these methods.

The first category consists of those friendly to the counterinsurgency. These people to a greater or lesser extent collaborate with the government. The undesired behaviour, therefore, is that they diminish or stop their collaboration, or even switch sides and turn towards the insurgency. According to the logic of Western, population-centric counterinsurgency all of this should not be deterred by use of force, but rather by persuasive methods that reward cooperation. If necessary, this might be accompanied by the limited use of non-violent, so-called soft coercion such as the (threat of) withdrawal of military, political or economic support.[51] Deterrence, thus, is provided by the denial or loss of benefits. This can be addressed through, for instance, a strategy of co-option with local power-holders.[52] The counterinsurgency campaigns in Iraq and Afghanistan have demonstrated that such a strategy might be particularly effective in gaining increased support for the government, as epitomized by the Sunni awakening movement in Iraq. Yet, while it sometimes took several years before counterinsurgents gained sufficient understanding in order to determine who should be engaged and what methods were most effective, the most challenging aspect was to remain in control of co-opted local power-holders. As such actors typically act to maximise their self-interest, the threat that these allies either diminished their collaboration or even switched side was always very real. Localised deterrence, therefore, was instrumental in implementing an effective system of checks and balances that kept the counterinsurgency in control and mitigated undesired behaviour.

In the second category are those neutral to the conflict, the so-called fence-sitters. In this case, the undesired behaviour not only concerns (the start of)

[49]Kitzen 2016, pp. 93–101; van Kuijck 2017; Perloff 2010, pp. 17–19; Ledgerwood et al. 2014, p. 533. See also Filippidou 2020a, b.

[50]Kitzen 2016, pp. 58, 67–68; Leites and Wolf Jr. 1970, p. 126.

[51]Kitzen 2016, pp. 157–165.

[52]Kitzen 2012a, 2016.

collaboration with the insurgency, but also all other actions with a spoiling influence. Again, the Western emphasis on 'hearts and minds' prescribes that such an audience is preferably engaged through persuasive methods backed up by soft coercion if necessary. The difference with the previous category is that in the case of neutrals soft coercion is more accepted as a method to enforce compliance. One particular powerful illustration of the effectiveness of localised deterrence in such a case concerns the targeting of an actor's power basis through manipulation of his supportive network and the empowering of rivals. The thorough vetting of the local human landscape will help to identify local political players as well as the pattern and structure of political authority in the target society. Based on this advanced understanding potential spoilers or opponents can be singled out and their power base might be attacked by (the threat of) reaching out to rivals willing to cooperate.[53] This, for instance, has been practiced repeatedly in Afghanistan to curtail the power of warlords who threatened the international effort and whose spoiling behaviour could be effectively deterred in this way.

The third and last category is made up of those hostiles towards the counterinsurgency, i.e. sympathisers among the population and active members of the insurgency. Here the undesired behaviour that should be deterred is a continuation of collaboration with the insurgents or further participation in the insurgency. For the sake of this, the use of different coercive methods, varying from the use of force to soft coercion, is widely accepted—although in Western counterinsurgency compellence might also include persuasive methods. For the application of localised deterrence, it is useful to distinguish between irreconcilable extremists and more moderate reconcilable individuals. The latter can be engaged either through soft methods or by (the threat of) force in order to make them comply or even to convince them to switch sides. Yet, as an example from Afghanistan demonstrates, this is difficult to accomplish as military organizations are used to deal with adversaries by use of force.[54] In this particular case a Taliban leader's local power-base was effectively eroded which led him to offer a switch towards the government side. Since this individual was already listed for either being captured or killed, it proved impossible to accommodate his proposal. Thus, a huge chance to turn the local situation was missed due to a lack of flexibility from the side of the counterinsurgents. This also points to the prominent place of targeting in Western military operations.[55] While this might not always be the best option for deterring behaviour of the more moderate individuals, it is highly effective for use against the more extremist, irreconcilable senior and mid-level leaders. In most cases this specific method does not so much function to deter the involved individual, but far more aims to enforce compliance from the wider (relevant segments of) insurgency

[53]See e.g. Ray 2015, p. 143; Byman 2016, p. 72; Kitzen 2016, pp. 96–7.

[54]Kitzen 2012a, 2016.

[55]Kitzen (forthcoming).

and its supporters. A so-called strategy of decapitation, indeed, can have a profound impact on the organisation as a whole.[56]

These insights into the application of localised deterrence for influencing behaviour in different groups allow us to conclude this section by drawing up a taxonomy of localised deterrence in counterinsurgency. Conceptually, three different approaches can be discerned. Each approach is tailored to a specific audience and relevant behaviour, and therefore relies on a specific mix of methods. Yet, it should be emphasized again that implementing the concept first and foremost remains a local matter. Only when the salient questions of what, who, why, and how are answered on the basis of a profound understanding of the local, emic perspective, localised deterrence can be effectively implemented in the practice of counterinsurgency warfare.

15.8 Conclusion

This chapter has explained why understanding the local context is essential for effectively deterring undesired behaviour. Such localised deterrence is crucial since not all actors make the same cost-benefit analysis and the population at the grass roots level, as a consequence of the increasing role of violent non-state actors, has become far more important in modern conflicts. The re-emergence of global power competition is expected to further contribute to this trend as non-state groups will be increasingly exploited as proxies in grey zone warfare. Counterinsurgency, in this regard, provides some answers for fighting violent non-state actors that intricately interact with the local population. As the struggle for control over the population essentially is a local fight, counterinsurgency prescribes understanding the local culture and perspective. Yet, Western counterinsurgency does not provide a sufficient answer since its focus on attitudes and persuasive methods does hamper the adoption of an effective mix of methods for deterring non-desired behaviour. Rather, deterrence and compellence are both sides of the same coin that can be achieved through a combination of coercive and persuasive tactics, depending on both the objective and the local context. Moreover, the top-down character of strategic and military decision-making often prevents developing and incorporating a true emic understanding of the local social landscape. Hence, we urge for a change in mind-set and approaches towards both counterinsurgency and deterrence.

Localised deterrence offers an approach for stopping non-desired behaviour or maintaining a (desired) status quo on the basis of a profound emic understanding of the local context and conflict dynamics. This not only allows for properly identifying a specific behaviour, but also for selecting the right target audience, the triggers and motives of relevant behaviour as well as the tactics that are most fitting in a certain environment. The concept, thus, has triggered the development of novel

[56]See, for instance, Johnston 2012; Price 2012.

approaches that operationalize localised deterrence by answering the pivotal questions of what, who, why, and how. Although first and foremost a local approach, our exploration of the practical application of the concept in counterinsurgency has allowed us to draw up a conceptual taxonomy. According to this categorisation three different types of audiences (friendly, neutral, enemy) with each a specific undesired behaviour and a unique mix of methods can be distinguished. Furthermore, it was also found that challenges in the practical application of localised deterrence not only concern the development of a local understanding and the subsequent design of an effective approach, but also involve the adoption of a flexible mind-set that allows for effectively shifting between various methods. Yet, this chapter has provided some examples in which localised deterrence was effectively incorporated in the struggle for control in recent counterinsurgency campaigns.

Newly available tools offer a far more structured and methodological strong approach towards the concept. Hence, we would like to conclude by suggesting to adopt localised deterrence as a distinct topic of deterrence studies and explore new avenues of research in order to contribute to the emerging body of knowledge on the deterrence of violent non-state actors. This is especially important as much of the empirical evidence has not yet been published. By setting a research agenda the field can optimally benefit from the data of recent cases in, among others, Iraq, Afghanistan, and the Sahel, which will become available over the next years. We, in this regard, would like to suggest to study the fundamental value of the concept outside the context of counterinsurgency, to further explore the way the questions of what, who, why, and how can be answered, and how the concept can be implemented most effectively. This will not only contribute to the further conceptualisation and theorization of localised deterrence, but also will shed a light on the wider practical utility of the concept against violent non-state actors who are increasingly exploiting their networked ties with local populaces throughout the world—either for their own purposes or as proxies in the global power competition. The strongest contribution to the field, in this regard, is expected to come from localised deterrence's departure from the one-fits-all approach as originally entrenched in classical coercion theory. Since all behaviours are influenced by the specific local context, culture, and perceptions of the audience, it is pivotal to further explore this new strand in deterrence theory.

References

Adelaja A O, Labo A, Penar E (2018) Public Opinion on the Root Causes of Terrorism and Objectives of Terrorists: A Boko Haram Case Study. Perspectives on Terrorism 12:35–49.

Ajzen I, Timko C (1986) Correspondence between health attitudes and behaviour. Basic and Applied Social Psychology 7:259–276

Andersen M L, Taylor H F (2008) Sociology. Understanding a Diverse Society. Belmont, Thomson Wadsworth

Argomaniz J, Vidal-Diez A (2015) Examining Deterrence and Backlash Effects in Counter-Terrorism: The Case of ETA. Terrorism and Political Violence, 27:160–181

Asal V, Phlips BJ, Rethemeyer RK, Simonelli C, Young JK (2019) Carrots, Sticks, and Insurgents Targeting of Civilians. Journal of Conflict Resolution 63:1710–1735

Barfield T J (2014) Weapons of the Not So Weak in Afghanistan: Pashtun Agrarian Structure and Tribal Organization. In: Johnson T H, Zellen B S (eds) Culture, Conflict, and Counterinsurgency Stanford University Press, Stanford CA, pp 95–119

Bebber R J (2014) Developing an IO Environmental Assessment in Kost Province, Afghanistan: Information Operations at Provincial Reconstruction Team Khost in 2008. In: Johnson T H, Zellen B S (eds) Culture, Conflict, and Counterinsurgency. Stanford University Press, Stanford CA, pp 196–214

Beetham D (2012) Political Legitimacy. In: Amenta E, Nash K, Scott A (eds) The Wiley-Blackwell Companion to Political Sociology. Blackwell Publishing, West Sussex, pp 120–129

Benmelech E, Klor E F (2016) What Explains the Flow of Foreign Fighters to ISIS? National Bureau of Economic Research, Cambridge MA

Bergman A, Lindgren M (2018) Navigating between an emic and an etic approach in ethnographic research. Crucial aspects and strategies when communicating critical results to participants. Ethnography and Education, 13:477–489

Black J (2016) Insurgency and Counterinsurgency. A Global History. Rowman & Littlefield, Lanham

Bourne M (2014) Understanding Security. Palgrave Macmillan, New York

Brathwaite K J H, Konaev M (2019) War in the city: Urban ethnic geography and combat effectiveness. Journal of Strategic Studies 1–36.

Breekveldt R, Kitzen M (2019) Coercion and Non-State Actors: Lessons from the Philippines. CTX (Combatting Terrorism Exchange) 9:13–28

Breekveldt R, Kitzen M (forthcoming) Control from the ground up. Embedding influence activities in the conduct of war. In: Johnson R, Kitzen M, Sweijs T (eds) The Conduct of War in the 21st Century. Routledge, Abingdon

Buesa M, Baumert T (2018) Hit the Core or Weaken the Periphery? Comparing Strategies to Break the Circle of Violence with an Embryonic Terrorist Group: The Case of Galician Resistance. Terrorism and Political Violence 30:475–502

Bunker R J (2016) Old and New Insurgency Forms. Strategic Studies Institute, Carlisle

Byman D (2016) 'Death Solves All Problems': The Authoritarian Model of Counterinsurgency. Journal of Strategic Studies 39:62–93

Cancian M F (2017) Tactics, Techniques, and Procedures of the Islamic State. Military Review, 3–4:52–61.

Castro M K, Coleman P T (2014) Multiculturalism and Conflict. In: Coleman P T, Deutsch M, Marcus EC (eds) The Handbook of Conflict Resolution. Theory and Practice. Jossey-Bass, San Francisco CA, pp 623–653

Cherney A, Murphy K (2019) Support for Terrorism: The Role of Beliefs in Jihad and Institutional Responses to Terrorism. Terrorism and Political Violence, 31:1049–1069

Clarke C P (2015) Countering PIRA Financing and Combating the Ability of Insurgents to Raise Funds through Crime in Northern Ireland during "the Troubles". In: Cline L E, Shemella P (eds) The Future of Counterinsurgency. Contemporary Debates in Internal Security Strategy. Praeger, Santa Barbara, pp 121–140

Clayton G, Thomson A (2014) The Enemy of My Enemy is My Friend … The Dynamics of Self-Defense Forces in Irregular War: The Case of the Sons of Iraq. Studies in Conflict & Terrorism, 37:920–935

Cohen R S, Chandler N, Efron S, Frederick B, Han E, Klein K, Morgan F E, Rhoades A L, Shatz H J, Shokh Y (2020) Peering into the Crystal Ball. Holistically Assessing the Future of Warfare. RAND, Santa Monica CA

Cook J, Vale G (2019) From Daesh to 'Diaspora' II: The Challenges Posed by Women and Minors After the Fall of the Caliphate. CTC Sentinel, 12:30–35

Courneya K S (1995) Understanding readiness for regular physical activity in older individuals: An application of the theory of planned behaviour. *Health Psychology, 14*:80–87
Cwalina W, Fakowski A, Newman B I (2015) Persuasion in the Political Context: Opportunities and Threats. In: Stewart DW (ed) The Handbook of Persuasion and Social Marketing. Volume 1: Historical and Social Foundations. Praeger, Santa Barbara, pp 61–128
De Tray D (2018) Why Counterinsurgency Fails. The US in Iraq and Afghanistan. Palgrave Macmillan, Cham
DeVore M R (2013) Institutions, Organizational Culture, and Counterinsurgency Operations: Why Do States Fight Similar Insurgencies Differently? Comparative Strategy 32:169–191
Dietz A S (2011) Countering the effects of IED systems in Afghanistan: an integral approach. Small Wars & Insurgencies, 22:385–401
Drumwright M E, Murphy P E (2015) Ethical Issues of Social Marketing and Persuasion. In: Stewart D W (ed) The Handbook of Persuasion and Social Marketing. Volume 1: Historical and Social Foundations. Praeger, Santa Barbara CA, pp 175–202
Elbahy R (2019) Deterring violent non-state actors: Dilemmas and implications. Journal of Humanities and Applied Social Sciences, 1:43–54
Ewi M, Salifu U (2017) Money Talks. A key reason youths join Boko Haram (Policy Brief 98). Institute for Security Studies, Pretoria
FAFT-GIABA-GABAC (2016) Terrorist Financing in West and Central Africa. Financial Action Task Force, Paris
Fanusie Y J, Entz A (2017a) Al-Qaeda in the Islamic Maghreb. Financial Assessment. Foundation for Defense of Democracies, Center on Sanctions & Illicit Finance, Washington DC
Fanusie Y J, Entz A (2017b) Al-Shabaab. Financial Assessment. Foundation for Defense of Democracies, Center on Sanctions & Illicit Finance, Washington DC
Felter C, Masters J, Sergie M A (2020) Al-Shabab. Council on Foreign Relations. https://www.cfr.org/backgrounder/al-shabab. Accessed 26 February 2020
Filippidou A (2020a) Deterrence: Concepts and Approaches for Current and Emerging Threats. In: Filippidou A (ed) Deterrence: Concepts and Approaches for Current and Emerging Threats. Springer, Cham, pp 1–18
Filippidou A (2020b) Deterring Violent Extremism and Terrorism. In: Filippidou A (ed) Deterrence: Concepts and Approaches for Current and Emerging Threats. Springer, Cham, pp 97–114
Financial Transactions and Reports Analysis Centre of Canada (2018) Terrorist Financing Assessment 2018. Financial Transactions and Reports Analysis Centre of Canada, Ontario
Gawthorpe A J (2017) All Counterinsurgency is Local: Counterinsurgency and Rebel Legitimacy. Small Wars & Insurgencies, 28:839–852
Giddens A (1986) The Constitution of Society. University of California Press, Berkeley/LA
Glasman L R, Albarracín D (2006) Forming attitudes that predict future behaviour: a meta-analysis of the attitude-behaviour relation. Psychological Bulletin, 132:778–822
Glenn R W (2015) Rethinking Western Approaches to Counterinsurgency. Lessons from post-colonial conflict. Routledge, Oxon
Gross Stein J (2012) Deterring Terrorism, Not Terrorists. In: Wenger A, Wilner A (eds) Deterring Terrorism: Theory and Practice. Stanford University Press, Stanford CA, pp 46–66
Harkness K A, Hunzeker M (2015) Military Maladaptation: Counterinsurgency and the Politics of Failure. Journal of Strategic Studies, 38:777–800
Hirose K, Imai K, Lyall J (2017) Can civilian attitudes predict insurgent violence? Ideology and insurgent tactical choice in civil war. Journal of Peace Research, 54:47–63
Hultquist P (2017) Is collective repression an effective counterinsurgency technique? Unpacking the cyclical relationship between repression and civil conflict. Conflict Management and Peace Science, 34:507–525
Hurd I (1999) Legitimacy and Authority in International Politics. International Organization, 53:379–408

Jardine E, Palamar S (2013) From Medusa Past Kantolo: Testing the Effectiveness of Canada's Enemy-Centric and Population-Centric Counterinsurgency Operational Strategies. Studies in Conflict & Terrorism, 36:588–608
Johnson D E, Mueller KP, Taft W H (2002) Across the Spectrum of Operations. The Utility of U.S. Military Forces in the Emerging Security Environment. RAND, Santa Monica CA
Johnson TA (2007) The Taliban Insurgency and an Analysis of Shabnamah (Night Letters). Small Wars and Insurgencies, 18:317–344
Johnson TH, Zellen B S (2014) Introduction. In: Johnson T H, Zellen B S (eds) Culture, Conflict, and Counterinsurgency. Stanford University Press, Stanford CA, pp 1–16
Johnston N (2018) Defining Terrorism and Insurgency: Beyond Morality. Small Wars Journal. https://smallwarsjournal.com/jrnl/art/defining-terrorism-and-insurgency-beyond-morality. Accessed 4 March 2020
Johnston PB (2012) Does Decapitation Work? Assessing the Effectiveness of Leadership Targeting in Counterinsurgency Campaigns. International Security 36:47–79
Jones S G (2017) Waging Insurgent Warfare. Lessons from the Vietcong to the Islamic State. Oxford University Press, New York
Kalyvas S N (2008) The logic of violence in civil war. Cambridge University Press, Cambridge
Katagiri N (2011) Winning hearts and minds to lose control: Exploring various consequences of popular support in counterinsurgency missions. Small Wars & Insurgencies, 22:170–195
Khalil J (2014) Radical Beliefs and Violent Actions are not Synonymous: How to Place the Key Disjuncture Between Attitudes and Behaviours at the Heart of Our Research into Political Violence. Studies in Conflict & Terrorism, 37198–211
Kilcullen D (2006) Three Pillars of Counterinsurgency [Paper Presentation]. U.S. Government Counterinsurgency Conference, Washington DC
Kilcullen D (2013) Out of the Mountains. The Coming Age of the Urban Guerrilla. Oxford University Press, Oxford
Kilcullen D (2016) Blood year. The unravelling of Western counterterrorism. Oxford University Press, New York
Kim K K (2014) Research on Transnational Advertising Agencies: Management, Structure, and Entry Strategies. In: Cheng H (ed) The Handbook of International Advertising Research. John Wiley & Sons
Kim Y, Blank S (2013) Insurgency and Counterinsurgency in Russia: Contending Paradigms and Current Perspectives. Studies in Conflict & Terrorism, 36:917–932
Kiras J D (2012) Irregular Warfare. In: Jordan D, Kiras J D, Lonsdale D J, Speller I, Tuck C, Walton C D (eds) Understanding Modern Warfare. Cambridge University Press, Cambridge, pp 224–290
Kiras J D (2013) Irregular Warfare: Terrorism and Insurgency. In: Baylis J, Wirtz J J, Gray C S (eds) Strategy in the Contemporary World. Oxford University Press, Oxford, pp 173–194
Kitzen M (2012a) Close Encounters of the Tribal Kind: The Implementation of Co-option as a Tool for De-escalation of Conflict – The Case of the Netherlands in Afghanistan's Uruzgan Province. Journal of Strategic Studies, 35:713–734
Kitzen M (2012b) Western Military Culture and Counterinsurgency: An Ambiguous Reality. Scientia Militaria: South African Journal of Military Studies, 40:1–24
Kitzen M (2016) The course of co-option: Co-option of local power-holders as a tool for obtaining control. University of Amsterdam, Amsterdam
Kitzen M (2017) 'Legitimacy is the Main Objective': Legitimation in Population-Centric Counterinsurgency. Small Wars & Insurgencies, 28:853–866
Kitzen M (forthcoming) Operations in Irregular Warfare. In: Sookermany A (ed) The Handbook of Military Sciences. Springer, Berlin
Klinger J M (2019) Social Science and National Security Policy. Deterrence, Coercion, and Modernization Theories. Springer, Cham
Lamb R D (2014) Rethinking Legitimacy and Illegitimacy. A New Approach in Assessing Support and Opposition across Disciplines (CSIS Report). Rowman & Littlefield, Lanham

Larsdotter K (2014) Regional Support for Afghan Insurgents: Challenges for Counterinsurgency Theory and Doctrine. Journal of Strategic Studies, 37:135–162
Ledgerwood A, Callahan S P, Chaiken S (2014) Changing Minds: Persuasion in Negotiation and Conflict Resolution. In: Coleman P T, Deutsch M, Marcus E C (eds) The Handbook of Conflict Resolution: Theory and Practice. Jossey-Bass, San Francisco, 533–557
Leites N, Wolf Jr C (1970). Rebellion and Authority: An Analytic Essay on Insurgent Conflicts. Markham Publishing Company, Chicago
Lett J (1990) Emics and etics: Notes on the epistemology of anthropology. In: Headland T N, Pike K L, Harris M (eds) Emics and etics: The insider/outsider debate. Sage, Newbury Park CA, pp 127–142
Liebman E (2019) Deterring Terrorism: A Model for Strategic Deterrence. Routledge, Oxon
Liu W, Opotow S (2014) Aggression and Violence. Causes and Correctives. In: Coleman P T, Deutsch M, Marcus E C (eds) The Handbook of Conflict Resolution. Theory and Practice. Jossey-Bass, San Francisco CA, pp 681–707
Long J M, Wilner A S (2014) Delegitimizing al-Qaida. Defeating an "Army Whose Men Love Death". International Security 39:126–164
Lukes S (2005) Power: a radical view. Palgrave Macmillan, Basingstoke
Lune H, Berg B L (2017) Qualitative Research Methods for the Social Sciences. Pearson, Essex
Luttikhuis B (2018) Generating distrust through intelligence work: Psychological terror and the Dutch security services in Indonesia, 1945–1949. War in History, 25:151–171
Lutz B, Lutz J (2010) Terrorism. In: Collins A (ed) Contemporary Security Studies. Oxford University Press, Oxford, pp 338–358
Mabon S (2015) Locating Terrorism Studies. In: Kennedy-Pipe C, Clubb G, Mabon S (eds) Terrorism and Political Violence. Sage, London, pp 5–17
Mackay A, Tatham S, Rowland L (2011) Behavioural Conflict. Why understanding people and their motivations will prove decisive in future conflict. Military Studies Press, Essex
Mackay A, Tatham S, Rowland L (2012) The Effectiveness of US Military Information Operations in Afghanistan 2001–2010: Why RAND missed the point (Central Asia Series 12/02a). Defence Academy of the United Kingdom, Shrivenham
Maison D (2019) Qualitative Marketing Research. Understanding Consumer Behaviour. Routledge, Oxon
Mansfield D (2017) Understanding Control and Influence: What Opium Poppy and Tax Reveal about the Writ of the Afghan State. Areu, Kabul
Marone F, Vidino L (2019) Destination Jihad: Italy's Foreign Fighters. International Centre for Counter-Terrorism, The Hague
Martínez Jiménez A (2015) The problem of evil (Bachelor Thesis: El Problema del Mal), University of Oviedo, Oviedo. https://www.researchgate.net/publication/339413359_El_problema_del_mal. Accessed 5 March 2020
Mazarr M J (2015) Mastering the Gray Zone: Understanding a Changing Era of Conflict. Strategic Studies Institute, Carlisle
Metz S (2012a) Rethinking insurgency. In: Rich P B, Duyvesteyn I (eds) The Routledge Handbook of Insurgency and Counterinsurgency. Routledge, Oxon, pp 32–44
Metz S (2012b) Psychology of Participation in Insurgency. Small Wars Journal. https://smallwarsjournal.com/jrnl/art/psychology-of-participation-in-insurgency. Accessed 4 March 2020
Metz S (2017) Abandoning Counterinsurgency: Toward a More Efficient Antiterrorism Strategy. Journal of Strategic Security, 10:64–77
Migdal J S (1988) Strong Societies and Weak States. State-Society Relations and State Capabilities in the Third World. Princeton University Press, Princeton
Miller V N (2016) When Push Comes to Shove: A Comparative Concept Analysis of Motivation and Coercion in Nursing Education. Nursing Forum, 51:164–172
Minoia G, Pain A (2017) Understanding Rural markets in Afghanistan (Working Paper 58). Secure Livelihoods Research Consortium, London

Moghadam A, Berger R, Beliakova P (2014) Say Terrorist, Think Insurgent: Labeling and Analyzing Contemporary Terrorist Actors. Perspectives on Terrorism 8.5. http://www.terrorismanalysts.com/pt/index.php/pot/article/view/374/html. Accessed 4 March 2020

Morris M W, Leung K, Ames D, Lickel B (1999) Views from Inside and Outside: Integrating Emic and Etic Insights about Culture and Justice Judgment. Academy of Management Review, 24:781–796

Musgrave N (2015) The Root Causes of Terrorism. In: Kennedy-Pipe C, Clubb G, Mabon S (eds) Terrorism and Political Violence. Sage Publications, London, pp 103–118

Nix J (2015) Do the Police Believe that Legitimacy Promotes Cooperation from the Public? Crime & Delinquency 1–25

Norwegian Ministry of Foreign Affairs and Ministry of Defence (2016) A Good Ally: Norway in Afghanistan 2001–2014 (Official Norwegian Reports)

O'Gorman R (2011) The evolutionary logic of terrorism: understanding why terrorism is an inevitable human strategy in conflict. In: Silke A (ed) The Psychology of Counter-Terrorism. Routledge, New York, pp 62–75

Olson J M, Zanna M P (1993) Attitudes and Attitude Change. Annual Review of Psychology, 44:117–154

Onuoha F C (2014) Why do Youth Join Boko Haram? United States Institute of Peace, Washington DC

Ortmann G (2017) Deconstructing the Business of Terrorism (Master's Thesis). Centre Européen de Recherches Internationales et Stratégiques, Brussels

OSCE (2018) Guidelines for Addressing the Threats and Challenges of "Foreign Terrorist Fighters" within a Human Rights Framework. OSCE Office for Democratic Institutions and Human Rights, Warsaw

Pampinella S (2015) The Effectiveness of Coercive and Persuasive Counterinsurgency Practices since 1945. Civil Wars, 17:503–526

Patterson W (2016) Democratic Counterinsurgents. How Democracies Can Prevail in Irregular Warfare. Palgrave Macmillan, London

Paul C, Yeats J, Clarke C P, Matthews M (2015a) Assessing and Evaluating Department of Defense Efforts to Inform, Influence, and Persuade: Desk Reference. RAND, Santa Monica CA

Paul C, Yeats J, Clarke C P, Matthews M, Skrabala L (2015b) Assessing and Evaluating Department of Defense Efforts to Inform, Influence, and Persuade: Handbook for Practitioners. RAND, Santa Monica CA

Payne K (2013) Social Psychology in Classic Counterinsurgency Writing. Defence Studies, 13:80–98

Pechenkina A O, Bennett D S (2017) Violent and Non-Violent Strategies of Counterinsurgency. JASSS, 20:1–11

Pechenkina A O, Bausch A W, Skinner K K (2019) How do civilians attribute blame for state indiscriminate violence? Journal of Peace Research, 56:545–558

Perloff R M (2010) The dynamics of persuasion. Communication and attitudes in the 21st century. Routledge, New York

Petit V (2019) The Behavioural Drivers Model: A Conceptual Framework for Social and Behaviour Change Programming. UNICEF, Amman

Powers P (2007) Persuasion and Coercion: A Critical Review of Philosophical and Empirical Approaches. HEC Forum, 19:125–143

Price B C (2012) Targeting Top Terrorists: How Leadership Decapitation Contributes to Counterterrorism. International Security 36:9–46

Ray T (2015) Net-Centric Logistics: Complex Systems Science Aims at Moving Targets. In: Fellman P V, Bar-Yam Y, Minai A A (eds) Conflict and Complexity. Countering Terrorism, Insurgency, Ethnic and Regional Violence. Springer, New York, pp 137–146

Reus-Smit C (2007) International Crises of Legitimacy. International Politics, 44:157–174

Romano D (2012) Turkish and Iranian Efforts to Deter Kurdish Insurgent Attacks. In: Wenger A, Wilner A (eds) Deterring Terrorism: Theory and Practice. Stanford University Press, Stanford CA, pp 228–250

Rossman G B, Rallis S F (2017) An Introduction to Qualitative Research. Learning in the Field. Sage Publications, Thousand Oaks CA
Rueda M R (2017) Popular Support, Violence, and Territorial Control in Civil War. Journal of Conflict Resolution, 61:1626–1652
Schmid A P (2011) The Routledge Handbook of Terrorism Research. Routledge, Oxon
Schram P (2019) Managing Insurgency. Journal of Conflict Resolution, 63:2319–2353
Schutte S (2015) Geography, Outcome, and Casualties: A Unified Model of Insurgency. Journal of Conflict Resolution, 59:1101–1128
Secure Livelihoods Research Consortium (2017) Understanding Rural Markets in Afghanistan (Policy Briefing 27). Secure Livelihoods Research Consortium, London
Silverman D (2019) What Shapes Civilian Beliefs about Violent Events? Experimental Evidence from Pakistan. Journal of Conflict Resolution, 63:1460–1487
Suchman M C (1995) Managing Legitimacy: Strategic and Institutional Approaches. Academy of Management Review, 20:571–610
Tatham S (2015a) The Solution to Russian Propaganda is not EU or NATO Propaganda but Advanced Social Science to Understand and Mitigate its Effect in Targeted Populations (Policy Paper No. 4). National Defence Academy of Latvia, Riga
Tatham S (2015b) Using Target Audience Analysis to Aid Strategic Level Decisionmaking. Strategic Studies Institute, Carlisle PA
Tatham S, Giles K (2015) Training Humans for the Human Domain. Strategic Studies Institute, Carlisle PA
Tatham S, Le Page R (2014) NATO Strategic Communication: More to be Done? (Policy Paper No. 1). National Defence Academy of Latvia, Riga
The Soufan Group (2015). Foreign Fighters: An Updated Assessment of the Flow of Foreign Fighters into Syria and Iraq. The Soufan Group, New York
Toros H (2008) ‘’We Don’t Negotiate with Terorrists!’: Legitimacy and Complexity in Terrorist Conflicts. Security Dialogue, 39:407–426
Treadwell J (2018) Doing Ultrarealist Ethnography: Romanticism and Running with the Riotous (While Buying Your Round). In: Rice S K, Maltz M D (eds) Doing Ethnography in Criminology. Discovery through Fieldwork. Springer, Cham, pp 289–302
Ucko D H (2016) ‘The People are Revolting’: An Anatomy of Authoritarian Counterinsurgency. Journal of Strategic Studies, 39.1:29–61
Unal M C (2016) Terrorism versus Insurgency: A Conceptual Analysis. Crime, Law and Social Change 66.1:21–57
UNSC (2018) Letter dated 7 November 2018 from the Chair of the Security Council Committee pursuant to resolutions 751 (1992) and 1907 (2009) concerning Somalia and Eritrea addressed to the President of the Security Council. UN Doc S/2018/1002
Vale G (2019) Women in Islamic State: From Caliphate to Camps. International Centre for Counter-Terrorism, The Hague
Van Kuijck C (2017) Delegitimising the Adversary: Understanding Actor and Audience Analysis as a Tool to Influence and Persuade. In: Ducheine P A L, Osinga F P B (eds) NL Arms: Netherlands Annual Review of Military Studies 2017. Winning Without Killing: The Strategic and Operational Utility of Non-Kinetic Capabilities in Crises. TMC Asser Press, The Hague
Warren R P (2016) Ideological Motivations of Arab Foreign Fighters as Insurgents and Terrorists: From 1980s Afghanistan to the Syrian Insurgency. In: Romaniuk S N, Webb S T (eds) Insurgency and Counterinsurgency in Modern War. CRC Press, Boca Raton FL, pp 53–72
Wenger A, Wilner A (2012) Deterring Terrorism: Theory and Practice. Stanford University Press, Stanford
Wilner A (2010a) Delegitimising Terrorism: A better way to counter radicalization and recruitment in the west. AIMS
Wilner A (2010b) Targeted Killings in Afghanistan: Measuring Coercion and Deterrence in Counterterrorism and Counterinsurgency. Studies in Conflict & Terrorism, 33.4:307–329

Wilner A (2011) Deterring the Undeterrable: Coercion, Denial, and Delegitimization in Counterterrorism. Journal of Strategic Studies, 34.1:3–37
Wilner A (2013) Fencing in Warfare: Threats, Punishment, and Intra-War Deterrence in Counterterrorism. Security Studies, 22.4:740–772
Wilner A (2015a) Deterring Rational Fanatics. Pennsylvania University Press, Philadelphia
Wilner A (2015b) Contemporary Deterrence Theory and Counterterrorism: A Bridge Too Far? NYU Journal of International Law and Politics, 47.2:439–462
Wong D H (2009) Power, Its Forms, Bases, and Uses. Transaction Publishers, London
Wong S, Guggenheim S (2018) Community-Driven Development. Myths and Realities (Policy Research Working Paper 8435). World Bank Group – Social, Urban, Rural and Resilience Global Practice, Washington DC
Zhukov Y M (2012) Counterinsurgency in a non-democratic state: the Russian example. In: Rich P B, Duyvesteyn I (eds) The Routledge Handbook of Insurgency and Counterinsurgency. Routledge, Oxon, pp 286–300

Dr. Martijn Kitzen (Ph.D., MA) is associate professor of war studies at the Netherlands Defence Academy. His research and teaching focus on irregular warfare, special operations, counterinsurgency and stabilization in highly fragmented societies. He has been involved in pre-deployment training for various nations, worked as in-theatre advisor in Afghanistan, and served as academic advisor for the revision of NATO's AJP 3.4.4 (counterinsurgency). Martijn holds a Ph.D. in history and a MA in political science and is a former military officer with experience in NATO and UN missions.

Christina van Kuijck (LLM, MA) is a research scientist currently working for the Netherlands Ministry of Defence. Her work focuses on behaviour change, strategic communication, and international law, particularly in the context of counterterrorism and counterinsurgency.

Chapter 16
"This Has Triggered a Civil War": Russian Deterrence of Democratic Revolts

Maarten Rothman

Contents

Abstract This chapter examines the use of deterrence by President Putin of the Russian Federation against potential democratic revolts. It combines insights from the literatures on democratic revolutions and social movements on the one hand and deterrence and coercion on the other. This exploratory research sketches a rough model of a strategy to deter democratic revolts. From Putin's perspective, democratic revolts present a severe strategic threat. The chapter distinguishes two channels through which he can discourage or deter democratic revolts: suppression and the threat of intervention. It focuses on the latter and specifically on punishment after the revolt. Democratic revolts are not enacted by a unitary actor but by an emergent collective which, strictly speaking, does not exist prior to the event; this deprives the deterrent actor of the part of his arsenal that goes through backchannels. The alternative, targeting the population at large, carries increased risk that the threat backfires. Putin formulates carefully according to a rhetorical strategy that obscures his own role while ensuring the threat is mainly carried by news media, which report the failing aspirations of previous democratic revolts and the pains

M. Rothman (✉)
Faculty of Military Sciences, Netherlands Defence Academy, Breda, The Netherlands
e-mail: mgdrothman@hotmail.com

F. Osinga and T. Sweijs (eds.), *NL ARMS Netherlands Annual Review of Military Studies 2020*, NL ARMS, https://doi.org/10.1007/978-94-6265-419-8_16

suffered by the people who fought for them. It serves Russia's interests to periodically feed the media by manufacturing incidents in any of the large number of frozen conflicts in which it is involved.

Keywords Putin · Democratization · Third Wave · Revolution · Agency · Activism · Intervention · Deterrence · Punishment · Frozen conflict

> Of course, political and social problems have been piling up for a long time in this region [the Middle East and Northern Africa], and people there wanted change. But what was the actual outcome? Instead of bringing about reforms, aggressive intervention rashly destroyed government institutions and the local way of life. Instead of democracy and progress, there is now violence, poverty, social disasters and total disregard for human rights, including even the right to life.

(Vladimir Putin in a speech to the UN General Assembly on 28 September 2015.)[1]

16.1 Introduction

This chapter examines the use of deterrence by President Putin of the Russian Federation against potential democratic revolts. From Putin's perspective democratization is a strategic threat not only to his own regime but also to his friends and allies, especially in the near abroad or what might be called his sphere of influence. Certainly Putin is not the only leader of a non-democratic state who views democratization negatively, but he does seem to be particularly active in fighting and discouraging democratic revolts against his allies.

Besides the utility of understanding the activities of an important factor in international politics today, the study of Putin's strategy promises to fill a gap in the literature on deterrence. Deterrence theory from the first concerned itself with the relations between states. Its focus on the use of military threats as a means to prevent war eminently suited the Cold War.[2] As proxy wars between the superpowers gained attention and strategic thought turned to limiting (horizontal and vertical) escalation, the conceptual frame was broadened to include coercive diplomacy, or simply coercion, meaning the use of military threats to compel one state to concede the demands of another.[3] After 1989 the emphasis on frightening

[1]Putin 2015. All quotes are from the version published by the Office of the President of Russia.
[2]Buzan and Hansen 2009.
[3]Schelling 1966; George 1991.

away the other superpower faded and Western scholarship began to include discussion on coercing non-state actors, especially insurgent groups.[4] Subsequent literature has understandably focused on terrorist organizations and, more recently, on renewed superpower competition, not only with Russia but also China. It has also gradually incorporated aspects of constructivism, matching a shift in security studies generally.[5] This has re-emphasized the importance of psychology and communication. It also increased attention to non-Western views, including of the spread of democracy and expansion of the Western sphere of influence; however, only the latter has been approached from the perspective of deterrence. Studies on coercing non-state actors have included assistance to friendly states, such as the US efforts against the Vietcong; Russian intervention in Syria also fits this category. However, they have focused on violent non-state actors and not on democratic movements.

Meanwhile the literature on social movements deals overwhelmingly with domestic relations. It usually includes domestic repression as well as the means available to social movement to put pressure on the authorities.[6] Certainly this fits coercion and deterrence broadly defined, i.e. inducing fear to coerce an adversary to yield to the coercer's will, though the usual term for the use of fear in the relations between the state and its citizens is state terror. Van Creveld remarked on the salutary effect of Hafez al-Assad's 1982 bombing of Homs, discouraging further revolts by the Muslim Brotherhood and stabilizing his regime.[7] Over the past two decades the resilience of authoritarian regimes has become an established topic in research on revolutions.[8] Discussion of influence by outside powers in the social movement literature however, is largely limited to direct assistance to the authorities (increasing their capacity for repression) and expositions on exploitative economic relations prompting such movements in the global South.[9] What is left out of both approaches is analysis of the potential for a powerful state to use military threats to discourage popular movements against its puppets and allies.

This chapter intends to start filling that gap. Exploratory research is not meant to provide definitive answers but to draw out key concepts and hypotheses about the relations between them, while providing just enough empirical evidence to demonstrate their validity as questions. I believe that a brief case study of Russia's activities in its near abroad will furnish that evidence and allow me to sketch a rough model of a strategy to deter democratic social movements—in other words: to provide proof of concept. To be clear, we do not have access to Russia's state secrets nor to Putin's thoughts, therefore this sketch cannot prove that they are

[4]Byman and Waxman 2002. For an overview of the current state of the research on this issue, see chapter "Deterring Violent Non-state Actors" by Eitan Shamir in this volume.

[5]Knopf 2010; Lantis 2009; Lupovici 2010, 2017; see also Buzan and Hansen 2009.

[6]E.g. Stewart et al. 2012.

[7]Van Creveld 2008.

[8]Goldstone 2011; Hess 2014.

[9]E.g. Bennett 2012; Martínez-Torres and Rosset 2010.

working according to such a strategy in a formal sense. I can only prove that their activities fit with the model I develop; if they do, it demonstrates merely that the model may have some utility in understanding their goals, ways and means.

The chapter proceeds as follows: The next section sets out Russia's interest in discouraging democratic revolts. I proceed to distinguish third party deterrence from domestic repression so as to get a clear view of the strategy in question. Section 16.4 tackles the problem of the adversary which, in the case of revolution, cannot be considered a coherent actor prior to the moment of revolt. I argue that this imposes severe restraints on coercion. Finally, in Sects. 16.5 and 16.6, I outline respectively the pains Russia can inflict, and has inflicted, on a country after a revolution, and the ways in which these pains can be kept alive as a deterrent to future democratic revolts.

16.2 Strategic Impact of Democratic Revolts

This investigation must start by acknowledging the strategic importance of democratic revolts. Between 1974 and 2005, 67 countries experienced a regime change towards democracy, fifty of them driven by popular movements. The number of democracies more than doubled, from 34 to 88, while the percentage of the world population living in a democracy rose to over 50%.[10] Since then the rate of democratization has dropped, though the rate of pro-democracy revolts has stayed nearly the same. (It is not entirely clear what explains their declining success rate.)

The strategic impact of the change has been enormous. Democratic states are no longer a beleaguered minority, they now easily find friends in other democracies around the world. Southern and eastern Europe have been transformed, not only introducing democracy at home but also acceding to membership in NATO and EU. Latin America for the most part followed suit. The United States' allies along the Pacific Rim also democratized. Western claims to defend freedom and democracy gained credibility. While the US military adventure in Iraq after 2003 squandered part of that gain, it did not negate the soft power advantage of having a socio-political system that peoples across the world strive to emulate.

I do not here adopt an idealist perspective on these changes; viewing them through the eyes of Putin means assessing their impact in realist terms.[11] The West gained an enormous amount of territory, along with its population and resources. It increased its own strategic depth in Europe while stripping Russia of its buffer zone. As Russia's former satellites switched of their own accord, the West gained all this at very little cost to itself. NATO now directly borders Russia and the border sits much closer to Russia's strategic heartland than to NATO's historic core on the

[10]Rothman 2017; Hale 2013; Kinsman 2011; Doorenspleet 2005; Huntington 1991.

[11]Tsygankov 2015; Larson and Shevchenko 2014; Sakwa 2013.

shores of the Atlantic. Periodic democratic revolts in Russia's neighbours, including Ukraine and Georgia, keep up the pressure. Even when they fail to install democratic regimes, they demand Russia's attention and resources. Russia has spent resources to prop up friendly regimes; it has fought an open war in Georgia in 2008 and a covert one in Ukraine from 2014, while giving substantial military support to Assad in Syria from 2012 and intervening directly from 2015. Each of these conflicts started with a democratic revolt and in each, Russia was fighting not to expand its influence but to keep what it had. From Putin's perspective, then, democratic revolts present a severe strategic threat.

In an earlier article, I analysed Putin's rhetoric, focusing on the speech he gave to the United Nations in 2015.[12] I argued that he invokes realism as a denial of the agency of pro-democracy protesters. He recasts democratic revolts as extensions of Western influence, even calling the Maidan Revolution "a coup d'état from abroad"[13] and putting promotion of democracy in Ukraine and Syria in the same category as armed interventions such as in Libya 2011 and the US invasion of Iraq in 2003, all of which he condemns as breaches of the principle of state sovereignty. But the reality is that the revolts had domestic causes, were largely triggered by domestic events and their main protagonists were domestic NGOs.[14] While the realist overlay is fitting when considering the outcome of the recent waves of democratization, it does not fit its causes or its operative mechanisms. In this chapter, I proceed on the assumption that Putin is well aware of this and is confusing the matter on purpose. His rhetoric aims at discouraging Western intervention, as well as gaining diplomatic credit with leaders of other non-democratic states, but surely he is under no illusion that doing so will end the revolts themselves. So what is he doing to discourage those?

16.3 Deterrence and Domestic Repression

We can distinguish two channels through which Putin and his allies may discourage or deter democratic revolts. The first is suppression by the authorities of the affected country. The second is the threat of intervention, either in support of those allies during the uprising or as punishment after their overthrow.

Certainly, these two are often intertwined; as Byman and Waxman remark "the fundamental issue is whether a specific threat, in the context of other pressures, significantly affected an opponent's decision making."[15] The adversary, in this case the pro-democracy protesters or prospective protesters (more on them in Sect. 16.4),

[12]Rothman 2017. That chapter also dealt extensively with Western support for democratic revolutions, to reduce complexity I leave it out of the present chapter.

[13]Putin 2015.

[14]Rothman 2017; cf. Lukes 2005; Mattern 2005.

[15]Byman and Waxman 2002, p. 32.

experiences both domestic repression and the threat from outside at the same time and, to the extent that he regards the local authorities as marionettes, is even likely to view them as coming from the same source. The two channels are also quite closely linked conceptually, as explained above.

Nevertheless, I will focus here only on the threat of punishment after the fact. My first reason is that there are already sizeable literatures on domestic repression and intervention in civil wars per se; focusing on the potential effect of a third-party deterrent adds a new element into the mix (and it fits the theme of this volume). The second is that intervention in order to punish after democratic revolts has been a unique characteristic of Russian foreign policy in recent decades. Interventions in Moldova and Georgia actually predate Putin so it is unwise to view them only as expressions of his personal politics, it is probably more correct to see them as motivated by the attitudes of a significant section of the Russian political elite.[16] Still, the number and intensity of such activities have grown during Putin's tenure to the extent that Western observers now perceive them as a threat not only to Russia's smaller neighbours but also to NATO.

Such fears are perhaps overblown if, as I argue, Russia's interventions are responses to democratic revolts, but they do reflect a ramping up of Russia's efforts to limit the spread of democracy in its sphere of influence.[17] Note that Russia has not always answered regime change with armed intervention, the strategy of co-opting the new leaders is also part of its repertoire, for example in Kyrgyzstan after the 2005 Tulip Revolution and in Armenia in 2018. Armed intervention is clearly not the only tool in its toolbox.[18] Where it has opposed the new government, Russia has shown a preference for hybrid intervention using local insurgents in combination its own assets, particularly intelligence operators and so-called peacekeeping forces.[19] NATO's worry about Russia's activities is focused on this mode of operation, i.e. on capabilities rather than intentions. Below I show that hybridity offers major advantages to Russia in the context of a democratic revolt, only some of which apply to operations against NATO targets.

It is useful to draw out a few distinctions between domestic repression and punishment after the fact in order to get a clearer view of the type of intervention that concerns us here. Domestic repression is under the control of the local authorities, Putin's allies, who might take some guidance or direction from him but for the most part rely on local resources and personnel. The effectiveness of domestic repression depends on local restraints and sympathies, including those of security services personnel. The decision to use violence is often a pivot point, when the loyalty of the security services is tested against their sympathy for the protesters and their goals; it is frequently the point at which they refuse their orders

[16]Tsygankov 2015; Tsygankov and Tsygankov 2010; Seely 2017; Larson and Shevchenko 2014; Sakwa 2013.

[17]Thornton 2017.

[18]Cf. Seely 2017.

[19]Seely 2017; Savage 2018.

and the regime's authority collapses (examples include the first democratic revolt of our era, the 1974 Carnation Revolution in Portugal and the 2014 Maidan revolution in Ukraine). Russian punishment makes use of local strongmen but also employs Russian operators and usually a sizeable contingent of soldiers and, most importantly, the punishment is directed from Moscow.[20] Russia's ability to inflict punishment therefore does not suffer the same constraints: most of the men with guns are not compatriots, do not share local sympathies, and such defections as there may be do not threaten the collapse of Moscow's authority.

There is also a difference in the timing of the actions. Domestic repression takes place prior to and during pro-democracy protests, and afterwards if the regime survives them. The punishment threatened by Putin takes place after the revolt, if the regime does not survive. The threat, of course, is active at every stage of the process, but that is a matter I take up below. First we must deal with a problem in identifying the adversary.

16.4 The Elusive Adversary

Democratic revolts are not enacted by a unitary actor but by a collective which, strictly speaking, does not exist prior to the event. Revolutions are attempts at regime change bypassing the regular procedures through mass mobilization. This last element seems to indicate a degree of organization but this is misleading. The academic literature links revolutions to social movements[21] which, in turn, are described as "a network of informal interactions between a plurality of individuals, groups and/or organizations, engaged in a political or cultural conflict, on the basis of a shared collective identity".[22] The people taking to the streets are often called by a collective noun but their collectivity does not lie in any organization they are all part of. They do not even always share the same goals, other than removing the current regime; revolutionary movements are frequently rainbow coalitions with divergent ideas about the ordering of society after the revolution.

Most protesters are discontented citizens who might take to the streets if pushed too far, or who are already disposed to protest but waiting for the right opportunity. The root cause of democratic revolts is dissatisfaction with the conditions of life (poverty and lack of economic opportunity as well as lack of political rights) under the ancient regime but such regimes are not easily toppled, in fact in the face of widespread discontent they are remarkably resilient.[23] Protesters face a collective action problem: they find safety in numbers but, to get them to turn out, someone

[20]Savage 2018.

[21]Karatnycky 2005.

[22]Diani 1992; cf. James and Van Seters 2014.

[23]Goldstone 2011; Way 2011; Hess 2014.

needs to initiate the protest while, if they initiate protests alone or in a small group, they can easily be arrested by the authorities.[24] Much recent debate has focused on the contribution of social media as a new and relatively efficient form of horizontal communication between protesters but again such networks seem to form during the event rather than to presage them; revolutionary groups who organize through social media before the revolution are quite susceptible to interference by the authorities.[25] This is why triggers events, such as blatant election fraud, are so important for aspiring protesters, as they can expect a large number of people at the same time to be angry enough to protest. Protests jumping from one country to another in a revolutionary wave have a similar effect.[26] In effect the trigger event turns a dissolute mass into an actor.

Security services of autocratic regimes spend much effort trying to identify potential protest leaders. It is possible to fashion a sociological profile of such individuals but very hard to fine-tune it to such an extent that it can be used to pinpoint the next protest's leaders. Authoritarian regimes can arrest members of activist groups, if they can find them, or institute forms of repression which inhibit or disrupt their activities. It is true that activist groups form a crucial component of revolutions because their members are more skilled than the average protester, better trained and knowledgeable about effective tactics. In this sense they indeed provide a degree of organization to the larger group.[27] But there are usually many activist groups, most of them small and quite loosely organized themselves, and it is hard to tell in advance which of them will prove decisive in the event. It is impossible to measure how many revolts were prevented by the security services' efforts against potential leaders or how they affected the success rate of those that did occur but it should be noted that those revolts that did occur (approximately 1.5 per year worldwide)[28] always found activists willing and able to help organize them.

The lack of an adversary prior to democratic revolts deprives the deterrent actor of a part of his arsenal. When there is no clear organization, there are no backchannels for secret negotiations, no threats to intimidate the leadership, no bribes to drop a collective demand in return for personal reward.[29] These options return in time, when new leaders emerge out of the revolt, but even then leaders are unlikely to disown the revolution that made them and their control over their followers is likely insufficient to take them along. More importantly, carrots and

[24]Tucker 2007; Tilly 1978.

[25]Hussain and Howard 2013; Rod and Weidmann 2015; Little 2016.

[26]Hale 2013; Saideman 2012; Snow and Benford 1992.

[27]Rod and Weidman 2015.

[28]Kinsman 2011; after 2011 popular revolts in Maldives, Central African Republic, Tunisia, Ukraine, Thailand, Abkhazia, Hong Kong, Burkina Faso, Burundi, South Korea, Jordan, Sudan, Algeria, Iraq, Lebanon, Armenia, Nicaragua, Haiti and Bolivia kept up the pace (19 in 9 years). This list includes both successful and unsuccessful revolts but not regional rebellions, small-scale protests and social movements with limited aims.

[29]Seely 2017.

sticks aimed specifically at leaders cannot be used when they have not yet emerged, so this does nothing to deter potential revolters.

This leaves the deterrent actor with one remaining option: targeting the people at large. In terms of communication this means public diplomacy. Byman and Waxman point to "audience costs" increasing the risk that a threat backfires.[30] Leaders do not want to be seen caving in to foreign demands; they and their supporters are prone to anger instead. The lack of backchannel, or even a confidential diplomatic channel, thus complicates matters for the coercer. To avoid overcoercion, as Byman and Waxman call it, coercing states can refrain from specific threats and speak more vaguely about dire consequences. This may explain the passive form in this passage from Putin's UN speech:

> Sooner or later, this logic of confrontation was bound to spark off a major geopolitical crisis. And that is exactly what happened in Ukraine, where the people's widespread frustration with the government was used for instigating a coup d'état from abroad. This has triggered a civil war.[31]

The audience knows that there would have been no civil war without Russian intervention; Putin is speaking about himself, he is implying that it might happen again, but the passive form allows him to cast civil war as a warning rather than a threat.

16.5 Punishment and Threat

Byman and Waxman helpfully provide an analysis of coercive mechanisms, the next section liberally borrows from their work. As explained above, neither they nor subsequent students of coercion have extended the analysis to popular movements. However, they include strategies to weaken an adversary state and to hurt the population in order to put pressure on the government (Byman and Waxman call them unrest strategies), from which we may simply leave out the second step.[32]

Russia intervened in Georgia in 1991, 2003 and 2008, and in Ukraine in 2005 and again in 2014, each time except 2008 directly after a democratic revolution. (In 2008 Russia intervened to prevent Georgia retaking a separatist province which was created after the 1991 revolution.) In each of these cases it mixed economic sanctions with support to insurgents. Economic sanctions include cutting of delivery of natural gas at subsidized prices, driving up the cost of living in the target country. Embargoes reduce exports, forcing companies to reduce production and lay off workers, leading to unemployment. The destruction of physical assets in war also imposes economic hardship on the population. The effect of economic pain is not only that it hurts directly but also that it negates one of the most salient promises

[30]Byman and Waxman 2002, p. 36; Weeks 2008; cf. Fearon 1994.

[31]Putin 2015.

[32]Byman and Waxman 2002, pp. 65–72, 76–78.

of democratic revolution; after all economic malaise and rampant corruption are two of their most important drivers.[33]

Support to insurgents is Russia's signature mode of intervention. The ethnic composition of most ex-Soviet republics is such that minorities are prominent in some regions, even if they do not make up a majority in them, and they have tended, with some prodding from Moscow, to clamour for autonomy or even independence. There is no doubt that Russian intelligence supported radical separatist groups and probably created some out of thin air. Russian support propped up separatist "governments" in Transnistria, Abkhazia, South-Ossetia and the Donbass. The material consequences of war include administrative paralysis, loss of economic assets, social fragmentation and displacement of population. Each of these hurts the population as a whole.[34] Another important effect of such insurgencies is loss of territory and national humiliation. This too strikes at the hopes of the revolutionaries, at least the many among them who hated the regime for putting the interest of their patron over those of their countrymen.

The effects of Russia's intervention are enhanced by the conditions of social and political confusion in the immediate aftermath of revolution. Political and administrative confusion limit the ability of the new government to counter effectively. Government positions are unfilled, chains of command interrupted, the security services (a crucial support for the old regime until the final moments) in disarray. Divisions between various former opposition groups offer opportunities for divide and rule for Russia to exploit. These are ideal moments for an intervention, particularly in hybrid form so as to seemingly offer chances for reconciliation (inhibiting strong countermeasures) and harness support from elements of the old government coalition.[35] Crucially, hybrid intervention through domestic opposition groups (however artificial) masks the extent of foreign agency, thereby limiting the rally around the flag effect in the short term. It also maintains a degree (however limited) of plausible deniability and thus a chance of diplomatic de-escalation in the medium term (including with Western supporters of the democratizers). In Abkhazia and South-Ossetia diplomatic de-escalation resulted in Russian troops stationed in separatist territory as "peacekeepers". In the long term, hybridity's mask allows Putin to present the pain he inflicted as a warning rather than a direct threat.

I already briefly touched on the temporal dimension above, namely, outlining the differences between domestic repression and intervention. There I placed intervention after a democratic revolt; but it can also be viewed as before another democratic revolt. Deterrence depends on credibility, which draws on the deterrer's past record of imposing the conditions that they are threatening for the future. Thus

[33]Hale 2013.

[34]Byman and Waxman 2002, pp. 117–120, analyze support for an insurgency from the perspective of pressuring a regime, in line with their perspective on pressuring a population; I again leave out the second part.

[35]Bohomolov and Lytvynenko 2012; Tsygankov 2013; Wilson 2015.

Russia's interventions are a warning to future protesters as well as a punishment. From this perspective such interventions have two targets: one to punish and one to deter. Byman and Waxman warn that: "Unrest strategies frequently fail, however, because the population cannot sufficiently influence decision making or because the coercive threat backfires, increasing popular support for defiance."[36] The first argument does not apply here because the population is itself the decision-maker. The second does not apply because the population punished is not the same as the population being deterred. Naturally this does require that the second population is aware of the pains suffered by the first. This means that the coercer must find a way to turn the short-term effects of intervention in the immediate aftermath of revolution into a long-term deterrent of the next wave. Hence final part of the puzzle: communicating the costs of defiance to an amorphous future actor at an unspecified future time.

16.6 Keeping the Threat Alive

Russia has the power to hurt democratic protesters where it counts, directly targeting the promise of a better life after the revolt. It also has the power to extend the hurt, propping up separatist governments, keeping tensions alive and thereby ensuring regular incidents of low-level violence with a risk of escalation—and that risk manageable as long as Moscow maintains its influence on the separatists. Russia has also repeatedly created crises over the delivery of natural gas, using late payments and price fluctuations as an excuse. There is a use to these crises beyond further punishment: it keeps the pain on the front page of newspapers.

Consider the limitations already named: not knowing the leadership or the organizational shape or structure of his future adversary, the coercer must use public diplomacy; but the application of coercion to the population as a whole risks angry resistance while an open threat in the presence of an audience rewards defiance and increases the cost of compliance. We have already seen that Putin formulates carefully according to a rhetorical strategy that obscures his own role. Still, the risk of the threat backfiring can be reduced further if the message were carried by another medium. News media, which report the failing aspirations of previous democratic revolts and the pains suffered by the people who fought for them, have the same deterrent effect. Note that the effect does not depend on the framing; it is sufficient that the news reports remind the potential revolter of the pain and punishment. It serves Russia's interests, then, to periodically feed the media stories of this kind by manufacturing incidents.

This interest in keeping the threat alive fits with another salient feature of Russian policy with regard to its near abroad: the large number of frozen conflicts. Russia has not used its clear military advantage to push for a definitive settlement of

[36]Byman and Waxman 2002, p. 65.

armed conflicts in which it involved itself but has contented itself with ceasefires. It maintains these at some cost to itself by stationing troops in the breakaway republics. Presumably it gains something from the conflicts' unresolved state. Analysis of these conflicts generally focuses on local nationalisms, while acknowledging that Russia's interest in them lies rather in preventing the affected countries from allying with the West.[37] In this respect the presence of Russian forces on their territory and the possibility of using them if the conflict were, at Moscow's discretion, to flare up again, restrains the governments of Moldova, Georgia and Ukraine. From the perspective adopted in this chapter, the advantage lies rather in the warning to other peoples in Russia's orbit.

Rather than viewing frozen conflicts as outcomes or results of Russia's foreign policy, they should be seen as instruments. They are better described with the term "managed instability"[38] as this term makes it explicit that Russia is in control of the situation and is applying the pain strategically. If the above analysis is correct, it does so not only to influence events in the target country but also to signal to potential democratic protesters elsewhere that a revolution carries tremendous costs.

16.7 Conclusion

This chapter combined insights from the literatures on democratic revolutions and social movements on the one hand, and deterrence and coercion on the other. Together they gave greater insight in an under investigated aspect of Russian foreign policy, namely the way in which it deters democratic revolts against governments in its sphere of influence. As exploratory research the conclusions presented here cannot be taken as the last word on the matter but should be seen rather as directions for further research.

As we have seen, the threat is formed out of previous instances of punishment after a revolution, its credibility maintained by nonresolution of the resulting "separatist" conflicts. Gradually, over a long period of time, the creation and periodic flaring up of frozen conflicts build up the shadow of the future. The strategy outlined in this chapter is an example of general deterrence, a long-term threat that prevents an action whether it is planned or not. By contrast immediate deterrence is directed at a specific, planned event; with respect to democratic revolts the absence of a coherent actor prior to the uprising makes such specificity impossible.

The particular condition of facing an unknown adversary also imposes more stringent constraints on communicating threats than usual because it eliminates back channels and forces the coercer to rely on public diplomacy. Thus the crucial element in the strategy is communicating the threat of punishment in a way that

[37]Coyle 2017.

[38]Tolstrup 2009; contra Seely 2017.

avoids blowback. The chapter has emphasized the importance of signaling in support of deterrence, not just by words but also by deeds. Research in coercive diplomacy has recognized this long ago[39] but the analysis had not been extended to social movements; this chapter suggests it may be even more important in such cases than between state actors or between states and violent non-state actors which usually possess some sort of organizational structure.

The combination of a carefully worded "warning" by Putin and news reports of gruesome events elsewhere avoids adding insult to injury and allows for greater diplomatic flexibility. Hybrid operations and managed instability both aid in communicating the threat. In this sense, the research here supports and extends Robert Seely's conclusion that Russia's current leadership has successfully fused warfare and statecraft.[40]

Like Seely, I view Russia's goals as largely defensive; the strategy outlined here is tailor-made to deter democratic revolutions against its allies in the near abroad. The particular combination of tools used in the strategy cannot be copied wholesale to other theaters, though further research may discover applications of some of its elements, or combinations of elements, that could be used elsewhere. Counterstrategies, including assistance from other powerful states, have been deliberately left out of consideration here. Obviously these would be relevant topics for further research.

References

Bennett E A (2012) Global social movements in global governance. Globalizations 9:799–813

Bohomolov O, Lytvynenko O V (2012) A ghost in the mirror: Russian soft power in Ukraine. Chatham House, London

Buzan B, Hansen L (2009) The evolution of international security studies. Cambridge University Press, Cambridge

Byman D, Waxman M (2002) The dynamics of coercion: American foreign policy and the limits of military might. Cambridge University Press, Cambridge

Coyle J J (2017) Russia's Border Wars and Frozen Conflicts. Springer, Cham

Diani M (1992) The concept of social movement. The Sociological Review 40:1–25

Doorenspleet R (2005) Democratic transitions: Exploring the structural sources of the fourth wave. Lynne Rienner Publishers, Boulder

Fearon J D (1994) Domestic political audiences and the escalation of international disputes. American Political Science Review 88:577–592

George A (1991) Forceful Persuasion: Coercive Diplomacy as an Alternative to War. United States Institute of Peace Press, Washington DC

Goldstone J (2011) Understanding the Revolutions of 2011. Resilience and Weakness in Middle Eastern Autocracies. Foreign Affairs 90:8–16

Hale H E (2013) Regime Change Cascades: What We Have Learned from the 1848 Revolutions to the 2011 Arab Uprisings. Annual Review of Political Science 16:331–353

[39]George 1991.

[40]Seely 2017.

Hess S (2014) Sources of Authoritarian Resilience in Regional Protest Waves: The Post-Communist Colour Revolutions and 2011 Arab Uprisings. Government and Opposition 51:1–29
Huntington S P (1991) The third wave: Democratization in the late twentieth century. University of Oklahoma Press, Norman
Hussain M M, Howard P N (2013) What Best Explains Successful Protest Cascades? ICTs and the Fuzzy Causes of the Arab Spring. International Studies Review 15:48–66
James P, Van Seters P (2014) Globalization and politics, vol. 2: Global social movements and global civil society: A critical overview. Sage, London
Karatnycky A (2005) How freedom is won: from civic resistance to durable democracy. Freedom House, New York
Kinsman J (2011) Democracy rising: Tunisia and Egypt, when idealists got it right. Policy Options Montreal 32:37–43
Knopf J W (2010) The fourth wave in deterrence research. Contemporary Security Policy 31:1–33
Lantis J S (2009) Strategic culture and tailored deterrence: Bridging the gap between theory and practice. Contemporary Security Policy 30:467–485
Larson D W, Shevchenko A (2014) Russia says no: Power, status, and emotions in foreign policy. Communist and Post-Communist Studies 47:269–279
Little A T (2016) Communication Technology and Protest. The Journal of Politics 78:152–166
Lukes S (2005) Power and the Battle for Hearts and Minds. Millennium Journal of International Studies 33:477–493
Lupovici A (2010) The Emerging Fourth Wave of Deterrence Theory: Toward a New Research Agenda. International Studies Quarterly 54:705–732
Lupovici A (2017) Toward a Securitization Theory of Deterrence. International Studies Quarterly 63:177–186
Martinez-Torres M E, Rosset P M (2010) La Vía Campesina: the birth and evolution of a transnational social movement. The Journal of Peasant Studies 37:149–175
Mattern J (2005) Why 'Soft Power' Isn't So Soft: Representational Force and the Sociolinguistic Construction of Attraction in World Politics. Millennium Journal of International Studies 33:583–612
Putin V (2015) 70th session of the UN General Assembly http://en.kremlin.ru/events/president/news/50385 Accessed 6 September 2016
Rod E G, Weidmann N B (2015) Empowering activists or autocrats? The Internet in authoritarian regimes. Journal of Peace Research 52:338–351
Rothman M (2017) On the Instrumentality of Soft Power; or Putin Against Democracy Promotion. In: Ducheine P A L, Osinga F P B (eds) NL ARMS - Netherlands Annual Review of Military Studies 2017 - Winning Without Killing: The Strategic and Operational Utility of Non-Kinetic Capabilities in Crises. TMC Asser Press, The Hague
Saideman S M (2012) When Conflict Spreads: Arab Spring and the Limits of Diffusion. International Interactions 38:713–722
Sakwa R (2013) The cold peace: Russo-Western relations as a mimetic cold war. Cambridge Review of International Affairs 26:203–224
Savage P J (2018) The Conventionality of Russia's Unconventional Warfare. Parameters 48:77–86
Schelling T (1966) Arms and Influence. Yale University Press, New Haven
Seely R (2017) Defining Contemporary Russian Warfare: Beyond the Hybrid Headline. The RUSI Journal 162:50–59
Snow D A, Benford R D (1992) Master frames and cycles of protest. In: Morris A D, Mueller C M (eds) Frontiers in Social Movement Theory. Yale University Press, New Haven, pp 133–155
Stewart C J, Smith C A, Denton R E Jr (2012) Persuasion and social movements. Waveland Press, Long Grove
Thornton R (2017) The Russian Military's New 'Main Emphasis' Asymmetric Warfare. The RUSI Journal 162:18–28
Tilly C (1978) From mobilization to revolution. Addison-Wesley, Reading MA

Tolstrup J (2009) Studying a negative external actor: Russia's management of stability and instability in the 'Near Abroad'. Democratization 16:922–944
Tsygankov A P (2013) Moscow's soft power strategy. Current History 112:259–264
Tsygankov A P (2015) Vladimir Putin's last stand: The sources of Russia's Ukraine policy. Post-Soviet Affairs 31:279–303
Tsygankov A P, Tsygankov P A (2010) National ideology and IR theory: Three incarnations of the 'Russian idea'. European Journal of International Relations 16:663–686
Tucker J A (2007) Enough! Electoral Fraud, Collective Action Problems, and Post-Communist Colored Revolutions. Perspectives on Politics 5:535–551
Van Creveld M (2008) The changing face of war: Combat from the Marne to Iraq. Presidio Press, New York
Way L (2011) The Lessons of 1989. Journal of Democracy 22:13–23
Weeks J L (2008) Autocratic audience costs: Regime type and signaling resolve. International Organization 62:35–64
Wilson J L (2015) Russia and China Respond to Soft Power: Interpretation and Readaptation of a Western Construct. Politics 35:287–300

Dr. Maarten Rothman (Ph.D.) is associate professor of International Security Studies at the War Studies Department of the Netherlands Defence Academy. He obtained his Ph.D. from Purdue University.

Chapter 17
Deterrence in Peace Operations: Look Beyond the Battlefield and Expand the Number of Targets and Influence Mechanisms

Peter Viggo Jakobsen

Contents

Abstract The peace operations literature suffers from a narrow focus on battlefield deterrence. It ignores the need to deter actors beyond the battlefield from supporting the combatants using force, and analyses the use of military threats and force in peace operations in a vacuum without taking into account the other instruments that deterring actors employ simultaneously to influence the combatants, combatant allies, combatant supporters and bystanders that undermine deterrence in peace operations. Since most peace operation forces lack the capacity and willingness to threaten and use force in accordance with the requirements stipulated by rational deterrence theory, influencing actors beyond the battlefield is more important with respect to deterring violence than the military efforts undertaken by peace operation forces to deter combatants from using force or to compel them to stop doing so. Accordingly, this chapter develops a new analytical framework that will enable peace operation theorists and practitioners to target all the actors that undermine deterrence on the battlefield and beyond with all the tools at their disposal—

P. V. Jakobsen (✉)
The Institute for Strategy, The Royal Danish Defence College, Copenhagen, Denmark
e-mail: peja@fak.dk

P. V. Jakobsen
Center for War Studies, University of Southern Denmark, Odense, Denmark

F. Osinga and T. Sweijs (eds.), *NL ARMS Netherlands Annual Review of Military Studies 2020*, NL ARMS, https://doi.org/10.1007/978-94-6265-419-8_17

persuasion, inducement and coercion. The framework will improve both theory and practice by providing a better understanding of the conditions under which peace operations can contribute to deterring and, if need be, compelling combatants from using force as well as identifying the tools that practitioners can employ to this end. It highlights that peace operations merely constitute the top of the deterrence iceberg, and that peace operation forces must be supported by other actors and tools to succeed with respect to deterring violence and facilitating conflict resolution.

Keywords coercion · deterrence · norms · peacekeeping · peace enforcement · persuasion · promises · punishment · rewards and threats

17.1 Introduction

The deterrence literature has developed through four waves, and, as stated by Osinga and Sweijs in the preface of this volume, the ambition in this book is to start a fifth by using new and emerging insights to address the challenges created by the growing rivalry among China, Russia and the United States, the changing character of war and rapid technological change.[1] The focus in this chapter is the nexus between deterrence theory and peace operations. The main challenge in the field of peace operations is to bring the understanding and practice of deterrence up to speed with the understanding and practice employed in most other fields. The peace operations literature is stuck in the second wave of deterrence theory that led to the formulation of the so-called rational theory of deterrence during the Cold War. According to this theory, deterrence is a rational strategy based on cost-benefit calculations, and the key to success is to communicate a clear threat to use force against potential attackers in a way that makes the cost of aggression exceed any conceivable gain.[2] Peace operation scholars and practitioners have used the rational theory of deterrence to identify the requirements for military deterrence at the tactical level, and to highlight the inability of many United Nations (UN) peace operation contingents to meet them.[3] This understanding has resulted in a trench war between two schools of thought.[4] In one trench, you have the "robust peacekeepers" advocating that peace operation forces be equipped and mandated to threaten and use force beyond self-defence to deter aggression and protect

[1]See the Preface by Osinga and Sweijs in the present volume; Jervis 1979; Knopf 2010; Lupovici 2010.

[2]See the symposium on rational deterrence theory in *World Politics* 41, no. 2 (January 1989), pp. 143–237.

[3]Berdal 2019; Crawford 1998.

[4]For reviews of this debate see Findlay 2003; Jakobsen 2000a.

civilians.[5] In the other trench, you have the "peacekeeping traditionalists" arguing that this will never work, because (UN) peace forces rarely have the military capacity and the willingness required for deterrence success in situations where consent from the conflicting parties is limited or non-existent.[6]

Attempts to authorize peace forces to use force beyond self-defence to deter violence have not been particularly successful, and the increasing number of aid workers and UN peacekeepers killed in recent years indicates the need for a new approach (see Table 17.1). Going back to traditional peacekeeping as advocated by the peacekeeping traditionalists is not a solution in itself, however, as there is far more to deterrence than the deployment of peacekeeping forces as this chapter will show.

I draw on two findings from the third and fourth waves of deterrence theory to propose a better solution. I conceptualize aggressors as coalitions composed of combatants, combatant allies, combatant supporters and bystanders, and incorporate military deterrence into a broader influence strategy that also involves persuasion and inducement. The resulting framework has three advantages compared to the predominant understanding of deterrence in the peace operations literature. First, it increases the number of deterrence targets. Second, it highlights that deterring actors have more influence mechanisms than military threats and use of force. Third, it shows that a peace operations force merely constitutes the top of the deterrence/influence iceberg. Other factors may make its (lack of) military capacity irrelevant for deterrence or rather influence success.

My argument has five parts. The first presents the predominant understanding of deterrence in peace operations theory and practice. The second develops a new typology of actors causing deterrence failure in peace operations. The third part shows how peace forces and other deterring actors use persuasion and inducement as well as coercion to increase the prospects of deterrence success. The fourth illustrates the advantages of the framework in a case study of the UN operation in Sierra Leone (UNAMSIL). UNAMSIL is a paradigmatic case for the robust peacekeeping school, and I use it to demonstrate that there was far more to its success than the deployment of a peacekeeping force capable and willing to use force at the tactical level. The chapter ends with a conclusion summarizing the main points and their implications for peace operations theory and practice.

[5]Nsia-Pepra 2017; Cruz et al. 2017.

[6]Berdal, op cit; Karlsrud 2015.

Table 17.1 Aid worker and UN peacekeeping (PKO) fatalities 1997–2017

	1997	1999	2001	2003	2005	2007	2009	2011	2013	2015	2017
Aid workers	39	33	27	87	53	88	109	86	156	110	139
UN PKO	49	39	72	108	131	90	121	115	110	125	138

(*Source* Aid Worker Security Database and United Nations Operations and Crisis Centre)

17.2 Rational Deterrence in Peace Operations—The Predominant View

The peace operation literature conceptualizes deterrence as the use of military threats to deter armed actors from attacking others in the mission area. The key to success is to deploy a peace force capable of using force against any attacker in a way that makes the costs of aggression exceed any conceivable gain. The peace force must threaten to use its military capacity against any potential attacker in a clear and credible manner for deterrence to succeed.

If follows from this understanding that unarmed observer forces and lightly armed peacekeeping forces have no or very limited military deterrence capacity (see Table 17.2). As Alan James has put it in a seminal work, "peacekeepers are not in the business of threatening and using force".[7] Their presence may have a deterrent effect if potential attackers believe that attacks on the peace force will trigger retaliation from other actors that outweigh the benefits, but the force itself has little military deterrent effect and depends upon consent and cooperation from the parties to the conflict for its success. Robust peacekeeping forces and peace enforcement forces have more military deterrence capacity as well as a mandate to use force beyond self-defence (see Table 17.2). This gives them a military capacity to deter attacks at the tactical and strategic levels respectively, if they have the capability to do so and issue credible threats of force to punish non-compliance or deny potential attackers their objectives.

In this perspective, deterrence is a question of military capacity and a willingness to issue and execute threats of force that will make the cost of aggression exceed any gain. Deterrence success is a function of effective command and control, equipment, force numbers, training, mandates, credibility and threats. If deterrence fails, unarmed observers and peacekeepers have no option but to withdraw or call upon others to intervene militarily. This is the option advocated by peacekeeping traditionalists. To prevent deterrence failure and withdrawals, the robust peacekeeping school advocates the deployment of peace forces mandated, capable and willing to use force beyond self-defence to deter aggression. Yet this option rarely exists as very few peace forces meet these military requirements for deterrence success.

[7]James 1990, p. 2.

Table 17.2 Peace operation forces, warfighting forces and military deterrence

Force type	Composition and tasks	Consent	Use of force	Deterrence capacity
Observer force	– Unarmed military observers tasked to monitor compliance	– Consent and cooperation from the parties to the conflict necessary for success	– None	– No military deterrence capacity
Peacekeeping force	– Lightly armed units in soft-skinned vehicles tasked to monitor compliance	– Consent and cooperation from the parties to the conflict necessary for success	– Minimum use of force in self-defence only at the tactical level	– Limited military deterrence capacity
Robust peacekeeping force	– Armed military units tasked to monitor and enforce compliance at the tactical level	– Consent and cooperation from the parties to the conflict at the strategic level necessary for success	– Use of force in self-defence and to enforce compliance at the tactical level	– Military deterrence capacity at the tactical level
Peace Enforcement force	– Combat capable military force tasked to monitor and enforce compliance	– Some consent and cooperation from the parties necessary for success	– Use of force in self-defence and to enforce compliance at the strategic level	– Military deterrence capacity at the strategic level
Warfighting force	– Combat capable military force tasked to defeat designated enemies and impose compliance upon them	– No consent and cooperation required for success	– Use of force to defeat all armed opposition	– Not applicable as the purpose is to win a war; not to use threats to prevent or stop one

(*Source* The author)

The predominant understanding of deterrence provides poor explanations of peace operation outcomes. Unarmed military observers and peacekeeping forces lacking the capability and willingness to threaten and use force in a credible manner have contributed to deterrence and mission success in several peace operations, whereas highly capable forces have failed to do so. The failure of NATOs peace

enforcement mission in Afghanistan clearly demonstrates that there is more to peace operations success than military deterrence at the tactical and strategic levels.[8]

This lack of explanatory power makes it necessary to rethink the understanding of deterrence in the peace operations literature. Two contributions made in the third and fourth waves of deterrence theory are useful to this end. The first is the move away from analysing deterrence as battlefield interaction between unitary (state) actors. The problems experienced by peacekeeping forces in the 1990s and the September 11 2001 terrorist attacks have led deterrence scholars to conceptualize deterring actors and aggressors as coalitions and networks. The second contribution is the move to view deterrence as part of a broader influence strategy, which integrates threats, persuasion and positive inducements into a coherent strategy. The next sections briefly present these contributions and demonstrate their relevance and implications for peace operations theory and practice.

17.3 Increasing the Number of Actors to Deter

The repeated attacks on the United Nations Protection Force (UNPROFOR) in Bosnia (1992–1995) induced scholars to examine how peace forces could use military threats and limited force to deter attacks from occurring in the first place, and to coerce aggressors to stop their use of force when deterrence broke down. Drawing on the works of second-generation deterrence (and compellence) theorists, I developed a parsimonious *ideal policy* framework identifying the minimum conditions for success that a strategy must meet to maximise the prospects of deterring or compelling combatants from attacking each other, civilians or the peace force. Compellence involves threats and, if need be, use of limited force to coerce an actor to do something against its will, i.e., stop an ongoing attack or give up something of value such as territory. Peace forces deployed in a context of ongoing conflict usually attempt to deter and compel at the same time, and the distinction between the two types of threat can be fluid and situational in this environment. Peace forces may often need to threaten and use force in order to stop attacks and re-establish deterrence, and this makes the *ideal policy* framework useful as it covers both types of threat.

The *ideal policy* is composed of a (1) a threat of force to defeat the opponent or deny it its objectives quickly with little cost; (2) a deadline for compliance; (3) an assurance to the adversary that compliance will not lead to more demands; and finally (4) an offer of carrots or positive inducements for compliance. To make a threat so potent and credible that the costs of non-compliance become unbearable,

[8]NATO forces were configured and mandated to carry out peace enforcement when they deployed in 2003. However, the unexpected level and ferocity of Taliban resistance forced it to change its posture and engage in counterinsurgency and warfighting instead.

the coercer should ideally have the capability to defeat the adversary quickly with little cost. The logic here is that that a threat to fight a short victorious war is inherently more credible than a threat to fight a long and bloody one. A deadline for compliance is key when the coercer is trying to stop attacks and other forms of hostile behaviour already taking place. It helps to create the sense of urgency and fear of unacceptable escalation in the mind of the adversary that is required for success. Moreover, unwillingness to issue a deadline is likely to be regarded as a sign of weakness and a lack of resolve by the adversary, who will be under pressure and prone to misperception and wishful thinking. Deadlines serve to limit the scope for such mistakes as well as counter-coercion and salami tactics aimed at undermining the willingness of the coercer to execute its threat. Assurance against future threats, the third component, serves to convince the adversary that compliance will not trigger tougher demands. This is crucial, as the adversary will have little incentive to comply if it fears this to be the case. Finally, use of inducements is included to reduce the costs of compliance for the adversary and increase the benefits of refraining from or stopping the use of force.[9]

My case study of UNPROFOR highlighted the difficulties involved when a coalition of actors has to formulate and implement a coercive strategy meeting the requirements of the *ideal policy*. Disagreements among the troop contributing nations, UN and NATO representatives and the permanent members of the UN Security Council often undermined threat credibility. The difficulties of meeting the *ideal policy* requirements were compounded by the fact that the coercing actors had to coerce several actors simultaneously. In addition to the main combatants made up by Bosnian Croat, Bosniak and Bosnian Serb forces, the UN and NATO also had to coerce Serbia to stop its support for the Bosnian Serbs. The use of economic sanctions played a key role in coercing Serbian President Milosevic to pressure the Bosnian Serbs to cease fire and accept the Dayton Peace Accords, which ended the war in Bosnia in 1995.[10]

The Bosnian conflict highlighted a need to move beyond the rational unitary assumption that second wave deterrence and compellence theory rests on. The conflict pitted coalitions against each other, and this created a need to deter and, if need be, coerce a variety actors on and beyond the battlefield simultaneously. It was not sufficient for deterrence success to threaten the use of force against the combatants. It was also necessary to threaten actors supporting aggression at the regional and global levels. Deterrence had to be tailor-made at each level to target the relevant actors, and threat credibility had to be established and maintained from the UN Security Council to the battlefield. Coalitional cohesion emerged as an important requirement of success.[11]

The September 11 2001 terrorist attacks reinforced the need for multi-level and multi-actor deterrence. The need to deter terrorist attacks posed a seemingly

[9]Jakobsen 1998, pp. 25–34; Jakobsen 2000b.

[10]Jakobsen 1998, op. cit.

[11]Jakobsen, op. cit.

unsurmountable problem: how do you deter highly committed terrorists willing to die for their cause? The solution provided by deterrence theorists was to disaggregate terrorist organisations into their component parts such as operatives carrying out attacks, financiers, logisticians, recruiters, supporting population segments, state supporters and religious/ideological leaders.[12] This made it possible to target each component with tailor-made campaigns to influence them to refrain from or cease their support for terrorist activities.

The key take-away from these efforts to rethink deterrence theory and practice to meet the challenges posed by internationalized intra-state conflicts and transnational terrorist networks is the need to target all the actors contributing to deterrence failure at the local, regional and global levels simultaneously. It is not sufficient to focus on tactical and operational (mission area) deterrence as most of the peace operation literature currently does. It is also necessary to target the actors beyond the battlefield that enable combatants to use force against peace forces, civilians and other parties to the conflict. The actors that make or break deterrence in peace operations can be categorized in four groups:

(1) *Combatants* that use force on the battlefield in mission areas in ways that cause deterrence to fail;
(2) *Combatant allies* that provide direct material support (men, materiel and money) to combatants using force;
(3) *Combatant supporters* that prevent others from taking action to stop deterrence failure by blocking action in regional or global institutions; and finally
(4) *Bystanders* that fail to use their power to reduce or stop deterrence failure at all levels from the battlefield to the global level.

The African Union-United Nations Hybrid Operation in Darfur (UNAMID) deployed in 2007, which by mid 2020 had suffered 278 fatalities,[13] illustrates the utility of the typology. The case is useful because it is very easy to identify actors contributing to deterrence failure in each of the four categories. The Sudanese government was the principal *combatant* causing deterring failure in the mission areas using militias to attack civilians, humanitarian organisations and UNAMID forces.[14] China's was Sudan's key *combatant ally* providing it with material (economic and military) support.[15] China, assisted by Russia, also acted as a *combatant supporter* by opposing UN resolutions threatening use of force and sanctions, and by insisting that UN peacekeepers deploy with the consent of the Sudanese government. This made it difficult for the UN Security Council to punish the Sudanese government for undermining deterrence. Finally, the Western great powers in the Security Council acted as *bystanders* because they refused to provide

[12]Knopf 2010, p. 10; Lupovici 2010; Wilner 2011.
[13]As of 3 August 2020. https://peacekeeping.un.org/en/mission/unamid.
[14]Lynch 2014a.
[15]Shinn 2009.

troops and aircraft for UNAMID and did little to influence the Sudanese government, China and Russia to prevent, stop and reduce the violence.[16]

The UNAMID case highlights the need to go beyond the mission area in order to identify all the actors influencing deterrence outcomes. To increase the prospects of deterrence success, all actors on the battlefield and beyond with a motivation and a capacity to undermine deterrence need to be influenced to refrain from doing so. Successful deterrence in peace operations require cooperation and support from key actors at all levels simultaneously, and anyone contemplating the deployment of peace forces need to assess the likelihood of obtaining the necessary cooperation at all these levels, regardless of the type of operation envisaged. Successful deterrence in peace operations is a team effort requiring cooperation and coordination from the local to the global level. Yet identifying whom to influence is only half the battle. The next step is to identify which influence mechanisms to use. This is the topic of the next section.

17.4 Increasing the Number of Influence Mechanisms

In addition to the need for adopting a multi-actor and multi-level perspective, my *ideal policy* analysis of UNPROFOR also showed that the prospects for deterrence and compellence success increased when deterring actors coupled threats with persuasion and positive inducements.[17] Other third and fourth wave studies show similar results suggesting the need for integrating deterrent threats into broader influence strategies that use threats to increase the costs of attacks *as well as* rewards to increase the benefits of restraint (not attacking) simultaneously.[18]

This adds two additional influence mechanisms—persuasion and inducement—to the quiver of deterring actors. This insight has found its way into the peace operations literature. Lise Morjé Howard captures all three mechanisms in her recent study of peacekeeping power. However, she regards them as alternatives and ends up making the peacekeeping traditionalist argument that coercion is not an option for (UN) peacekeepers.[19] She consequently fails to consider how peace forces and other actors in mission areas can use all three mechanisms simultaneously to increase their leverage vis-à-vis potential attackers. Since Howard's study focuses on the activities undertaken by UN peacekeeping operations in the field, she

[16]Lynch 2014b.

[17]Jakobsen 1998, op. cit.; Jakobsen 2000b, op. cit.

[18]George 2003, p. 465; George and Smoke 1974, p. 606; Stein 1991; United States Department of Defense 2006, p. 5; Wilner op. cit., pp. 7–8. For a classic first generation study also suggesting the use of promises to influence costs and benefits simultaneously see Snyder 1961, pp. 9–10.

[19]Howard 2019.

also ignores the leverage that these mechanisms can provide beyond the battlefield vis-à-vis combatant allies, combatant supporters and bystanders. The section below briefly presents the three mechanisms and their operational activities in turn.

Persuasion involves the transmission of information and knowledge to persuade (potential) attackers to refrain from using force. Such persuasion can be linked to peace processes and negotiations addressing the underlying drivers of conflict, or to common or local cultural understandings and norms making the resort to force illegitimate or counterproductive. As pointed out by fourth wave deterrence theorists, norms and taboos can increase the prospects of deterrence success by increasing the reputational costs of using force.[20] The norms of deterrence, non-proliferation, and non-use have in this way contributed to the success of nuclear deterrence.[21] In the same way, deterring actors can use global and local cultural norms and taboos as part of their efforts to persuade combatants, combatant allies, combatant supporters and bystanders to refrain from (contributing to) the use of force.[22] Persuasion seeking to deter aggression takes two forms: general and immediate. General persuasion is undertaken in peacetime to prevent violence from breaking out in the first place. Immediate persuasion is undertaken during crises or war to stop the outbreak of violence or to reduce or stop ongoing violence.

General persuasion improves the prospects of deterrence success by building support for and internalizing norms that make the resort to force illegitimate. Examples of such efforts include information campaigns, educational programs, and advocacy campaigns seeking to increase the knowledge and respect for international humanitarian law (IHL), prohibit sexual violence against women, terrorism, violence against non-combatants, use of child soldiers, use of "barbaric" weapons such as landmines, chemical weapons, nuclear weapons, "killer" drones and so on. The UN, the International Committee of the Red Cross (ICRC) and many humanitarian organisations carry out such activities targeting states, schoolchildren, university students, the public, the mass media and Armed Non-State Actors (ANSAs).

Immediate persuasion seeks to convince identified (potential) combatants in mission areas to refrain from or to cease use of force. The UN, the ICRC and Non-Governmental Actors (NGOs) operating in conflict zones do this by engaging directly with actors that threaten to or undermine deterrence, and by providing information about ongoing conflicts to other actors with a capacity to influence them: local community leaders, the media, other organisations and states. These organisations have developed handbooks and humanitarian negotiation tools to help their personnel create and preserve consent and cooperation from combatants at the tactical level.[23]

[20]Lupovici 2010; Nye 2016/17, pp. 60–63; Wilner 2011.

[21]Freedman 2013; Tannenwald 2007.

[22]Schirch 2006.

[23]ICRC 2015; Bessler 2006.

When general and immediate persuasion proves insufficient with respect to preventing and stopping military aggression, deterring actors can resort to *inducement*, which backs persuasion with positive inducements in the form of promises and rewards. The rewards can be non-tangible in the form of recognition and legitimacy and tangible in the form of resources and services or silence in the face of human suffering or violations of IHL.

With respect to recognition and legitimacy, the mere act of negotiation and cooperation with a peace force or an international mediator may serve as a positive incentive bestowing legitimacy on an armed group. ANSAs with political aspirations often use cooperation with international actors to demonstrate their legitimacy and ability to govern areas under their control.[24] The importance attributed to such legitimacy is not only visible in way that ANSAs use it strategically. It is also visible in the way governments fighting ANSAs attempt to deny them legitimacy by banning contacts between ANSAs and the UN and other international organisations, and by designating ANSAs as terrorists.[25]

The resources and services that peace forces and humanitarian organisations command constitute another important source of leverage that can be used as positive incentives in bargaining situations. Peace forces and humanitarian organisations bring food, water, medical services, and employment opportunities; they rent offices, housing and cars and help grow the local economy.[26]

A third positive incentive commanded by peace forces and humanitarian organisations is (a promise to maintain) silence in the face of humanitarian suffering or atrocities/war crimes. This is an asset that UN peace forces, ICRC and Médecins Sans Frontières (MSF) have used over the years in their dealings with governments and non-state actors to gain and preserve humanitarian access.[27] It has gained in importance as aggressors have come to fear public denouncements. For instance, al-Shabaab will only grant access to areas under its control to humanitarian organisations that promise not to speak out publicly against the group.[28] (Promise of) silence has clear and obvious limits as it may facilitate continued aggression in some circumstances. Nevertheless, it does provide leverage that can be used to influence aggressors (combatants, allies and supporters) fearing external intervention to take steps to reduce or stop the use of violence on the battlefield.

When peace forces and humanitarian organisations break their silence and name and shame identified aggressors, they cross the threshold from inducement to *coercion*. This mechanism relies on threats and punishments short of full-scale force in order to influence actors to refrain from or stop using force. It consequently incorporates both deterrence and compellence, in addition to the use of military threats and limited force that dominates the rational deterrence debate in the peace

[24]Loeb 2013, p. 16.

[25]Grace 2015; Jackson 2012.

[26]Abild 2009, p. 14.

[27]Kellenberger 2004; Magone et al. 2011, pp. 6, 46, 92, 110, 120.

[28]Jackson and Aynte 2013, p. 10.

operation literature. Deterring actors have three additional coercive instruments at their disposal: naming and shaming, suspension/termination of peace operations and political and economic sanctions.

Naming and shaming become coercion when the identification of actors responsible for undermining deterrence is accompanied with calls for or threats of punitive action (political, economic and military) to stop them. Humanitarian organisations instruct their personnel to use naming and shaming actively to mobilize local populations, the media and international public opinion to pressure combatant allies, combatant supporters and bystanders to take punitive action to stop combatants using force.[29]

(Threats of) suspension or termination of humanitarian relief and peace operations are used frequently against combatants, but it has also been employed against bystanders using humanitarian assistance as an alibi for inaction to coerce them to act. In 1992, a threat to withdraw from Somalia made by a group of American NGOs helped to coerce the United States to launch a military intervention into Somalia (Operation Restore Hope) to create a secure environment for humanitarian operations.[30]

(Threats of) diplomatic and economic sanctions are frequently used in support of peace forces to deter aggression or more frequently to compel combatants, combatant allies and supporters to take action to stop attacks already occurring. Diplomatic sanctions involve restriction of diplomatic representation and interaction, suspension of organisational memberships, cultural and sport bans and the establishment of war crimes tribunals. Economic sanctions cover a wide array of instruments such as arms embargoes, asset freezes, commodity bans (for instance, charcoal, diamonds, oil and timber), financial restrictions and travel bans. The UN relied on both types of sanctions in its attempts to compel primarily the Former Republic of Yugoslavia/Serbia-Montenegro to end its material support for the Bosnian Serb forces during the war in Bosnia 1992–95 and deter escalation.[31] Since then, the use of UN sanctions has grown significantly,[32] in 2015 a major study found that 59% of UN sanctions were used together with peace forces to manage armed conflicts.[33]

All the mechanisms and means depicted in Table 17.3 contribute to deterrence in peace operations, and most of them are employed simultaneously from the local to the global levels by NGOs, peace forces, international organisations and states to influence the coalition of actors (combatants, combatant allies, combatant supporters and bystanders) that undermines deterrence in a specific conflict. Table 17.3 illustrates that the existing peace operation literature focussing on the requirements of military battlefield deterrence misses most of the picture and exaggerates the

[29]ICRC 2012; Slim and Bonwick 2005, p. 86.

[30]Lischer 2003, p. 102.

[31]Knudsen 2008.

[32]Giumelli 2015; Radtke and Jo 2018.

[33]Biersteker and Hudáková 2015, p. 7.

Table 17.3 Mechanisms and means for influencing actors undermining deterrence in peace operations

Persuasion: information, education and training	General: – IHL and human rights training, education and information campaigns – Campaigns aimed at banning weapons systems, stopping the proliferation of small and light arms, the use of child soldiers and so on Immediate: – Explaining combatant objectives are best achieved by means of negotiation and will be undermined by use of force – Informing combatants about their IHL obligations and humanitarian principles in order to gain access to civilians in need – Providing information about atrocities and violations to advocacy groups, journalists, governmental organisations and governments – Appeals to all actors undermining deterrence in a given conflict to take steps to stop the use of force
Inducement: promises and rewards	– Legitimacy derived from cooperating with internationally recognized organisations – Humanitarian assistance to civilians enabling governments and armed groups to divert resources to military capacities or gain support from the local population – Payment for accommodation, services and local staff benefiting the local economy and thereby governments and armed groups – Direct payment to combatants for protection and humanitarian access – (Promise of) silence concerning human suffering and violence in exchange for compliance
Coercion: threats and punishment	– (Threat to engage in) naming and shaming of all types of actors contributing to undermine deterrence in order to mobilize local, regional and global pressure on them to stop – (Threat to issue) calls for diplomatic, economic, or military measures against all types of actors contributing to deterrence failure at the local, regional and global levels – (Threat to) suspend or terminate humanitarian operations and peace negotiations – (Threat to) punish aggressors/deny them their objectives politically, economically and militarily – (Threat to) use force to enforce compliance with international demands at tactical or strategic levels

(*Source* The author)

contribution made by battlefield deterrence to overall success. The peace operations literature assumes wrongly that effective deterrence hinges on the deployment of a peace force capable of threatening and using force against the combatants in a way that will make aggression too costly. Yet many peace forces have contributed to successful deterrence without meeting these requirements, because their

deployment was supported by the use of persuasion, inducements and other forms of coercion such as threats or use of diplomatic and economic sanctions that made the costs of aggression too high for the combatants, their allies and supporters and the costs of inaction too high for the bystanders. The UN operation in Sierra Leone (UNAMSIL) illustrates the limits of battlefield deterrence and highlights the advantages of adopting the more comprehensive understanding of deterrence proposed in this chapter.

17.5 Reinterpreting UNAMSIL

UNAMSIL has been chosen because it constitutes a paradigmatic case for the robust peacekeeping school. Its proponents use it to argue that combat capable peace forces are a sine qua non for deterrence and mission success. While it is true that UNAMSIL's eventual success in part can be attributed to the deployment of combat capable forces and effective use of limited force, it is equally clear that it took far more than credible threats and use of force to turn the operation around (see Table 17.4).

UNAMSIL (1999–2005) had a chapter VII mandate authorizing the use of force beyond self-defence to protect civilians and implement a peace agreement between the government of Sierra Leone and the rebel movement Revolutionary United Front (RUF). The mission got off to a bad start when RUF reneged on its commitment to disarm and took over 500 UN soldiers hostage in May 2000. Fearing the collapse of UNAMSIL, UN Secretary-General (UNSG) Kofi Annan appealed to the three bystanders with the capacity to prevent it from happening: France, the United Kingdom (UK) and the United States. The UK responded positively to the appeal undertaking a hasty deployment of 700 paratroopers to evacuate Western citizens, stabilize the situation and prevent the collapse of the UN mission. The UK subsequently beefed up an existing Security Sector Reform (SSR) program enabling the Sierra Leonean army and police to take more effective action against RUF. The UK also took the lead with respect to mobilize support for UNAMSIL in the UN Security Council. It penned subsequent UN resolutions strengthening the UNAMSIL mandate and increasing the size of the force from 11,000 to 17,000 personnel. The United States supported the UK efforts and stepped up its military support for African countries providing troops for UNAMSIL. The UK also penned UN resolutions targeting the principal combatant allies and supporters that enabled RUF to continue its aggression. These resolutions imposed sanctions on Libya to deny it the ability to provide material support to RUF and named and shamed Burkina Faso into ceasing its assisting weapon sales to RUF. These actions were in part prompted by a global NGO advocacy campaign against blood diamonds, which pressured bystanders to take action to make it harder for RUF to finance its military campaign with the sale of diamonds. These efforts enjoyed strong regional support as the Economic Community of West African States (ECOWAS) led by Nigeria pressured RUF and Liberia to accept the Abuja Cease Fire Agreements I (2000) and

Table 17.4 Influencing the coalition of actors undermining deterrence in Sierra Leone 2000–2002

	Persuasion	Inducements	Coercion	Outcome
Combatants - Armed Forces Revolutionary Council (AFC) -Kamajors -Revolutionary United Front (RUF) - Sierra Leone's Army (SLA) - West Side Boys (WSB)	UK and UN media campaigns highlighting benefits of peace process and costs of resistance, - UNAMSIL outreach program - ECOWAS brokered Abuja Cease Fire Agreements I (2000) and II (2001) - Training of SLA military and the police force	- Amnesty for combatants - Cash payments and skills training for ex-combatants - Government release of RUF prisoners as reward for compliance (2001) - Rebel integration into national army - Increased pay for soldiers and police - Quick impact projects to win popular support - Truth and Reconciliation Commission (2002)	- UK use of force destroys WSB (2000) - UK over horizon force punishing non-compliance - UK supported SLA operations against RUF (2000) - Guinea defeat of RUF offensive (2001) - More assertive UNAMSIL (2001) - Economic sanctions imposed on RUF (2001) - UN War crimes tribunal (2002)	- Successful disarmament (2002) - Election result respected by combatants (2002)
Combatant allies - Liberia provided weapons and training to RUF and bought its diamonds			- NGO and UN reports naming and shaming Liberia for supporting RUF (2000, 2001) - UN arms embargo, ban on diamond exports travel ban imposed on Liberia (2001)	- Support for RUF significantly reduced
Combatant Supporters Burkina Faso helped RUF to sell diamonds and buy arms	- NGO advocacy campaign against blood diamonds		NGO, UK, US and UN naming and shaming Burkina Faso for assisting RUF (2001)	Burkina Faso ceased its support for RUF
Bystanders - United Kingdom - United States - France	UNSG Annan appeal to the three bystanders to intervene to prevent UNAMSIL collapse (2000) - NGO advocacy campaign against trade with blood diamonds from Sierra Leone		NGO advocacy campaign naming and shaming governments and firms facilitating trade with blood diamonds from Sierra Leone - Consumer boycotts against blood diamonds	- UK military intervention, and leadership in UNSC (2000–2002) - US support of UK - US training of African UNAMSIL contingents (2000)

(*Source* Berman and Labonte 2006; Rashid 2016; Ucko 2016)

II (2001). In addition, Guinea successfully defeated a 2001 RUF offensive weakening its military capacity considerably.

In sum, it took the efforts of a deterring coalition made up of a united Security Council led by the UK, a global NGO advocacy campaign against blood diamonds, strong regional diplomatic and military support, strengthened government security forces, active military support from the UK and a reorganized and strengthened UNAMSIL peace force to produce the disarmament of RUF and the national election that ended the civil war in Sierra Leone in 2002. As is clear from Table 17.4, the deterring actors relied on a combination of diplomacy, inducement and coercion to achieve this result. The significant strengthening of the UN force in 2000–2001 may well have been a necessary condition for the successful outcome of the UNAMSIL operation. But it was by no means sufficient, and it would not have succeeded in the absence of the other factors supporting its efforts at the local, regional and global levels.

17.6 Conclusion

The peace operations literature regards the deployment of a peace force capable of threatening and using force to punish aggressors or deny them their objectives as the sine qua non to deter violence and protect civilians. It ignores that deterrence needs to be established and maintained at other levels as well, and it cannot explain why unarmed military observers and peacekeeping forces incapable of threatening and using force have often contributed to deterrence and mission success. This chapter has developed a new analytical framework that solves this puzzle. To be successful actors deploying peace forces must not only deter combatants from using force. They must also deter the allies and supporters that enable combatants to use force, and they must influence bystanders with a capacity to make a difference to take action against them. To succeed deterring actors cannot rely solely on threats and use of force. They must supplement their use of coercion with persuasion and inducement and devise and implement influence strategies that draw on all three components. At present theorists and practitioners ask the following question when contemplating the deployment of a peace operation: how much military capacity will it take to deter or compel the combatants from using force at the tactical or strategic level? Instead, they need to adopt a wider perspective and ask the following questions:

(1) Who are the principal combatants, how much military capability do they have, and how can they be influenced to refrain from using it by means of persuasion, inducement and coercion?
(2) Who are the principal combatant allies, how do they support the combatants and how can their support be stopped by means of persuasion, inducement and coercion?

(3) Who are the principal combatant supporters, how do they support the combatants and how can their support be stopped by means of persuasion, inducement and coercion?
(4) Who are the principal bystanders with a capacity to influence the combatants, their allies and supporters, and how can they be influenced to act by means of persuasion, inducement and coercion?

Deterring actors contemplating the deployment of peace forces to deter the use of force must ask and revisit these four questions repeatedly as the peace operation evolves. The coalition of actors undermining deterrence may change in the course of the operation, and so will the (lack of) opportunities to influence each of its members. The answers provided to these questions are crucial for devising effective influence strategies. An influence strategy must be tailored to each actor contributing to undermine deterrence, and each strategy should combine persuasion, inducement and coercion for maximum impact.

References

Abild E (2009) Creating humanitarian space: a case study of Somalia. UNHCR Research Paper 184.
Berdal M (2019) What Are the Limits to the Use of Force in UN Peacekeeping? In: De Coning C, Peter M (eds) United Nations Peace Operations in a Changing Global Order. Palgrave Macmillan, Cham, 113–132. https://link.springer.com/content/pdf/10.1007%2F978-3-319-99106-1_6.pdf. Accessed 3 August 2020
Berman E G, Labonte M T (2006) Sierra Leone. In: Durch W J (ed) Twenty-First-Century Peace Operations. United States Institute of Peace, Washington DC, 141–227
Biersteker T, Hudáková Z (2015) UN sanctions and peace negotiations: possibilities for complementarity. Oslo Forum Papers 4
Cruz C A S, Philips W R, Cusimano S (2017) Improving Security of United Nations Peacekeepers. United Nations, New York
Findlay T (2003) The use of force in UN peace operations. Oxford University Press, Oxford
Freedman L (2013) Disarmament and Other Nuclear Norms. Washington Quarterly 36.2:92–108
George A L (2003) The Need for Influence Theory and Actor-Specific Behavioral Models of Adversaries. Comparative Strategy 22.5:463–487, https://doi.org/10.1080/01495930390256527 Accessed 3 August 2020
George A L, Smoke R (1974) Deterrence in American Foreign Policy. Columbia University Press, New York
Giumelli F (2015) Understanding United Nations targeted sanctions: an empirical analysis. International Affairs 91.6:1351–1368
Grace R (2015) Frontline Negotiations with Non-State Armed Groups. Harvard Humanitarian Initiative's Advanced Training Program on Humanitarian Action, Harvard
Howard L M (2019) Power in Peacekeeping. Cambridge University Press, Cambridge
Humanitarian Negotiations Information Portal, http://www.humanitariannegotiations.org/resource-database/. Accessed 3 August 2020
ICRC (2012) Enhancing protection https://www.icrc.org/eng/assets/files/other/icrc-002-0956.pdf Accessed 3 August 2020
ICRC (2015) Safer Access for all National Societies Increasing acceptance, security and access to people and communities in need http://saferaccess.icrc.org/. Accessed 15 January 2020

Jackson A (2012) Talking to the Other Side: Humanitarian Engagement with Armed Non-State Actors. HPG Policy Brief 47
Jackson A, Aynte A (2013) Talking to the other side: Humanitarian negotiations with Al-Shabaab in Somalia. HPG Working Paper December
Jakobsen P V (1998) Western Use of Coercive Diplomacy: A Challenge for Theory and Practice. Palgrave Macmillan/Houndmills, Basingstoke, Hampshire
Jakobsen P V (2000a) The Emerging Consensus on Grey Area Peace Operations Doctrine: Will It Last and Enhance Operational Effectiveness? International Peacekeeping 7.3:36–56 https://doi.org/10.1080/13533310008413848. Accessed 3 August 2020
Jakobsen P V (2000b) Reinterpreting western use of coercion in Bosnia-Herzegovina: Assurances and carrots were crucial. Journal of Strategic Studies 23.2:1-22. https://doi.org/10.1080/01402390008437788. Accessed 3 August 2020
James A (1990) Peacekeeping in International Politics. St. Martin's Press, New York
Jervis R (1979) Deterrence Theory Revisited. World Politics 31.2:289–324. https://doi.org/10.2307/2009945. Accessed 3 August 2020
Karlsrud J (2015) The UN at war: examining the consequences of peace enforcement mandates for the UN peacekeeping operations in the CAR, the DRC and Mali. Third World Quarterly 36.1:40-54. https://doi.org/10.1080/01436597.2015.976016. Accessed 3 August 2020
Kellenberger J (2004) Speaking Out or Remaining Silent in Humanitarian Work. International Review of the Red Cross 86.855:593–609
Knopf J W (2010) The Fourth Wave in Deterrence Research. Contemporary Security Policy 31.1:1–33. https://doi.org/10.1080/13523261003640819. Accessed 3 August 2020
Knudsen R A (2008) The Comprehensive UN Sanctions against the Federal Republic of Yugoslavia – Aims, Impact and Legacy. Kolofon Forlag, Oslo
Lischer S K (2003) Collateral Damage: Humanitarian Assistance as a Cause of Conflict. International Security 28.1:79-109. https://doi.org/10.1162/016228803322427983. Accessed 3 August 2020
Loeb J (2013) Talking to the other side Humanitarian engagement with armed non-state actors in Darfur, Sudan, 2003–2012. HPG Working Paper August
Lupovici A (2010) The Emerging Fourth Wave of Deterrence Theory—Toward a New Research Agenda. International Studies Quarterly 54.3:705-732. https://doi.org/10.1111/j.1468-2478.2010.00606.x. Accessed 3 August 2020
Lynch C (2014a) Now We Will Kill You. Foreign Policy 8 April 2014. https://foreignpolicy.com/2014/04/08/now-we-will-kill-you/. Accessed 3 August 2020
Lynch C (2014b) A Mission That Was Set Up to Fail. Foreign Policy 8 April 2014. https://foreignpolicy.com/2014/04/08/a-mission-that-was-set-up-to-fail/. Accessed 3 August 2020
Magone C, Neuman N, Weissman F (2011) Humanitarian Negotiations Revealed. The MSF Experience. Hurst & Company, London
McHugh G, Bessler M (2006) Humanitarian Negotiations with Armed Groups A Manual for Practitioners. United Nations, Ocha
Nsia-Pepra K (2017) Moral Obligation: Un Missions Should Not Abandon Vulnerable Civilians In Critical Times 25 August 2017. https://peaceoperationsreview.org/thematic-essays/moral-obligation-un-missions-should-not-abandon-vulnerable-civilians-in-critical-times/. Accessed 3 August 2020
Nye Jr S (2016/17) Deterrence and Dissuasion in Cyberspace. International Security 41.3:44–71. https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00266. Accessed 3 August 2020
Radtke M, Jo H (2018) Fighting the Hydra: United Nations sanctions and rebel groups. Journal of Peace Research 55.6:759–773
Rashid I (2016) Sierra Leone: The Revolutionary United Front. In: Hughes M, Miklaucic M (eds) Impunity: Countering Illicit Power in War and Transition. National Defense University, Washington DC, 190–216
Schirch L (2006) Civilian Peacekeeping. Life & Peace Institute, Östervåla
Shinn D H (2009) China and the Conflict in Darfur. The Brown Journal of World Affairs 16.1:85-100. https://www.jstor.org/stable/24590742. Accessed 3 August 2020

Slim H, Bonwick A (2005) Protection: An ALNAP Guide for Humanitarian Agencies. Overseas Development Institute, London

Snyder G H (1961) Deterrence and Defense: Toward a Theory of National Security. Princeton University Press, Princeton

Stein J G (1991) Deterrence and reassurance. In: Tetlock P E, Husbands J L, Jervis R, Stern P C, Tilly C (eds) Behaviour, society and nuclear war. Oxford University Press, New York, 9–72

Tannenwald N (2007) The Nuclear Taboo: The United States and the Non-Use of Nuclear Weapons since 1945. Cambridge University Press, Cambridge

Ucko D H (2016) Can Limited Intervention Work? Lessons from Britain's Success Story in Sierra Leone. Journal of Strategic Studies 39.5-6:847-877. https://doi.org/10.1080/01402390.2015.1110695. Accessed 3 August 2020

United States Department of Defense (2006) Deterrence Operations Joint Operating Concept. United States Department of Defense, Washington. https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joc_deterrence.pdf?ver=2017-12-28-162015-337. Accessed 3 August 2020

Wilner A (2011) Deterring the Undeterrable: Coercion, Denial, and Delegitimization in Counterterrorism. Journal of Strategic Studies 34.1:3-37. http://dx.doi.org/10.1080/01402390.2011.541760. Accessed 3 August 2020

Peter Viggo Jakobsen (Ph.D.) is Associate Professor at the Institute for Strategy at the Royal Danish Defence College, and Professor (part time) at the Center for War Studies, University of Southern Denmark. He has written extensively on coercion, coercive diplomacy, deterrence, peace operations and the use of force.

Part IV
New Instruments and Domains of Deterrence

Chapter 18
Targeted Sanctions and Deterrence in the Twenty-first Century

Francesco Giumelli

Contents

Abstract The use of sanctions is often associated with coercion and deterrence. The former implies that sanctions contribute to changing the behaviour of targets, while the latter suggests that the damage threatened by sanctions should discourage actors from embarking on certain policies. However, sanctions have evolved substantially over the last twenty years, thus this chapter discusses whether the emergence of targeted sanctions was enough to change the classical deterrence/sanctions relation. This chapter argues that while there are similarities with the past, there are elements of change that need to be carefully considered. On the one hand the imposition of a cost to certain policy actions, the existence of an audience and the potential impact on the wider society remain central problems for both comprehensive and targeted sanctions. On the other hand, targeted sanctions present unique features that directly interact with the concept of deterrence. First, sanctions do not target states and governments only, but also individuals and non-state actors. Second, targeted sanctions are designed to reduce their impact not only on innocent civilians, but there are clear boundaries of damage that can be inflicted on targets. Third, targeted sanctions can have a moral hazard problem, so that their imposition

F. Giumelli (✉)
University of Groningen, Groningen, The Netherlands
e-mail: f.giumelli@rug.nl

F. Osinga and T. Sweijs (eds.), *NL ARMS Netherlands Annual Review of Military Studies 2020*, NL ARMS, https://doi.org/10.1007/978-94-6265-419-8_18

creates an incentive for actors to embark on the very actions that sanctions aim to deter.

Keywords comprehensive sanctions · humanitarian suffering · targeted sanctions · travel restrictions · assets freeze · human rights · moral hazard

18.1 Introduction

Sanctions as an instrument of coercive diplomacy has been analysed and investigated through the lens of compellence, namely with the aim of altering the course of action of a state, or deterrence.[1] In this latter case, sanctions increase the cost of certain policy actions that states would decide not to pursue because the costs would outweigh the benefits. The connection between sanctions and deterrence holds also across 'waves', since sanctions were either threatened by President Wilson in the 1920s as a 'deadly and silent remedy' to avoid future wars or widely used during the Cold War for lower level threats than nuclear annihilation.[2] The fourth wave of deterrence, however, highlighted the emergence of asymmetric threats in the international system which was posed by international terrorist groups. The emergence of this phenomenon, especially with the 09/11 attacks, has created the conditions for the evolution of sanctions from targeting states to targeting individuals and non-state groups.[3] The impact of such an innovation, which is only partly represented by sanctions on terrorist groups, on how sanctions and deterrence can be interlinked when targets are not states has not been yet fully explored in the academic debate. This chapter aims to address this gap.

This chapter investigates how sanctions and deterrence interact in the twenty-first century. More specifically, the chapter explores the implications for deterrence of the emergence of targeted sanctions with a view to answer the question of the volume of the need (or the lack of it) of a broader debate to constitute the fifth wave of deterrence studies. While this final assessment is for the reader, this chapter argues that targeted sanctions share elements of continuity with their comprehensive predecessors, but they also present new and unique features that provide further nuances to the concept of deterrence. There are at least three arguments that corroborate this thesis. First, targeted sanctions aim also at individuals, and individuals behave according to different logics compared to complex organizations such as states. Second, while the classical deterrence was based on the promise of serious damage to be inflicted, targeted sanctions are designed not to inflict lethal pain on their targets. Finally, deterrence originates from the avoidance of nuclear confrontations, wide military conflicts and terrorist attacks, but sanctions

[1] Doxey 1971, 1972; Morgan 2012.

[2] Foley 1923.

[3] Cortright and Lopez 2002.

today are used for a very long list of objectives, which fundamentally alter the premises of the instrument. This chapter has both theoretical and practical implications. The theoretical implications are clearly linked with the overall attempt done in this volume to enhance the understanding of sanctions at the onset of the twenty-first century. The practical implications are directed at both the potential enhancement that would qualify new sanctions cases and at providing useful information to base future decisions on. This analysis is supported by empirical research done on cases of sanctions imposed by the United Nations (UN) and the European Union (EU), but the cases are only demonstrative of the nature of the problem and the principles should be applicable to all cases of sanctions.

The chapter is divided into four sections. First, in Sect. 18.2, the evolution of sanctions from comprehensive to targeted will be presented. Second, in Sect. 18.3, the chapter introduces at length targeted sanctions and its potential implications for deterrence. Third, in Sect. 18.4, this discussion follows an analytical contribution which attempts to highlight continuity and change in the interaction between sanctions and deterrence. Finally, the conclusion summarizes the main argument of the chapter and indicates future lines of investigation.

18.2 The Nexus Between Sanctions and Deterrence

Sanctions are foreign policy instruments that are naturally linked to deterrence. For instance, Galtung in his pioneering article on Rhodesia suggests that sanctions can either punish the receiver or to make it comply with some sort of request.[4] In both cases, sanctions are supposed to inflict a pain on the receiver, and the (naïve) logic goes that such economic pain would translate into political gain. The infliction of pain as punishment is understood through the deterrence prism in two ways. First, the imposition of sanctions aims to deter the repetition of certain behaviours, such as the escalation of a conflict. Second, sanctioning a receiver shapes the expectations of other actors (or potential targets in the future) of the implications of certain activities. In both cases, targets would refrain from engaging further in behaviours undesired by senders in order to avoid the negative consequences that would be caused by sanctions.

International sanctions are seen in the literature as predominantly an instrument of foreign policy.[5] The first example in history is normally the Megarian decree issued by Athens as described by Thucydides in his recount of the Peloponnesian wars. The sanctions consisted of a complete trade embargo between the cities of the Delian league and the city of Megara. The same principles applied during the Medieval era when castles and cities were besieged by armies battling for

[4]Galtung 1967, p. 376.

[5]Doxey 1971; Wallensteen and Staibano 2005; Hufbauer et al. 2007.

supremacy.[6] Accordingly, the economic impact imposed on the population would be avoided if the rulers decided to open the gates and concede to the (sometimes various) requests of the besiegers.

The practice to limit trade for political objectives continued even when states became the main actors of the international system since the Treaty of Westphalia in 1648. Once again, sanctions would be set up with a coercive objective, namely the one to change the course of a behaviour that has already altered,[7] as done by the United States on France and the Great Britain to "to induce Great Britain and France to abandon their policies of seizing neutral American ships".[8] However, sanctions also started to be seen explicitly as a way to shape future expectations, and therefore behaviours, of states. During the negotiations in the aftermath of the Great War, President Wilson talked about sanctions as a "silent and deadly remedy" to avoid future wars.[9] In essence, Wilson imagined that the threat of sanctions in the form of a total embargo was to be imposed on deviant states to dissuade, and thus deter, belligerent behaviours from any state. In other words, the collective security mechanism of sanctions in the League of Nations was a precursor for deterrence strategies in the nuclear era.

The advent of nuclear technology dwarfed the premises of sanctions-based deterrence, especially after the failed attempt to prevent the colonial expansion of Italy in Abyssinia in 1936.[10] Sanctions played a role in the Cold War, as demonstrated by the level of attention devoted to the subject by scholarly literature,[11] but they were linked to deterrence for undesirable behaviours at a lower level of threat compared to what was at stake for nuclear deterrence. In a key study on sanctions published in 1990, the list of case studies suggest that sanctions have been very frequently used to support democratic practices, to address the Apartheid, to destabilize governments among many others.[12] Resorting to sanctions against specific practices is the basic logic of deterrence, so that precisely because certain practices become more 'expensive', then states would be deterred not to embark on certain behaviours. However, interestingly enough, sanctions understood as foreign policy instruments have been normally applied by states against other states (or by similar political actors before the Treaty of Westphalia, such as cities, empires and the like), but things ought to change.

[6]Gravett 2007.

[7]Giumelli 2011.

[8]Frankel 1982, p. 291.

[9]Foley 1923.

[10]Strang 2013.

[11]Galtung 1967; Doxey 1971; Baldwin 1985.

[12]Hufbauer et al. 1990; For a sample of cases, see the website of the Peterson Institute for International Economics, available here: https://www.piie.com/summary-economic-sanctions-episodes-1914-2006.

18.3 The Evolution of Sanctions

In the early 1990s, sanctions looked like the measures imposed by Athens on Megara in 432 B.C.[13] When Iraq decided to occupy Kuwait in 1990, the UN decided to impose a comprehensive embargo on Iraq. This sanctions regime has been accused for decades for the killing of 500,000 Iraqi children.[14] While this assessment has been questioned, the fact that the comprehensive embargo on Iraq had humanitarian implications is without doubts.[15] The same principles were applied to other crises in the early 1990s, such as the Federal Republic of Yugoslavia, Haiti and Rwanda.[16] In these three cases, sanctions were imposed, at least, on wide economic sectors so that the humanitarian consequences became of the primary concerns of the international community.

In addition to it, sanctions were counterproductive as the real targets managed to either avoid the impact of sanctions or, occasionally, be strengthened by it. Evidence to support this thesis can be found for the four mentioned-above cases. For instance, Serbia benefited from the arms embargo as they were the only ones with weapons in the Yugoslav conflicts as well as Saddam Hussein managed to redirect the economic costs away from him and, instead, entirely on its internal opposition. In the case of Rwanda and Haiti, sanctions were not deemed to be the decisive factor in stopping the genocide or convincing the military junta to leave the country. Sanctions were not only ineffective, but they were also responsible for humanitarian consequences and, occasionally, for strengthening the targets that were supposed to be 'coerced'.

The watershed regarding the debate was the notorious assessment published by Lancet that blamed UN sanctions for the death of 500,000 children in Iran.[17] This evidence triggered an academic-led debate with practitioners on the reform of sanctions in order to make them 'smart'.[18] Three international processes—Bonn-Berlin, Interlaken and Stockholm—were organized to discuss ways in which sanctions could be designed to maximize their impact on the responsible individuals for certain policies that needed to be changed, while limiting the unnecessary humanitarian impact on innocent bystanders.[19]

This evolution of sanctions practice was also made possible by the emergence of the international individual responsibility principle in global politics.[20] According to a state-based society, the only legitimate actors of the international system are states. This is clear when reading, for instance, the UN Charter, which allows states

[13]Tsebelis 1990.

[14]Ali and Iqbal 1999.

[15]Alnasrawi 2001; Hoskin 1997.

[16]Cortright and Lopez 1995.

[17]Smith et al. 1995; Ali and Iqbal 1999.

[18]Cortright and Lopez 2002; Brzoska 2003; Cortright et al. 2002.

[19]Biersteker et al. 2005.

[20]Sunga 1992; van Sliedregt 2012.

to participate, vote and discuss in the Security Council and the General Assembly. However, the end of the Cold war saw the proliferation of international tribunals tasked with the responsibility to adjudicate individual responsibilities in domestic conflicts, such as the ones in the former Yugoslavia and Rwanda.[21] The proceedings of these Tribunals/Courts took place during the discussion to set up an International Criminal Court (ICC), which became operational in 2002 thanks to the Rome Statute signed in 1998,[22] which established that individuals, and not only states, could become the target of international organizations under certain conditions. This is why sanctions became 'targeted' at individuals and non-state groups beyond states.

18.4 What Are Targeted Sanctions?

Targeted sanctions are restriction of freedoms for individuals and non-state entities.[23] While they can be directed also at certain sectors of the economy, this is not necessarily a novel factor that has been a practice also during the Cold War, such as the example of sanctions on South Africa for the Apartheid demonstrates.[24] Targeted sanctions can be shaped in several ways, some of them being simply the individualization of restrictions reserved in the past to states only. Conventionally, sanctions can take the form of arms embargoes, trade restrictions, travel bans, asset freeze and financial restrictions.[25]

Arms embargoes are the quintessential form of sanctions used to target states and it has been used to limit access to weapons for individuals and groups such as political parties and rebel groups. Under such regimes, individuals and/or their associates as well as associates linked to certain groups cannot purchase weapons and military equipment.[26] Similar restrictions have been applied to the so called 'dual-use goods', namely items that can be used with both civilian and military purposes.[27] This applies, for instance, to satellite and telecommunication technologies or to metal alloys that could be used in nuclear programs.

Weapons are a special subcategory of trade sanctions and targeted sanctions also limit access to non-military items for individuals and groups. The *ratio* for such a measure is to either undermine the economic position or to constrain the capacity to operate for individuals and groups. For instance, the economic position of individuals and groups is affected by the ban on luxury items imposed on the

[21]Schabas 2006.

[22]Lee 1999.

[23]Cortright et al. 2002; Cortright and Lopez 2002.

[24]Crawford and Klotz 1999.

[25]Biersteker et al. 2016.

[26]Brzoska and Lopez 2009.

[27]Tamada and Achilleas 2017.

Democratic People's Republic of Korea (DPRK) and the ban on certain activities that were directly linked to the economic position of the Revolutionary Guard in Iran. Once again, these sanctions are to be added to the list of potentially very invasive sanctions, such as EU sanctions on the Iranian export of oil or the UN ban on diamonds from Liberia and Sierra Leone.

Other measures gained the lion's share of individual sanctions, namely travel bans and freeze of assets. By definition, the ban from traveling and the freezing of assets are measures that directly affect individual freedoms. These restrictions can be either based on a function that is being performed, such as restrictions insofar as an individual is serving in Government, or because of actions, such as the violation of human rights. These types of sanctions have been imposed several times since the UN inaugurated the era of targeted sanctions with Al Qaeda/Taliban in 1999 and, especially, after the attacks on 09/11 when hundreds of names were added to the list of the 1267 Committee and were subjected to a travel ban and a freeze of assets.[28] Often a freeze of assets is also intended as a financial restriction because payments from and to individuals subjected to freeze of assets are also forbidden. However, financial restrictions regard more than payments, but can also regard the purchase of bonds and the provision of insurance services, such as in the case of Russia and Iran.

Quite unexpectedly, practitioners were caught by surprise when domestic and international courts started to review cases of allegedly human rights violations in cases of individual listings. The Kadi case, which was an historical decision that brought the Court of Justice of the European Union on the verge of reviewing the decisions of the Security Council,[29] was a wake-up call to all as targeted sanctions posed severe legal challenges to this emerging practice of sanctions. For instance, while a state's access to international markets could be restricted as per Chapter VII of the UN Charter, individuals' restriction of freedom is subjected to different standards and requirements so that basic principles of due process and effective remedy should apply.[30] Additionally, humanitarian exemptions and exceptions needed to be considered as while the responsibility chain for states subjected to sanctions can be up for discussion, the responsibility for an individual in need of medical care that has no access to his personal funds to cover for his/her treatment due to sanctions is clearly falling on the shoulders of the senders of sanctions.[31]

Overall, targeted sanctions present overlaps with former sanctions practices when the only possible and direct targets were states. However, legal challenges as well as impact perception from targeting individuals clearly sets a difference between the 'classic' way of understanding sanctions and the more recent 'targeted' form. In other words, if changes are affecting the functioning of sanctions in

[28]Biersteker et al. 2016.

[29]Eckes 2008.

[30]Biersteker and Eckert 2006.

[31]Graf Sponeck 2002.

general, this chapter explores whether a difference could emerge also by exploring the deterrence/sanctions nexus. The next section addresses this question.

18.5 Deterrence and Targeted Sanctions: Changes and Continuity

The evolution of sanctions from comprehensive to targeted poses challenges to the conventional understanding of the sanctions/deterrence nexus. Certainly, there are elements of continuity in how sanctions relate to deterrence, but there are at least three fundamental changes. First, targets are also individuals and their costs/benefits calculations differ from the ones of states upon which the conventional deterrence theory is also based. Second, while deterrence works (or can work) because certain actors could face a heavy sanction (i.e. nuclear annihilation), targeted sanctions are designed to cause limited damages. Finally, targeted sanctions have a moral hazard problem. The three premises, which will be elaborated below, give way to three theoretical considerations that will follow.

Certainly, targeted sanctions are aiming at individuals and entities, but they are still sanctions that are used in case of undesirable behaviours. This means that there are inevitable similarities with how sanctions contribute to deterrence. First and foremost, sanctions intend to add a cost to certain actions. Whether states or individuals, the ultimate objective of sanctions is to alter the cost/benefit calculations of targets so they would be deterred to embark on certain policies. This occurs regularly for practices that are, more or less, becoming consistent across time and space. For instance, the US, the EU and the UN all target human rights violations with the imposition of sanctions, the cases of Iran, Belarus and Venezuela are only a few in a long list of crises that were subjected to human rights sanctions in the last years. This applies also to conflicts. For instance, the government of South Sudan expressed concerns in several occasions for the threat to be the target of an arms embargo imposed by the United Nations, therefore the decisions of President Kiir were naturally influenced by this possibility.

Second, the very act of imposing sanctions should not only deter the direct targets, but it should also prevent future repetition of similar behaviours by other targets. In other words, sanctions events between targets and senders are observed by an audience of potential targets in the future. This applies to the various crises under which sanctions have been used, whether it is about human rights violations or non-proliferation policies. For instance, any state interested in developing a nuclear program would not be indifferent to the experiences of Iran and North Korea. Similarly, actors assess the opportunity to trigger or cause a conflict also by factoring in the possibility to receive sanctions, therefore conflicts might be prevented precisely to avoid the negative consequences of sanctions.

Finally, also targeted sanctions can have a rather broad impact on societies to similar extent than comprehensive ones. Indeed, if targeted sanctions are applied

either on multiple economic sectors, such as the case of North Korea, or on crucial ones, such as the case of oil for Iran, it is inevitable that the impact of sanctions can be felt across the targeted society. This phenomenon is only amplified by the fact that targeted sanctions are mainly implemented by firms and companies through de-risking decisions.[32] For instance, sanctions on Syria do not cover most trade, but the complexity of the situation on the grounds does not allow companies to engage in export/import activities without serious risks and, therefore, they 'de-risk' and decide to abandon any commercial operation with the country.[33]

These similarities notwithstanding, there are at least three aspects of targeted sanctions that challenge the classical deterrence/sanctions nexus. First, targeting states is not the same thing than targeting individuals or entities. In statistics, generating inferences on individuals from groups is a formal mistake known as *ecological fallacy*. In political science, complex organizations are often the combination of individual's preferences, therefore the way in which a complex organization (or an institution) behaves can be radically different from the individual preference of each of its members. For instance, individuals have a time span that can differ from the one of institutions. Any citizen of a country would behave thinking that their state will last longer than each of them. Additionally, the well-being of individuals is not always linked with the wellbeing of a nation. This means that individuals would not respond to economic pain in the same way that deterrence theory expects states to do. In occasions as identified also above, sanctions worked in favour of the very individuals that were supposed to be targeted, while affecting severely the wider society as in the case of Iraq in the 1990s.

Second, while the essence of comprehensive sanctions was to inflict a damage to targets so others would not behave alike, targeted sanctions are designed to reduce their impact to the minimum. This is not to say that sanctions are, therefore, toothless, but this certainly sets a difference with the classical approach to deterrence. Firstly, states do not have human rights, while individuals do. This means that targeted sanctions are structurally limited in their impact on individuals. For instance, the listing of individuals has been compared to criminal proceedings, therefore evidence need to be presented, 'indicted' individuals need to be heard, and there should be procedures to rectify mistakes made by listing authorities. In other words, individuals have rights that cannot be easily waived, which limit the impact of deterrence as understood "in a classical" sense. Rather, principles from criminal deterrence could apply as elaborated below.

Additionally, targeted sanctions are designed to limit humanitarian consequences on direct and indirect targets. The rather narrow design is the acceptance of a reduced 'impact' of sanctions in general, but the combination with human rights concerns means that the impact cannot hamper the minimal wellbeing of targets. For instance, payments for medical expenses and basic needs are to be authorized by the competent authorities. This is also true for the negative consequences of the

[32]Bures 2015; Bures and Carrapico 2018.

[33]Daher and Moret 2020.

wider population as a number of exemptions and exceptions are normally included in a sanctions regime. These refer, for instance, to the provision of humanitarian aid and the purchase of equipment for international missions. Further details on this point would go beyond the scope of this chapter, but it should suffice to state that deterrence doctrine would be concerned partly with the wider impact, but less with the consequences for individuals directly targeted. This holds true also for the fourth wave of deterrence literature.

Finally, targeted sanctions can increase the likelihood of the behaviours that they intend to discourage as they present a problem of moral hazard. Comprehensive sanctions were criticized because they would trigger the rally around the flag effect. Accordingly, the population under sanctions tends to side with its own government in order to withhold the pressure from an outsider force, as it happened in the case of Southern Rhodesia already in the 1960s.[34] Targeted sanctions were to avoid this unintended effect as the negative impact would not fall on the shoulders of the population, but if targeted sanctions are imposed (or can be imposed) in a conflictual situation, one party in conflict might have the incentive to provoke a conflict if it expects that targeted sanctions would be imposed on the other side. This argument was made to explain the breaking out of the Kosovo war. Since the international community had already expressed its preference against Serbia and Milosevic, parties in Kosovo engaged in provocative actions that, eventually, led to the conflict with the international intervention.[35] Targeted sanctions can have the same impact and, as such, they can have the opposite effect of what claimed by a potentially generalizable deterrence strategy.

These points lead to two broad considerations regarding the deterrence/sanctions nexus for a potential fifth wave in deterrence literature. First, deterrence at the international level is approximating the functioning of criminal deterrence in the domestic level.[36] The fourth debate focused on the asymmetric threat posed by international terrorism, so non-state actors acquired the status of international actors and, in a way, were treated as such. Therefore, they would suffer the consequences of their actions with the use of lethal violence against them, as demonstrated by the military response to the attacks on 09/11. At the same time, international terrorism would be worth global attention precisely because they would attempt the highest of the values, namely the security of states and their citizens. Instead, targeted sanctions have been used with an ever-growing list of crises, from international terrorism, to non-proliferation, conflict management, post-conflict reconstruction, but also asset recovery (the EU) and for combating organized crime and human trafficking (the US).

Second, the over-utilization of sanctions and their apparent light impact could undermine, rather than strengthen, an international criminal deterrence doctrine. For instance, nuclear deterrence was built on the fact that fact that nuclear weapons

[34]Galtung 1967.

[35]Kuperman 2008.

[36]Chalfin and McCrary 2017.

were used only once. The potentially destructive power of nuclear weapons was enough to make deterrence a viable approach to pursue. Instead, targeted sanctions have been growingly used and this could contribute to reduce their role in substantiating a deterrence strategy, or at least to consider deterrence a low-intensity doctrine. First, the practice of targeted sanctions show that they can be easily circumvented. There are numerous cases also in the European Union, where the capacity is certainly high, of companies being caught for violation of sanctions regimes.[37] Second, the evolution of sanctions at the micro-level has favoured the creation of countermeasures to further limit their impact. For instance, sanctions on Swift in 2012 have sparked a debate towards the creation of alternative platforms for international payments.[38] Second, the consolidation of crypto currencies has also provided further instruments to circumvent the impact of targeted sanctions. In general, the success of deterrence is fundamentally based on the consequences that actors will pay in case of certain behaviours. However, this sanctions inflation may have contributed to the establishment of a very different sanctions/deterrence nexus that would be easier understood as an instrument of criminal domestic politics rather than security/international politics.

18.6 Conclusions

The use of sanctions is often associated to coercion and deterrence. The former implies that sanctions contribute to change the behaviour of targets, while the latter suggests that the damage threatened by sanctions should discourage actors from embarking on certain policies. However, sanctions have evolved substantially in the last twenty years, thus this chapter discussed whether the emergence of targeted sanctions was enough to change the classical "deterrence/sanctions nexus". This chapter argued that while there are similarities with the past, there are elements of change that need to be carefully considered.

On the one hand, a sanction is a sanction, therefore the imposition of a cost to certain policy actions, the existence of an audience and the potential impact on the wider society remain central problems for both comprehensive and targeted sanctions. On the other hand, targeted sanctions present unique features that directly interact with the concept of deterrence. First, sanctions do not target states and governments only, but also individuals and non-state actors. Second, targeted sanctions are designed to reduce their impact not only on innocent civilians, but there are clear boundaries of damage that can be inflicted on targets. Third, targeted sanctions can have a moral hazard problem, so that their imposition creates an incentive for actors to embark on the very actions that sanctions aim to deter.

[37]Giumelli and Levi 2016.

[38]Majd 2018.

These features indicate that targeted sanctions are used in a global system targeting a wide range of behaviours and several actors involved at any levels of illicit activities. This system of deterrence is an evolution from the fourth wave as it does not only attempt to address a security related matter (i.e. terrorism), but it extends to a series of lower risk crises that would be better understood through a governance prism rather than a foreign policy one. As such, principles underlying criminal deterrence should be used to complement classical deterrence literature.

There are theoretical and practical implications from this viewpoint. From a theoretical angle, adding the individual level to the deterrence literature indicates the formation, or the understanding, of a different international system. As such, this study and approach should draw from the very wide debate that tries to understand the nature of the international system and international politics. While one of the main assumptions is to look at the world as divided in states, this analysis suggests that a multilevel governance approach might be more appropriate to make sense of the contemporary complexities of global politics. Second, the study of sanctions practices as well the analysis of the ways in which sanctions are evaded is a way to study different configuration of power structures and its uses in the international system. This directly contributes to understanding deterrence beyond material considerations strongly linked to costs and impacts of sanctions. Instead, sanctions and deterrence have (or should have) a common normative background that indicates what are the behaviours that should not be repeated. Indeed, the shift from foreign policy to governance in understanding sanctions presupposes that decision-making will be overtime less 'political' and more 'rule based'. The study of the rules upon which international criminal deterrence works is a worthwhile venue for future research.

At the same time, targeted sanctions can contribute to criminal deterrence, but also to deterrence in general, if they manage to have an impact on targets. Therefore, given targeted sanctions work at a micro level, the issue of institutional capacity is certainly to be taken more seriously than what has been done so far. First, the quality of listing targets is of essence, therefore deep knowledge of targets and targeted societies is crucial. A policy implication from this starting point is that public authorities making listing decisions ought to improve their knowledge base and their capacity to acquire new information when needed. Consequently, this becomes an issue of coordination with non-state actors that could have crucial information not in the hands of public authorities. This is already happening, for instance, with the regulation of the financial sector and the forced cooperation that banks and the like must guarantee to governments. Second, there is an issue of capacity building in the private sector. Since for-profit actors are becoming central allies in gathering information, it is of utmost importance that they are provided with the necessary information and expertise to fully comply with the spirit of the regulation. At the moment, the level of preparedness across countries and legal system is very uneven, which undermines the capacity for sanctions to credibly contribute to (criminal) deterrence. Finally, criminal sanctions reproduce a cat and mouse process, so targets and potentially targeted societies make preparations to be resilient in case of being targets of sanctions. While this is not new to deterrence

experts, the individual level of criminal deterrence requires a more attentive and capillary cooperation across different national and global institutions that is often undermined by political and strategic considerations. Although this cooperation is difficult, it is a necessary (yet insufficient) step to ensure that there could be a meaningful discussion regarding (criminal) deterrence in the twenty-first century.

References

Ali M M, Iqbal S H (1999) Sanctions and Childhood Mortality in Iraq. Lancet 27.355:1851-1857

Alnasrawi A (2001) Iraq: Economic Sanctions and Consequences, 1990–2000. Third World Quarterly 22.2:205–18

Baldwin D A (1985) Economic Statecraft. Princeton University Press, Princeton NJ

Biersteker T J, Eckert S (2006) Strengthening Targeted Sanctions Through Fair and Clear Procedures. Watson Institute for International Studies, Providence RI

Biersteker T J, Eckert S E, Halegua A, Romaniuk P (2005) Consensus from the Bottom Up? Assessing the Influence of the Sanctions Reform Process. In: Wallensteen P, Staibano C (eds) International Sanctions: Between War and Words in the International System. Routledge, London

Biersteker T J, Eckert S E, Tourinho M (2016) Understanding United Nations Targeted Sanctions. Cambridge University Press, Cambridge

Brzoska M (2003) From Dumb to Smart? Recent Reforms of UN Sanctions. Global Governance 9.4:519–35

Brzoska M, Lopez G A (2009) Putting Teeth in the Tiger: Improving the Effectiveness of Arms Embargoes. Emerald Group Publishing, Bingley UK

Bures O (2015) Political Corporate Social Responsibility: Including High Politics? Journal of Business Ethics 129:689–703

Bures O, Carrapico H (2018) Security Privatization. How Non-Security-Related Private Businesses Shape Security Governance. Springer, Cham Switzerland

Chalfin A, McCrary J (2017) Criminal Deterrence: A Review of the Literature. Journal of Economic Literature 55.1:5–48

Cortright D, Lopez G A (1995) Economic Sanctions: Panacea or Peacebuilding in a Post-Cold War World? Westview Press, Boulder CO

Cortright D, Lopez G A (2002) Smart Sanctions: Targeting Economic Statecraft. Rowman & Littlefield Publishers, Lanham MD

Cortright D, Lopez G A, Rogers E S (2002) Targeted Financial Sanctions: Smart Sanctions That Do Work. In: Cortright D, Lopez G A (eds) Smart Sanctions: Targeting Economic Statecraft. Rowman & Littlefield Publishers, Lanham MD, 23-40

Crawford N, Klotz A (1999) How Sanctions Work: Lessons from South Africa. St. Martin's Press, New York

Daher J, Moret E S (2020) Invisible Sanctions: How Over-Compliance Limits Humanitarian Work on Syria. Challenges of Fund Transfer for Non-Profit Organizations Working on Syria https://impact-csrd.org/reports/Invisible_Sanctions_IMPACT_EN.pdf Accessed: 14 May 2020

Doxey M P (1971) Economic Sanctions and International Enforcement. Oxford University Press, Oxford

Doxey M (1972) International Sanctions: A Framework for Analysis with Special Reference to the UN and Southern Africa. International Organization 26.3:527–50

Eckes C (2008) Judicial Review of European Anti-Terrorism Measures—The Yusuf and Kadi Judgments of the Court of First Instance. European Law Journal 14.1:74–92

Foley H (1923) Woodrow Wilson's Case for the League of Nations (edited). Princeton University Press/Oxford University Press, Princeton/London

Frankel J A (1982) The 1807-1809 Embargo Against Great Britain. Journal of Economic History 42.2:291–308
Galtung J (1967) On the Effects of International Economic Sanctions: With Examples from the Case of Rhodesia. World Politics 19.3:378–416
Giumelli F (2011) Coercing, Constraining and Signalling. Explaining UN and EU Sanctions after the Cold War. ECPR Press, Colchester
Giumelli F, Levi G (2016) Sanzioni: Alle Imprese Europee La Multa Arriva Dagli Usa. http://www.lavoce.info/archives/41389/sanzioni-alle-imprese-europee-la-multa-arriva-dagli-usa/ Accessed: 12 May 2020
Graf Sponeck H C (2002) Sanctions and Humanitarian Exemptions: A Practitioner's Commentary. European Journal of International Law 13.1:81–87
Gravett C (2007) The History of Castles, Fortifications around the World (revised and updated edn.). Rowman & Littlefield Publishing, Lanham MD
Hoskin E (1997) The Humanitarian Impacts of Economic Sanctions and War on Iraq. In: Weiss T G (ed) Political Gain and Civilian Pain: Humanitarian Impacts of Economic Sanctions. Rowman & Littlefield Publishers, Lanham MD/Oxford, 91-148
Hufbauer G C, Schott J J, Elliott K A (1990) Economic Sanctions Reconsidered. 2nd edn. Institute for International Economics, Washington DC
Hufbauer G C, Schott J J, Elliott K A, Oegg B (2007) Economic Sanctions Reconsidered. Peterson Institute for International Economics, Washington DC
Kuperman A J (2008) The Moral Hazard of Humanitarian Intervention: Lessons from the Balkans. International Studies Quarterly 521:49–80
Lee R S K (1999) The International Criminal Court: The Making of the Rome Statute : Issues, Negotiations, Results. Kluwer Law International, The Hague/London
Majd M (2018) The Cost of a SWIFT Kick: Estimating the Cost of Financial Sanctions on Iran. In: Epstein G A (ed) The Political Economy of International Finance in an Age of Inequality. Soft Currencies, Hard Landings. Edward Elgar Publishing, Cheltenham UK/Northampton MA, pp 175-193
Morgan P M (2012) The State of Deterrence in International Politics Today. Contemporary Security Policy 33.1:85–107
Schabas W (2006) The UN International Criminal Tribunals: The Former Yugoslavia, Rwanda and Sierra Leone. CUP, Cambridge
Smith F, Mary C, Zaidi S (1995) Health of Baghdad's Children. Lancet 346
Strang B G (2013) Collision of Empires: Italy's Invasion of Ethiopia and Its International Impact. Routledge, Abingdon/New York, NY
Sunga L S (1992) Individual Responsibility in International Law for Serious Human Rights Violations. Martinus Nijhoff, Dordrecht
Tamada D, Achilleas P (2017) Theory and Practice of Export Control. Balancing International Security and International Economic Relations. Springer, New York
Tsebelis G (1990) Are Sanctions Effective? A Game-Theoretic Analysis. Journal of Conflict Resolution 34.1:3–28
Van Sliedregt E (2012) Individual Criminal Responsibility in International Law. Oxford University Press, Oxford UK
Wallensteen P, Staibano C (2005) International Sanctions: Between Words and Wars in the Global System. Frank Cass, London/New York

Francesco Giumelli is Associate Professor in, and Deputy Head of the Department of International Relations and International Organization at the University of Groningen. A former Jean Monnet Fellow at the European University Institute (EUI), Fiesole, Italy, he has published widely on EU and UN sanctions.

Chapter 19
Deterrence, Resilience, and the Shooting Down of Flight MH17

Cees van Doorn and Theo Brinkel

Contents

Abstract Russian disinformation has thus far proven to be unconvincing for most Dutch target audiences. This is the conclusion of the present chapter. Information and disinformation have become effective weapons in international politics. This is part of a development where the weapons and concepts used in deterrence strategies have moved away from the military domain toward the political, economic, humanitarian, and communicative ones. In western literature, this is called hybrid warfare. In recent literature on hybrid warfare, resilience is often considered a key theme which may boost deterrence against hybrid activities and/or lower their impact. Most research on resilience and security is focused on infrastructure and resource planning. In this chapter, however, we attempt to ascertain how the existence of resilience in society can be observed. By looking at the case of the

C. van Doorn (✉) · T. Brinkel
Netherlands Defence Academy, Breda, The Netherlands
e-mail: cees@qvc.nl

T. Brinkel
e-mail: TBFM.Brinkel@mindef.nl

F. Osinga and T. Sweijs (eds.), *NL ARMS Netherlands Annual Review of Military Studies 2020*, NL ARMS, https://doi.org/10.1007/978-94-6265-419-8_19

Dutch reaction to the shooting down of flight MH17, we hope to illustrate how resilience works in deterrence to hybrid warfare. We try to establish how subversive Russian activities were taking place and what measures were taken by the Netherlands government in order to counteract them. We monitored societal resilience by looking for the presence of trust, social capital, and credible narratives in reaction to disinformation activities after a disruptive event. All these elements appeared to be present in the MH17 case. Overall, we conclude, the handling of the MH17 case has reinforced deterrence.

Keywords MH-17 · BUK · hybrid threats · resilience · social capital · trust · narrative

19.1 Introduction

On 17 July 2014, a Russian Buk missile shot down Malaysia Airlines flight 17 (MH17) during its flight from Amsterdam to Kuala Lumpur. The disaster occurred near an Eastern Ukrainian village called Hrabove. The crash site was situated in a conflict zone where pro-Russian separatists, including the Donbass People's Militia, were fighting regular Ukrainian troops. As a result of the crash, 298 passengers lost their lives. The victims originated from 10 different countries; most of them were Dutch (193), Malaysian (43), and Australian (27). Shortly after the shooting down of MH17, various actors began spreading messages that were meant to convince the Dutch public of the Russian allegation that Ukraine was responsible for the massacre. While these actors were mainly Russians, Ukrainians and even some Dutch nationals were also involved.[1]

The nature and intensity of disinformation campaigns such as these have widely been recognized. Information has become an effective weapon in international politics. This is part of a development where the weapons and concepts used in deterrence strategies have moved away from the military domain toward the political, economic, humanitarian, and communicative ones. In Western literature, this is called hybrid warfare. It ranges from support for populist parties and disinformation campaigns to the utilization of organized crime and individuals sympathetic to Moscow, from intelligence operations to military pressure. The general purpose is to create a political and cultural environment that serves the interests of the Russian Federation and weakens the cohesiveness of NATO and the European Union.[2]

The question is how these subversive Russian activities were taking place and what measures were taken by Western, or—to be more specific—the Netherlands government in order to counteract them. In recent literature on hybrid warfare,

[1]Rietjens 2019.

[2]Galeotti 2017.

resilience is often considered a key theme which may boost deterrence against hybrid activities and/or lower their impact. By utilizing findings regarding flight MH17 from previous research by Cees van Doorn, we hope to illustrate how resilience works in a context of deterrence in hybrid warfare.[3] Most research on resilience and security is focused on infrastructure and resource planning. We attempt to ascertain how the existence of societal resilience can be observed and how the findings relate to deterrence. To do so, we conducted a literature review to define the concepts of deterrence and resilience, which resulted in an analytical framework that can be used to monitor resilience in the case of flight MH17. A group of respondents was selected who were—or still are—highly involved in the case of flight MH17. They were interviewed and their comments are used as illustrations of the way the disaster was dealt with.[4] The final course of action comprised an analysis of the publications of government research agencies and others.[5] Voluntary digital forensics organizations, such as Bellingcat and the EEAS, repudiate disinformation by investigating narratives, sources, and channels. Bellingcat runs an international program to educate and train its volunteer network of digital forensic investigators. Web-based digital developments have enabled voluntary digital forensics organizations, as well as other individuals, to investigate and publicly debunk disinformation.[6]

19.2 Hybrid Threats

Deterrence has been the West's classic answer to outside threats. During the Cold War era, a war in Europe would have been so destructive that all efforts were focused on preventing such a disaster, which has traditionally been achieved by deterring the opponent (i.e., the Soviet Union) from even considering an armed attack. The possession and thus potential use of a vast array of nuclear weapons was

[3]Van Doorn 2019.

[4]They are members of the Dutch government, the Dutch Public Prosecution Service (PPS), the Dutch Safety Board (DSB), the Dutch press and relatives of the victims.

[5]Van Doorn 2019; a significant research element of Van Doorn's master thesis consisted of a process tracing approach of disinformation activities to gain insight into the relationship between flight MH17–related events and debunked cases of disinformation. This information was ordered into a comprehensive timeline. Due to space limitations, we could not incorporate this timeline here, but it can be found here: https://www.linkedin.com/posts/ceesvandoorn_extensive-timeline-of-disinformation-in-the-activity-6668960213137154048-lzhN.

[6]This phenomenon can be seen in other cases as well, such as the war in Syria and the poisoning of Sergei and Julia Skripal in March 2018. An accessible digital collection was created for all those who have dispersed disinformation. The alleged meddling in the 2016 U.S. presidential elections has raised the awareness of disinformation and urged governments, including the Dutch, to act. The Dutch government has acted strategically (i.e., in policy documents) as well as practically, as in the case of an awareness campaign against fake news that the Ministry of the Interior launched in March 2019.

considered a crucial element in this situation of mutually assured destruction. After the fall of the communist system, this type of conceptualization of deterrence moved to the background. Following the attacks of 9/11, deterrence was discussed mainly in relation to terrorism. The question was whether deterrence would be possible vis-à-vis terrorists for whom death is simply an entry into paradise. Authors such as Wilner argue that terrorists can indeed be deterred, if their behaviour and motivations can be manipulated by coercive, diplomatic, and ideological measures.[7] This argument has gained relevance in the context of hybrid warfare as well.

After the Russian seizure of Crimea in 2014 and the emergence of hybrid warfare, deterrence gained renewed acumen.[8] Hybrid warfare has been defined by Cullen as "the synchronized use of multiple instruments of power related to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects".[9] The debate on hybrid warfare broadened from a predominantly military phenomenon to a strategy which includes the whole of society. In the latter sense, hybrid warfare allows for vertical escalation, whereby one type of instrument, such as the military, is intensified, or for horizontal escalation, which means that more instruments (economic, communicative) will be put to work apart from the one already utilized.

Hybrid warfare opens the possibility to use all instruments short of actual war. Information warfare, to be more specific: disinformation campaigns, are a crucial element in this type of measure. By creating events, spreading fake news, communicating alternative narratives, strategies such as these disinformation campaigns are aimed at the heart of Western societies and the morale of the population. They are a symptom of what Rupert Smith called "war amongst the people", where the loyalty of the population is at stake.[10] War amongst the people essentially points at the absence of a traditional battlefield where identifiable armies are supposed to do physical battle against each other. Today's war theatres are the streets, the households, the countryside, the Internet, the convictions and fears of the people.[11] The West must learn to contend with strategic communication, disinformation, cyber-attacks, the manipulation of social unrest, and the use of unmanned drones.[12]

Several examples of information warfare have been identified. Intellectuals and think-tanks, the Russian Orthodox Church, Russian media such as RT and Sputnik news agency are used to discuss pro-Russian narratives. According to Galeotti,

[7]Wilner 2011, pp. 4–5.

[8]MCDC Countering Hybrid Warfare Project 2019, p. 3.

[9]Cullen and Reichborn-Kjennerund 2017, p. 8; see also Davis 2015, p. 5.

[10]Strachan n.d., p. 52.

[11]Smith 2005, p. 6.

[12]Davis 2015, p. 21.

insurgents, terrorists, paramilitaries and criminal groups can all be deployed in Kremlin's cause.[13] Treverton et al. (2018) mention the targeting of the Democratic Campaign in 2015 and 2016 in the United States by cyber operations that were linked to Russian Intelligence in support of the presidential candidature of Donald Trump. Later, such groups turned to the Netherlands, Germany and France, all in support of anti-European Union parties and candidates.[14] In its latest annual report, the Dutch Central Intelligence and Security Service (AIVD) discusses covert political influencing that is more intrusive than normal diplomacy or political lobbying. According to the AIVD, Russia is the main originator and has a strong association with the shooting down of MH17. The impact in the Netherlands has thus far been limited.[15] The Dutch ministers of Security and Justice and Home Affairs have judged this type of interference as highly undesirable, because this way foreign state actors affect the foundations of the democratic legal order and the open society.[16]

A classic military offensive would mean that NATO member-states invoke Article Five of the Washington Treaty, whereby an attack against one is considered an attack against all. This invocation rests upon the feeling of mutual solidarity among the NATO-members. Information warfare, aimed at influencing the people and the political leaders of the member-states, can undermine this feeling. By information warfare, Moscow aims to foster dividedness among citizens and distrust towards their governments, the EU and NATO. Authoritarian populist movements in the West itself and politicians and parties as Alternative für Deutschland, Front National in France, Jobbik in Hungary and the UKIP in the United Kingdom, play into the hands of Russia.[17] To quote Rupert Smith: "The battlefields of today are the streets, the households, the countryside, the Internet, the convictions and fears of the people."[18] Hybrid strategies and information warfare place new demands on the concept of deterrence.

19.3 Deterrence and Resilience

According to NATO, deterrence is the capability to deter an opponent from taking aggressive action against members of the alliance.[19] In the classical view, this effect is achieved in two ways: deterrence by punishment, which means both the credible threat and the actual capability to retaliate after an enemy attack, and deterrence by

[13]Galeotti 2017, pp. 5–6.
[14]Treverton et al. 2018, pp. 9, 43, 52.
[15]AIVD 2020, p. 81.
[16]Brief ongewenste buitenlandse inmenging 2018, p. 1.
[17]Galeotti 2017, p. 6; Nicolini and Janda 2016, p. 82.
[18]Smith 2005, p. 6.
[19]Rühle 2015.

denial, which regards the capability to block the ambitions of the opponent where NATO members would be the victims. In both aspects, the word "capability" is essential, as capability embraces the means (e.g., military personnel and equipment, infrastructure, and economic capacities) and the political resolve to employ these means.[20]

With the emergence of the recent debate on hybrid strategies and information warfare, a third way was added to that of denial and punishment: deterrence by delegitimization. This concept is based on the idea that non-traditional opponents, such as terrorists, are politically motivated. Wilner argues that the chances of achieving their political targets diminish when the foundations of their political motivation—such as publicity, cohesion, or sympathy among the population—are delegitimized.[21] According to Knopf this approach involves challenging terrorists' justifications for violence, an approach that has been labelled deterrence by counter-narrative or deterrence by delegitimization.[22] According to an information note of the Countering Hybrid Warfare project of 14 Western countries and the EU, the same logic applies to actors who use hybrid warfare strategies.[23]

In this section, we will discuss the meaning of the concept of resilience first and then its relevance to deterrence in a context of hybrid strategies and information warfare. Resilience, according to Rodin, "is the capacity of any entity—an individual, a community, an organization, or a natural system—to prepare for disruptions, to recover from shocks and stresses, and to adapt and grow from a disruptive experience".[24] Resilience usually concerns technical solutions and infrastructure; nevertheless, according to Rodin, resilience can also be found in attitudes, declarations, and images and observed in public debate and common values and objectives. In that respect, resilience is part of the social capital and trust in society, as well as the narratives that guide it.[25]

The general relationship between resilience and security is broadly recognised. According to Fjäder, for instance, security and resilience are both part of the current security paradigm. Security is preventive and proactive, whereas resilience is a combination of proactive and reactive measures, not directed at one particular threat but at all kinds of human, technical or natural disasters. Security is connected to territory, whereas resilience is more connected with a complex system, institutions, or a value chain. Resilience can contribute to security. A resilient society and a strong defence work as a deterrent that help to prevent an attack or an assault.[26] But there are also more specific reasons why resilience enhances deterrence in the context of hybrid warfare.

---

[20]Daalder 2017, p. 38.

[21]Wilner 2011, pp. 26–27.

[22]Knopf n.d., p. 18.

[23]MCDC Countering Hybrid Warfare Project 2019, p. 3.

[24]Rodin 2014, p. 3.

[25]Rodin 2015, p. 63.

[26]Fjäder n.d., pp. 122–123.

First, because it is impossible to deter all elements of the complex and diverse scope of hybrid strategies. Total defence is not feasible. According to Coaffee and Wood, resilience is a social condition that is helpful in managing the way risks are dealt with.[27] A resilient society will undermine and deny inimical efforts in many of the domains in which they may occur.

Second, because deterrence in hybrid warfare amounts to a test of will, Giegerich argues, resilience must be enhanced.[28] Deterrence depends on our societies making the desired impression on the opponent through the strength of our defence posture and our political resolve. Galeotti conveyed it plainly: The Kremlin must be convinced that the costs of political warfare are higher than potential gains.[29] Capabilities that impress the opponent, a track record of promises kept and consistency in policies all enhance deterrence, according to Gray. Furthermore, in his view, enemies play a role in that they will process the messages they receive and decide whether they will be deterred. They may recognize the strength of the defender's defence posture but simultaneously be unimpressed by its political resolve.[30] In a paper on the defence of the Nordic countries, Whiter indicates how they acknowledged the relevance of societal resilience. Finland, for instance, uses the term "psychological resilience", which is defined as "the ability of individuals, communities, society, and the nation to withstand the pressures arising from crisis situations and to recover from their impacts". Psychological resilience is seen there as a critical factor in the political determination of the Finnish population.[31]

Finally, in a context of hybrid strategies and information warfare, credibility can ultimately become the decisive weapon in defence of the West. In the view of Nicolini and Janda, in propaganda campaigns, disinformation is an often-used instrument. Veracity, consistency and respect for the truth are the exact opposite and enhance what has been described above as deterrence by delegitimization.[32] In its search for ways to deter hybrid threats, the European External Action Service (EEAS) of the EU stressed the importance of resilience. In a Food for Thought Paper for the EEAS, good governance and human rights and freedoms, as well as rule of law, fighting corruption, and a better system for funding political parties, were mentioned as "key ingredients in the fight against hybrid attack".[33] As was said above: total defence is not feasible. Nor is it desirable.

NATO has recognised the importance of resilience in deterring hybrid warfare by a renewed appreciation of Article Three of the Washington Treaty, the founding agreement of the North Atlantic alliance. Article Three provides that the allies "separately and jointly, by means of continuous and effective self-help and mutual

[27]Coaffee and Wood n.d., p. 505.
[28]Giegerich 2016, p. 65.
[29]Galeotti 2017, p. 15.
[30]Gray n.d., p. 258.
[31]Whither n.d., p. 65.
[32]Nicolini and Janda 2016, p. 83.
[33]Statewatch 2015, p. 22.

aid, will maintain and develop their individual and collective capacity to resist armed attack."

19.4 Monitoring Resilience

In the previous section, we argued that resilience enhances deterrence in several ways. In this section we consider the way resilience plays a role in the Russian information campaigns regarding the shooting down of flight MH17. We have taken the 2014 shooting down of flight MH17 as a case for our study because it has been an important disruptive experience, first for the families and friends of the victims. The attack has also affected Dutch society. It brought war closer to the people in the Netherlands; we respect that. What interests us here is the observation that the Putin regime immediately used this shooting down to come up with narratives which would foster uncertainty and distrust in the West in general and the Netherlands in particular.

In monitoring the presence of resilience in information warfare we need a workable set of building blocks that can serve as markers to help observe its presence. Societal resilience as such is not directly visible or measurable. But by looking at the aims of information warfare and its objectives it is possible to identify markers of a resilient society. As was stated above, by information warfare, Moscow aims to foster dividedness among citizens and distrust towards their governments, the EU and NATO. The opposite of distrust of citizens towards their governments is trust; the opposite of dividedness is social capital; the opposite of disinformation is a credible narrative. These markers have been selected on the basis of the criteria developed by the Stockholm Resilience Centre, Noordegraaf et al. (2018) and Versteegden.[34]

Trust means building trust in the nation and its institutions and combat distrust among citizens towards their governments, the EU and NATO. Trust is the willingness of citizens to believe in the authorities' ability to manage a crisis in the face of uncertainty, whereby citizens believe that the government will abide by ordinary ethical rules (e.g., telling the truth).[35] Social capital, in turn, relates to the bonds that hold people together. According to Durodié resilience has to do with the idea of who we are and where as a society we are heading. Feelings of social solidarity and self-sacrifice in society are important elements against dividedness.[36]

The use of a credible narrative, truth and transparency, can counter disinformation. The function of a narrative is to bring order in a world that is perceived as chaotic and unpredictable and serve as a framework. A strong narrative should be

[34]Stockholm Resilience Centre 2015; Noordegraaf et al. 2018; Versteegden 2018.

[35]Versteegden 2018, p. 26.

[36]Durodié 2005, pp. 42–44.

more credible than the disinformation that is to be debunked.[37] This entails deconstructing anti-democratic narratives, cultivating an informed debate and building one's own narratives on truth, values and vision. In the following section, we present our case study. After a short presentation of the case itself, we attempt to determine the degree of trust, social capital, and a credible narrative. We thus expect to obtain a picture of the resilience of Dutch society, which, again, affects the political determination of the country and ultimately its contribution to deterrence.

19.5 The Case

On 17 July 2014, flight MH17 was shot down over Ukraine. In the hours following the crash, different narratives began to emerge: Western media claimed that pro-Russian separatists downed the aircraft, while the Russian government blamed the Ukrainian military.[38] Furthermore, the Russian government stated that no missile had crossed from Russia into Ukraine. On 21 July, the United Nations Security Council unanimously adopted Resolution 2166, which condemned the shooting, called for an independent international investigation, and urged all UN member states to cooperate fully. Shortly after the crash, Dutch prime minister Mark Rutte began to use a triple narrative: bring the victims home, discover what happened, and find those responsible. On 18 July, he declared that he would not rest until the perpetrators were brought to court.

In October 2015, the Dutch Safety Board (DSB) issued its final report on the crash, concluding that a BUK surface-to-air system shot down the aircraft. In September 2016, the Dutch-led joint investigation team (JIT), which included police and judicial authorities from Australia, Belgium, Malaysia, the Netherlands, and Ukraine, presented its findings. The JIT disclosed that a missile was fired from an area that pro-Russian separatists controlled. In addition, the JIT found that the BUK was transported into Ukraine from the Russian 53rd Anti-Aircraft Brigade, based in Kursk. After shooting down flight MH17 and its passengers, the BUK returned to Russia.[39]

In May 2019, *De Groene Amsterdammer* reported that in the first two days following the crash, a St. Petersburg–based Russian troll factory issued at least 65,000 tweets blaming Ukraine for the shooting. Most of them were in Russian.[40] In the aftermath of the crash, alternative theories emerged, inspired predominantly by events undergoing investigation and public prosecution.[41] The first theory was that a Ukrainian Sukhoi Su-25 jet fighter downed the aircraft. The deputy chief of staff of the Russian Armed Forces, General Andrej Kartapolov, endorsed this theory

[37] Versteegden 2018, p. 26.

[38] Noordaa and Van der Ven, *Nepnieuws uit Sint Petersburg*.

[39] *Update investigation JIT MH17—press meeting*.

[40] Van der Noordaa and Van der Ven 2019.

[41] Rudin 2016.

in a press conference on 21 July 2014. Two days earlier, "Carlos", a so-called Spanish air traffic controller based in Ukraine, had initiated this theory over several tweets. This Twitter account proved to be fake.[42] The state-sponsored media outlet Russia Today even executed a test with a Su-25 to prove that the aircraft could reach the same altitude as flight MH17.[43]

Russian governmental institutions seem to propagate disinformation regardless of the consequences for their reputations. Disinformation activities originated primarily from actors in the Russian Federation but were also disseminated from Ukraine. The Security Service of Ukraine (SBU)[44] disclosed via Interfax that it had prevented a shrewd Russian attack on Dutch Foreign Minister Bert Koenders while he was visiting Ukraine.[45] Conversely, in August 2014, the SBU had propagated in a press conference that the target had not been flight MH17 but Aeroflot flight 2074; the intent had allegedly been to create a *casus belli* for the Russian Federation to invade Ukraine. The SBU and other Ukrainian government institutions quickly abandoned this theory.[46] Even in the Netherlands, an instance of disinformation involving a Dutch member of Parliament from the Christian Democratic Party occurred: He provided a fake witness with a text he had prepared.[47] Later, the party ended his role as spokesperson in the case of flight MH17.[48]

During the months and years to follow, the Russian narrative stabilized around the dominant message that Ukraine is responsible and all investigations are biased to discredit the Russian Federation. As soon as evidence that a surface-to-air missile caused the catastrophe emerged, the narrative changed from a Ukrainian Su-25 fighter jet to a Ukrainian BUK missile having been launched from Ukrainian-held territory. Russian state-sponsored outlets such as Russia Today and Sputnik supported both narratives. In the following sections, we monitor how Dutch society demonstrated societal resilience in the face of disinformation activities and attempts to sow doubt and discredit the investigation into the disaster. We focus on trust, social capital, and the narratives used in the discourse that surfaced after the disaster.

[42]Luhn 2014.
[43]Rudin 2016.
[44]SBU stands for Sloezjba Bezpeky Oekrajiny.
[45]RTL Nieuws 2014.
[46]Toler 2018a, b.
[47]Van der Peet 2017.
[48]Van Ast 2017.

19.6 Trust

Trust is the willingness of citizens to believe in the authorities' ability to manage a crisis. All interviewees who participated in this research mentioned this factor. For instance, the anonymous respondent from the government's crisis management organization asserted: "We were as open as we possibly could be towards the relatives of the victims and showed them what we were doing. This created mutual understanding and trust." The DSB acted similarly; Wim van der Weegen, as head of administrative affairs, advice, and communications/spokesperson, stated: "We practised openness as long as possible." The authorities understood the importance of exercising trust to avoid confusion and thus enhanced societal resilience against disinformation.

The Sociaal Cultureel Planbureau monitors social developments in Dutch society. Shortly after the shooting down of flight MH17, this institution reported that trust in the government had risen from 46 to 61% (see Fig. 19.1).[49] The September 2018 report indicated that 56% of the Dutch trust the government, which is a common figure in the Netherlands.[50] In fact, the Dutch demonstrate a stable trust level of over 70% in their legal system.[51] Research by the Centraal Bureau voor de Statistiek revealed a similar outcome between 2012 and 2018.[52]

The respondent from the government's crisis management organization had the same thoughts: "I think the Dutch population is still confident about the approach. They have faith we do this in a proper way and conscientiously." Public trust in the government is a clear sign of societal resilience, for trust is the opposition of doubt. As the government's crisis management organization's source mentioned: "In the first days, there was a lot of criticism towards the government's approach, mainly because of its being too careful. This really changed as soon as we started to repatriate the victims. Suddenly, we received a lot of positive feedback."

Whenever the DSB or JIT publicized a report, Russian sources responded with messages to undermine trust in these institutions. The government's crisis management organization confirmed: "The Dutch minister of foreign affairs summoned the Russian ambassador … to make clear Russia had to stop with its continuous efforts to discredit the DSB and JIT investigations. This step was taken when high-ranking Russian officials had started to amplify this narrative." Gaining and maintaining the trust of the victims' relatives has been a key factor in facilitating the investigation processes. As Piet Ploeg, chairman of the MH17 Disaster Foundation (see below) asserted: "Whatever these [Russian] people did to convince us, they simply didn't succeed because the vast majority of the relatives had faith in the

[49]Netherlands Institute for Social Research (SCP) 2018_3.

[50]Netherlands Institute for Social Research (SCP) 2018_3, p 15.

[51]Ibidem, Fig. 1.6.

[52]CBS 2019.

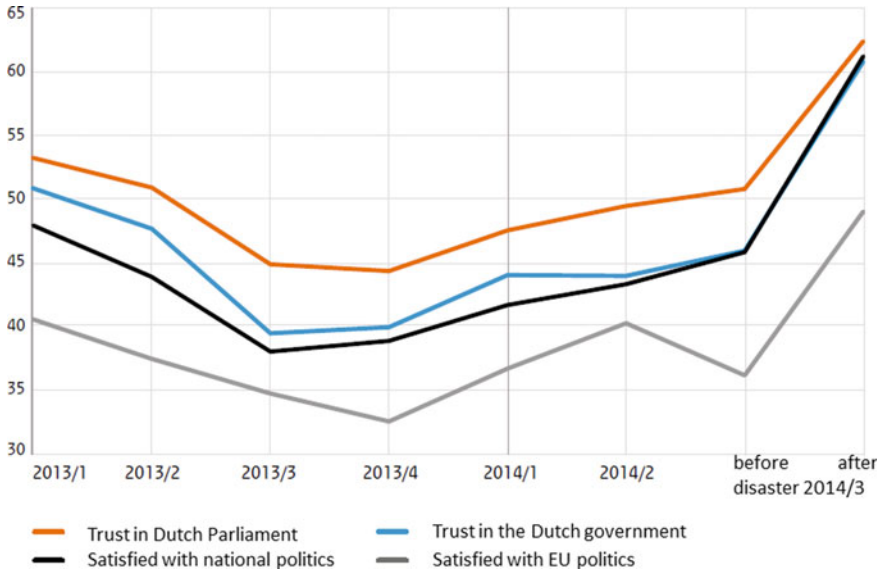

Fig. 19.1 Political confidence increases after the disaster (*Source* Netherlands Institute for Social Research (SCP) 2014_3, p. 2.)

government, the Public Prosecution Service, and the Dutch Safety Board. Even the more activist part of the relatives did." Ploeg thus clarified the correlation between trust and societal resilience against disinformation.

When one considers trust in a societal context, it is necessary to seek trust in social media as well, since social media platforms are also used for disseminating disinformation. Again, *De Groene Amsterdammer* analyzed over 65,000 tweets concerning flight MH17 that a Russian troll factory had sent in July 2014.[53] While the use of social media could not be researched extensively due to the time and space limitations of this chapter, it is clear that social media platforms have had a muting effect on the debate. Trust in the Dutch authorities was a constant factor. Like in other crises, such as the recent outbreak of COVID-19, trustworthy leadership guides the nation. Shortly after the disaster of flight MH17, trust in the Dutch government rose to 61%; afterward, trust returned to normal levels, regardless of disinformation activities (see Table 19.1).

[53]Van der Noordaa and Van der Ven 2019.

Table 19.1 Opinions on the Dutch government's actions in the case of flight MH17 (*Source* Peil.nl 2019)

What is your opinion on the government's actions in this case over the past year?	8-2-2015 (%)	5-27-2018 (%)
Positive	14	11
Quite positive	31	24
Neutral	26	30
Negative	13	13
Quite negative	15	16
Don't know/no opinion	1	6
Total	100	100

19.7 Social Capital

The Russian narratives have been particularly hurtful to the families and friends of the 298 victims. Shortly after the crash, the MH17 Disaster Foundation was founded to assist and support the victims' families. The PPS established a team of trained family counsellors to assist the families and retrieve the personal belongings of their loved ones for identification purposes. Its chairman, Piet Ploeg, attributes a key role to these counsellors: "An effect of the family counsellors was that they kept us together." This unity has made it difficult to create divisions within this group. National symbols have also encouraged unity. As Ploeg stated: "The government and the royal family were very much involved. This was very supportive for the victims of the relatives." This commitment, as demonstrated by the government's extensive support to the families and the role of national symbols, as signified by the Dutch royal family's involvement, proves how social capital in the case of flight MH17 contributes to societal resilience against the effects of disinformation. In this case, social capital helped to strengthen the ties between the disorientated and otherwise affected families and the government managing the emerging crisis.

Fons Lambie, an RTL journalist, mentioned how social capital contributes to societal resilience. He described the long line of funeral vehicles that transported the bodies from Eindhoven Airport to Hilversum over the Dutch highways. Standing on bridges and flyovers, thousands of people offered their respect to the funeral procession. Lambie: "This massive expression of grief that paid tribute to the hearse columns when the bodies returned really united the nation and made it very hard to cause divisions." However, according to Lambie, these circumstances could also change: "What would happen if a populist prime minister, like Thierry Baudet, would take office?" This event could very well cause a shift in thinking about flight MH17 as populist authoritarian movements in the Netherlands strive to improve relationships with Russia.[54] These parties also support the Russian narrative, as

[54]The Hague Centre for Strategic Studies 2017, p. 88.

Table 19.2 Opinion poll 27 May 2018: Who is responsible for the shooting down of flight MH17? (*Source* Peil.nl 2019)

Which party in the conflict in Ukraine shot down the aircraft?	5-27-2018 (%)
The Ukrainian army	5
Separatists who strive to separate Eastern Ukraine	22
The Russian army	52
Don't know/no opinion	21
Total	100

illustrated in a poll published on 27 May 2018 (see Table 19.2). It is mainly among the constituencies of the populist Party for Freedom and Forum for Democracy that sympathies for the Russian narratives can be found.[55]

On 9 March 2020, the official trial against Igor G., Sergey D., Oleg P., and Leonid K.—three Russians and one Ukrainian from Eastern Ukraine—for the murder of the 298 passengers on the Malaysian Airlines jet began in a court near Schiphol Airport. As two-thirds of the victims were Dutch and a Dutch team conducted the investigation, the trial is being held in the Netherlands. The public trial serves to deter by delegitimization as every single detail disclosed will discredit the alternative narratives that Russian actors have issued.

From day one, the Dutch authorities have made significant efforts to support the families of the victims. Despite the attempts to create division, overall, these families kept the rows closed with the crime investigation teams.

19.8 Credible Narrative

In the case of flight MH17, narratives have played a critical role. In fact, the case can be characterized as a battle of narratives. From the beginning, official and state-sponsored media outlets from Russia have blamed Ukraine for the shooting down of flight MH17. As soon as evidence began to collect, these media turned to a second, more defensive approach that strove to discredit the DSB and the findings of the JIT. The Dutch government's narrative has consistently focused on three courses of action: bringing the victims home, investigating the tragic crash, and finding those responsible. The respondent from the government's crisis management organization stated: "Prime minister Rutte uses this frame over and over to explain why things take so much time and uses it to show compassion with the relatives of the victims." As Piet Ploeg confirmed: "The government had a narrative as clear as a three-stage rocket: get back the victims, find out what happened, and bring the perpetrators to court."

[55]Peil.nl 2018.

The narrative of the Dutch government proved to be a helpful frame to counter disinformation since each of the respondents recognized the threefold approach. The design was well chosen to maintain a distinct separation in responsibilities between governmental institutions. It was also propagated as a frame for all separate activities. The government's crisis management organization's source commented: "In all those years, the prime minister always has been very clear about the different independent roles of the institutions DSB and JIT because he has been very much aware of the risk he would take to be framed as biased by the Russians." The design and execution of this narrative contributed to societal resilience because it served as a frame to counter disinformation.

Van der Weegen (DSB) offered a prime example of how creating an image can vigorously enhance resilience against disinformation. He stated: "The (iconic) reconstructed hull image has been thoroughly considered and designed in support of DSB's narrative (i.e., the findings to be presented cogently in a threefold approach: report, computer animation, and presentation in front of the reconstructed cockpit)."

The Dutch government communicated a triple narrative of returning the victims home, establishing what happened, and bringing the perpetrators to justice. The agenda of the Russian Federation was clear to all involved, and they responded by being aware of disinformation, shielding information from cyberattacks, and avoiding mistakes that could fuel disinformation activities.

19.9 Conclusion

In this chapter, we tried to establish is how subversive Russian activities were taking place and what measures were taken by the Netherlands government in order to counteract them. We monitored societal resilience by looking for the presence of trust, social capital, and credible narratives in reaction to disinformation activities after a disruptive event. All these elements appeared to be present in the MH17 case. In Dutch society, a feeling of trust in the government, the PPS, and the DSB emerged. Despite concerns about pro-Russian populist parties, social capital proved to be relevant to strengthening the ties between the disoriented and otherwise affected families and the government managing the crisis. The narrative that the government used—bring the victims home, discover what happened, and bring the perpetrators to court—was a robust frame in countering the effects of disinformation on Dutch society. Russian narratives were discredited. An independent and transparent criminal procedure is underway; it is aimed at truth-finding and fine-tuned toward the individual perpetrators and therefore an antidote to disinformation. To illustrate whether that contributes to deterrence, we have divided deterrence into deterrence by denial, punishment, and delegitimization.

Overall, the handling of the MH17 case has reinforced deterrence by denial. Russian disinformation has thus far proven to be unconvincing for most Dutch target audiences. Moreover, the prime minister has demonstrated his commitment to

the case, while the Dutch authorities have upheld a consistent narrative and fostered trust and social capital by example. The government has also respected the independent position of others, such as the PPS and the free press, in their search for the truth. Other sources of information, such as free independent news networks and digital forensic networks, have been paramount in discrediting disinformation and allowing the public to conclude what it actually is: lying. In the case of flight MH17, one newspaper disclosed how a Dutch MP instructed a fake witness in a meeting, and a Dutch weekly disclosed how a well-known Russian troll factory based in St. Petersburg disseminated over 65,000 tweets shortly after the crash. Digital forensic platforms such as Bellingcat and the EEAS initiative of the EU pose a serious threat to the originators of disinformation. During the prosecution process, for instance, civic journalists were a great help in disclosing the exact route of the BUK installation entering and leaving Eastern Ukraine. In summary, insofar as Russian alternative narratives have not been able to gain any real foothold in Dutch society, deterrence by denial has been enhanced.

The criminal proceedings against the suspected perpetrators of the shooting down of flight MH17 are themselves a movement toward punishment. The DSB and the Public Prosecution Service have played a key role in unravelling the catastrophic events, as well as prosecuting the alleged perpetrators. The latter formed the core of the international JIT; the research was thorough, transparent, and followed a fixed protocol. Furthermore, the DSB and JIT were aware of the risk of disinformation and introduced additional checks and balances to avoid mistakes. A resolution of the Security Council of the United Nations supported the entire procedure.

Finally, the legal proceedings and the MH17 trial, which began on 9 March 2020, have contributed to deterrence by delegitimization. The trial has demonstrated not only the determination of the Dutch to bring the perpetrators to court but also that every single detail that surfaces will discredit the alternative facts and narratives that Russian sources have disseminated. We have taken the killing of the 298 passengers on flight MH17 as our case. What we observed was best described by the Dutch government official who remarked: “I think the Dutch population is still confident about the approach. They have faith we do this in a proper way and conscientiously.” The case of flight MH17 offers a prime example of how a resilient society can deter an actor from conducting effective disruptive campaigns.

References

AIVD (Algemene Inlichtingen- en Veiligheidsdienst) (2020) Jaarverslag 2019 [Annual Report]. AIVD, The Hague

Brief ongewenste buitenlandse inmenging (2018) [Letter unwanted foreign interference], Brief van de minister van Veiligheid en Justitie Ferd Grapperhaus en de minister van Binnenlandse Zaken en Koninkrijksrelaties drs K.H. Ollongren aan de Voorzitter van de Tweede Kamer der Staten Generaal (16 March 2018). https://www.rijksoverheid.nl/documenten/kamerstukken/2018/03/16/tk-brief-ongewenste-buitenlandse-inmenging. Accessed 28 May 2020

CBS (2019) Public Trust in EU and Politics on the Rise. SCP 14/03/2019. https://www.cbs.nl/en-gb/news/2019/11/public-trust-in-eu-and-politics-on-the-rise. Accessed 9 March 2020

Coaffee J, Wood D M (n.d.) Security is Coming Home: Rethinking Scale and Constructing Resilience in the Global Urban Response to Terrorist Risk. International Relations 20.4:503–517. https://doi.org/10.1177/0047117806069416. Accessed 28 May 2020

Cullen P J, Reichborn-Kjennerund E (2017) Understanding Hybrid Warfare. MCDC Countering Hybrid Warfare Project, MCDC January

Daalder I H (2017) Responding to Russia's Resurgence; Not Quiet in the Eastern Front. Foreign Affairs 38. http://heinonline.org/HOL/LandingPage?handle=hein.journals/fora96&div=132&id=&page. Accessed 23 October 2017

Davis J (2015) Continued Evolution of Hybrid Threats; The Russian Hybrid Threat Construct and the Need for Innovation. The Three Swords Magazine 28:19–25

Durodié B (2005) Cultural Precursors and Psychological Consequences of Contemporary Western Responses to Acts of Terror. In: Wessely S, Krasnov V N (eds) Psychological Responses to the New Terrorism: A NATO-Russia Dialogue 37. IOS Press, Amsterdam, 37–53. http://www.durodie.net/pdf/Cultural%20Precursors%20and%20Psychological%20Consequences-Wessely.pdf. Accessed 7 December 2015

Fjäder C (n.d.) The Nation-State, National Security and Resilience in the Age of Globalisation. Resilience 2.2:114–129. https://doi.org/10.1080/21693293.2014.914771. Accessed 12 May 2020

Galeotti M (2017) Controlling Chaos: How Russia manages its political war in Europe. European Council on Foreign Relations, London

Giegerich B (2016) NATO's Strategic Adaptation, the Warsaw Summit and Beyond. The Polish Quarterly of International Affairs 1:61–68

Gray C (n.d.) Deterrence in the 21st Century. Comparative Strategy 19.3:257. https://doi.org/10.1080/01495930008403211. Accessed 22 January 2020

Knopf J W (n.d.) Fourth Wave in Deterrence Research. Contemporary Security Policy 31.1.1–33. https://doi.org/10.1080/13523261003640819. Accessed 28 May 2020

Luhn A (2014) The Infowar rages in Moscow, Foreign Policy, 18 July 2014. https://foreignpolicy.com/2014/07/18/the-infowar-rages-in-moscow/. Accessed 19 February 2020

MCDC Countering Hybrid Warfare Project (2019) Hybrid Warfare: Understanding Deterrence, Information Note. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/795220/20190304-MCDC_CHW_Info_note_6.pdf. Accessed 20 May 2020

Nicolini M, Janda J (2016) In the Area or Out of Business: Building Resilience to Hybrid Attacks. The Polish Quarterly of International Affairs 1:77–87

Noordegraaf M, Schiffelers M, Geuijen K, De Morree P, Pekelder J (2018) Op weg naar een Weerbare Open Samenleving. WODC, Utrecht

Oliker O (n.d.) Putinism, Populism and the Defence of Liberal Democracy. Survival 59.1:7–24. https://doi.org/10.1080/00396338.2017.1282669. Accessed 21 February 2017

Peil.nl (2018) De stemming van 27 mei 2018. https://www.noties.nl/v/get.php?a=peil.nl&s=weekpoll&f=2018-05-27.pdf. Accessed 21 February 2020

Peil.nl (2019) De stemming van 23 juni 2019. https://www.noties.nl/v/get.php?a=peil.nl&s=weekpoll&f=2019-06-23+frd.pdf. Accessed 20 February 2020

Rietjens S (2019) Unravelling Disinformation: The case of the MH17. The International Journal of Intelligence, Security and Public Affairs 21.3:195–218. https://doi.org/10.1080/23800992.2019.1695666. Accessed 20 April 2020

Risico en crisisbarometer. https://www.nctv.nl/onderwerpen_a_z/Risico-en-crisisbarometer/rcb-overzicht.aspx. Accessed 14 February 2020

Rodin J (2014) The Resilience Dividend, Being Strong in a World Where Things Go Wrong. Public Affairs, New York

Rodin J (2015) The Resilience Dividend; Managing Disruption, Avoiding Disaster, and Growing Stronger in an Unpredictable World. Profile Books, London

RTL Nieuws (2014) Aanslag op Nederlandse delegatie in Charkov verijdeld, 18 November 2014. https://www.rtlnieuws.nl/nieuws/artikel/1511341/aanslag-op-nederlandse-delegatie-charkov-verijdeld. Accessed 15 February 2020

Rudin M (2016) Conspiracy Files: Who shot down MH17. BBC News, 25 April 2016. https://www.bbc.com/news/magazine-35706048. Accessed 22 February 2020

Rühle M (2015) Deterrence: what it can (and cannot do), NATO Review, 20 April 2015. http://www.nato.int/docu/review/2015/also-in-2015/deterrence-russia-military/EN/index.htm. Accessed 19 December 2016

Smith R (2005) The Utility of Force; The Art of War in the Modern World. Random House, New York

Statewatch (2015) Food-for-thought paper "Countering Hybrid Threats". Working Document of the European External Action Service EEAS (2015) 731 (2015) Crisis Management and Planning Directorate 13/05/2015. http://www.statewatch.org/news/2015/may/eeas-csdp-hybrid-threats-8887-15.pdf. Accessed 19 November 2015

Stockholm Resilience Centre (2015) Applying resilience thinking; Seven principles for building resilience in social-ecological systems. https://www.stockholmresilience.org/research/research-news/2015-02-19-applying-resilience-thinking.html. Accessed 29 March 2019

Strachan H (n.d.) Strategy and Democracy, Survival 62.2:51–82. https://doi.org/10.1080/00396338.2020.17399499. Accessed 7 May 2020

The Hague Centre for Strategic Studies (2017) The Rise of Populist Sovereignism. The Hague Centre for Strategic Studies, The Hague

Toler A (2018a) Addressing the Aeroflot MH17 Conspiracy Theory. Bellingcat. https://www.bellingcat.com/news/uk-and-europe/2018/08/08/addressing-aeroflot-mh17-conspiracy-theory. Accessed 28 June 2019

Toler A (2018b) The Kremlin's Shifting, Self-Contradicting Narratives on MH 17. Bellingcat.com, 1 May 2018. https://www.bellingcat.com/news/uk-and-europe/2018/01/05/kremlins-shifting-self-contradicting-narratives-mh17/. Accessed 15 May 2020

Treverton G F, Thvedt A, Chen A R, Lee K, McCue M (2018) Addressing Hybrid Threats. Swedish Defense University, Center for Asymmetric Threat Studies, The European Centre of Excellence for Countering Hybrid Threats. Stockholm. https://www.hybridcoe.fi/wp-content/uploads/2018/05/Treverton-AddressingHybridThreats.pdf. Accessed 28 May 2020

Update investigation JIT MH17 – press meeting, Netherlands Public Prosecution Service, 24 May 2018. https://www.prosecutionservice.nl/topics/mh17-plane-crash/criminal-investigation-jit-mh17/speakers-text-jit-mh17-press-meeting-24-5-2018. Accessed 26 April 2020

Van Ast M (2017) Koenders noemt MH17-brief van Baudet "stuitend", Algemeen Dagblad, 6 September 2017. https://www.ad.nl/politiek/koenders-noemt-mh17-brief-van-baudet-stuitend~a7a86c81/. Accessed 16 February 2020

Van der Noordaa R, Van der Ven C (2019) Nepnieuws uit Sint Petersburg, De Groene Amsterdammer, 13 May 2019. https://www.groene.nl/artikel/nepnieuws-uit-sint-petersburg. Accessed 14 May 2019

Van der Peet A (2017) Omtzigt excuseert zich voor onzorgvuldigheid rondom "valse" getuigenis MH17 ramp, Algemeen Dagblad, 11 November 2017

Van Doorn C (2019) Societal resilience and an answer to disinformation: The case of flight MH17. Netherlands Defence Academy, Breda

Versteegden C (2018) Resilience can counter Dezinformatsiya, How the military considers its contribution to enhancing Dutch resilience. Netherlands Defence Academy, Breda

Whither J K (n.d.) Back to the Future? Nordic total defence concepts. Defence Studies 20.1:61–81. https://doi.org/10.1080/14702436.2020.1718498. Accessed 7 May 2020

Wilner A S (2011) Deterring the Undeterrable: Coercion, Denial and Delegitimization in Counterterrorism, The Journal of Strategic Studies 34.1:3–37. https://doi.org/10.1080/01402390.2011.541760. Accessed 20 May 2020

Cees van Doorn (MA) serves as a lieutenant-colonel in the Netherlands Army Reserve. He currently holds a position of Strategic Advisor in 1 NL-Civil Military Interaction Command.

Prof. Theo Brinkel is KVMO professor of Civil-military relations at Leiden University as well as associate professor of Security and Defence Policy at the Netherlands Defence Academy. He published on resilience, nation-building and pluralism and political decision-making on security and defence policy. Previously, he was Member of the Dutch Parliament and general-secretary of Pax Christi Netherlands.

Chapter 20
Cyber Deterrence: The Past, Present, and Future

Stefan Soesanto and Max Smeets

Contents

Abstract The question on whether and how deterring an adversary in or through cyberspace is feasible has provoked the minds of scholars and practitioners for decades. Today, cyber deterrence remains a quintessential anchoring concept for the political debates on cyber policy. However, does the concept of deterrence in cyberspace have a future when for almost three decades little to no seemingly feasible practical solutions nor an academic consensus have emerged? The purpose of this chapter is to situate the current debate on cyber deterrence within the historical evolution of deterrence thinking in cyberspace, clarify the existing conceptualizations, and comprehensively discuss whether the concept of cyber deter-

S. Soesanto (✉)
The Risk and Resilience Team, Center for Security Studies (CSS), ETH Zurich, Zurich, Switzerland
e-mail: stefan.soesanto@sipo.gess.ethz.ch

M. Smeets
Center for Security Studies (CSS), ETH Zurich, Zurich, Switzerland
e-mail: Smeets@ethz.ch

M. Smeets
Center for International Security and Cooperation, Stanford University, Stanford, CA, USA

M. Smeets
Centre for Technology and Global Affairs, University of Oxford, Oxford, UK

F. Osinga and T. Sweijs (eds.), *NL ARMS Netherlands Annual Review of Military Studies 2020*, NL ARMS, https://doi.org/10.1007/978-94-6265-419-8_20

rence has an analytical future. We argue that the future deterrence debate can move into four directions: increased incorporation of cyber deterrence as an element within the broader international security and contest in a multi-domain world. A deeper focus on the technical aspects of the cyber domain to achieve deterrence effects on the operational and tactical level. A closer analysis of compellence, as the alternative form of coercion. And an exploration of new strategic concepts that seeks to contain and blunt adversarial aggression in cyberspace that stands apart from traditional deterrence thinking.

Keywords Cyber Deterrence · Offensive Cyber Operations · strategy · cyberspace

20.1 Introduction

The question on whether and how deterring an adversary in or through cyberspace is feasible has provoked the minds of scholars and practitioners for decades. The definition of 'cyber deterrence' has evolved over time and been conceptually stretched.[1] Today, it remains a quintessential anchoring concept for the political debates on how to deal with the wide-range of cyber threats in general and offensive military cyber operations in specific. But does the concept of deterrence in cyberspace have a future when for almost 30 years little to no seemingly feasible practical solutions nor an academic consensus have emerged?[2]

The purpose of this chapter is to situate the current debate on cyber deterrence within the historical evolution of deterrence thinking in cyberspace, clarify the existing conceptualizations, and comprehensively discuss whether the concept of cyber deterrence has an analytical future.[3]

This chapter is logistically structured into three sections. The first section discusses the historical evidence of cyber deterrence literature—also delving into its conceptual origins. The second section looks at the two uses of the term in the present—and identifies six distinct cyber deterrence mechanisms. The third section is about the future of cyber deterrence research. It explains why a deeper understanding of the dynamics of cyber operations is essential for the cyber deterrence concept as a whole. It also explores avenues for new theoretical research that moves beyond the mere idea of traditional deterrence concepts. The chapter culminates with a conclusion that draws out several implications.

---

[1]Indeed, many other cyber terms—and the prefix itself—have suffered the same fate; Sartori 1970; Shires and Smeets 2016.

[2]For a more extensive discussion on the lack of agreement, see Brantly and Smeets, forthcoming. The general notion is that cyber deterrence below the threshold of armed attack is not working.

[3]Also, whilst compellence is a potentially more promising form of coercion in cyberspace, this chapter only focuses on cyber deterrence. For broader overviews on coercion and the strategic value of offensive cyber operations, see Borghard and Lonegran 2017; Smeets 2018; Libicki 2012; Byman and Waxman 2001.

20.2 The Past

To map the evolution of deterring an adversary online, it is worth venturing back to the early days of the hacking community. During the 1970s and 80s, phreakers—or phone hackers—used to listen to "the clicks and clunks and beeps and boops" to figure out how the telephone system worked and how they could manipulate it.[4] Although few underground stories from those hay days have been made public, the most well-known phreaker 'conflict' occurred back in 1989—when the Masters of Deception (MoD) went to 'war' against the Legion of Doom.[5] The 'cyber activity' of the time could include switching a target's phone carrier to another carrier; making a target's phone ring constantly to the effect that the victim had to unhook his phone and leave it unhooked for hours on end; or eavesdropping on and cross-connecting a victim's phone call (imagine you are calling your parents and suddenly a 911 operator joins the call wanting to know what your emergency is).[6] During this "gang-war in cyberspace", as *Wired* called it, deterrence was primarily discussed with a criminology mind-set—though with an ill understanding of seriousness of offense, rehabilitation, recidivism, and above all offender's motivations and ability to act. Kevin Mitnick spent five years in prison for various 'cyber crimes', including eight months in an isolation cell, when he was caught by the FBI in 1995. The reason he received this harsh treatment is because someone convinced the judge he was able to initiate "a nuclear war by whistling on a public telephone".[7]

Parallel to the end of the phreaking days and the expansion of the World Wide Web, the idea of—what was then called—information warfare, gained increasing traction within the US Department of Defense.[8] Definition-wise, it was an amalgam ranging from "media wars to electronic combat, and from economic competition to strategic conflict waged against civilian populations".[9] In a sense, information warfare then was what hybrid warfare is now. A concept that encompassed everything and was analytically so broad that it is hard to strategize, plan, and act around the term. Early attempts at bringing deterrence thinking into the information warfare discussion, led to the recognition that network defences were overall

[4]Lapsley 2013.

[5]This is an inherently western-biased conception of the emergence of the field. For an early history in the Chinese context (from 1995), see Henderson 2007.

[6]Slatalla and Quittner 1994.

[7]Mitnick 2012.

[8]The term is said to originate in 1970s, when Tom Rona in the Office of Net Assessment was investigating the relationships among control systems (now known as cybernetics). See Keuhl 2002.

[9]In fact, as the Congressional Research Service writes in a report, "Although several official documents now refer to "information warfare" in other countries, [as of 2018] the United States has no formal government definition of IW. The DOD definition of information operations refers only to military operations and does not emphasize the use of cyberspace to achieve nonmilitary strategic objectives"; Wheatley and Hayes 1996, p. iii; Theohary 2018, p. 6.

inadequate and that they needed to be improve to deter anyone. In other words, deterrence was largely equated with better defence.

Through several war-gaming scenarios, the United States Department of Defense (DoD) slowly but surely realized that the US would be unable to simply deter an adversary through defensive measures alone when they themselves were unable to climb their way out of the proverbial glasshouse.[10] Consequently, information warfare turned purely offensive, sparking concepts such as decapitation strikes—whose aim was to sever the linkages between an adversary's political leadership and the mechanisms it utilizes to control its civilian population; and counter command-and-control—which focused on breaking the communication links between an adversary's military leadership and the military assets deployed on the battlefield.[11] In essence, adversaries were seen as information hubs and spokes systems whose functioning was dependent upon the continuous information exchange between its parts. Anything from telephone lines, computers, radios, and media outlets were subsequently tagged as cut-off point to break this information flow and thereby weaken and subsequently defeat an enemy through sheer chaos creation.

In 1993, RAND's John Arquilla and David Ronfeldt introduced the concept of 'Netware' in an article titled "Cyberwar is Coming".[12] Netwar was distinctly different from cyberwar. Cyberwar stood in the tradition of counter command-and-control, by focusing on the disruption if not even destruction of adversarial information and communication systems. Its primary goal: tipping the balance on information and knowledge. Netwar by contrast was defined by Arquila and Ronfeldt as "trying to disrupt, damage, or modify what a target population 'knows' or thinks it knows about itself and the world around it".[13] Meaning, pure Netware was a societal-level focused, inherently non-violent, ideational conflict, aimed at disruption rather than destruction. To some degree Netware shared significant overlaps with what was then known as information-based deterrence, that is "turning international opinion against an aggressor, altering his perception of the military correlation of forces in theatre, and fostering instability in his country".[14] However, Netware, as Arquila and Ronfeldt defined it, was removed from the traditional battlefield and encompassed adversaries as diverse as "transnational terrorists, criminals, and even radical activists".[15] In other words, it also included organized non-state hacker communities. At its core, Arquila and Ronfeldt viewed an adversary not as one large harmonious network, but numerous smaller ones,

[10]Wheatley and Hayes 1996, op cit.

[11]Also see Broder 1990; Molander et al. 1996.

[12]It should be noted, however, is that it was the Mongol way of warfare from the 12th and 13th century which inspired Arquilla and Ronfeldt to coin the term 'netwar'. See Arquilla and Ronfeldt 1993.

[13]Arquilla and Ronfeldt 1993, op cit, p. 28.

[14]Nichiporuk 1999, p. 193.

[15]Ronfeldt and Arquilla 1999, p. 352.

each with their own internal stability, interests, and allegiances, that were organized to function as a somewhat coherent unit. The most important aspect of counter-Netware thinking was thus that an adversary could be potentially defeated by targeting the connectivity between and among these smaller networks, to shape how they interacted and behaved differently when disconnected from each other. Defending against a Netware would be inherently difficult, if not impossible, given how deep an adversary will have to penetrate into a target's society. Writing in the late 1990s, Arquila and Ronfeldt therefore concluded that, "it may be that deterrence against netwar will grow problematic, and all that will remain is a choice between either preclusive or depth-oriented defensive schemes. The former applies an ability to provide 'leak-proof' defences, while the latter accepts initial incursions, then aims to expel the intruders or invaders by means of counterattack."[16]

Amidst the question of how deterrence might work in the context of this more refined view of information warfare, the term cyber deterrence was forming. In his 1994 Wired piece, James Der Derian coins 'cyber deterrence' talking about the US Army's Desert Hammer VI war game exercise.[17] Far from outlining how an adversary can be deterred in cyberspace, Der Derian's term described the Army's fusing of "media voyeurism, technological exhibitionism, and strategic simulations" to create a hyper digitalized image of US military dominance across the four traditional battlespace domains.[18] Coming out of the aftermath of Desert Storm, which saw the baptism of stealth technology, precision guided ammunition use, and the unprecedented access of embedded journalists, Der Derian's definition made perfect sense. The major problem was that cyber deterrence stood apart from the cyberwar concept, had little to nothing to do with Netware, and only partially captured the logic of information warfare. What Der Derian's definition nonetheless did, was to point out the obvious fact: Deterrence is a mind game.

In 1995, the DoD eventually tasked RAND to explore "the development and achievement of national information warfare goals" in a series of wargames. While the final report by Molander et al. opened up more questions than answers, it does provide a few insights into the early days of cyber deterrence thinking as it is widely understood today. The report summarized the participant's question by noting that;

> [first], how will one make retaliatory threats and against whom when there is great uncertainty about the origin of an attack. Second, there is the question of the proportionality of any response when the immediate and collateral damage associated with a particular act of cyberspace retaliation is poorly understood by national decision makers. Third is the potential asymmetry of vulnerability between the United States, its allies, and the potential opponent. […] All of this points to the prospect that there will be no low-cost and conceptually simple deterrent concept that obviates the need to worry about future cyberspace attacks.[19]

[16]Ronfeldt and Arquilla 1996, p. 94.

[17]Der Derian 1994.

[18]Ibid.

[19]Molander et al. 1996, p. 38.

By 1996, still very few scholars and practitioners actually thought about deterrence in cyberspace as being feasible. Richard Harknett for example concluded that "the nature of Netware and cyberwar lend themselves to analytical frameworks and a strategic calculus dominated by offense-defence models, rather than by deterrence."[20] Gary Wheatley and Richard Hayes similar observed that "while significant, overall U.S. capability and will do not guarantee deterrence of information attacks."[21] It would take another 25 years for this 'demonstration of will' to translate into the strategic concept we now call: persistent engagement.

Figure 20.1 provides a historical overview of the journal articles, book chapters, and research reports written on the specific terms 'cyber deterrence' and 'cyberdeterrence'.[22] Based on the figure, we can roughly distinguish between three phases in the literature: The early period, stretching from the early 1990s to the DDoS attacks against Estonia in 2007. The advancement period, when publications on cyber deterrence sky-rocketed from 2007 until 2016. And the reflection period, which has seen publications on cyber deterrence drop from its height in 2016 to 2014 levels.[23]

[20]Harknett 1996.

[21]Participants at the 1993 US-Navy sponsored wargame titled 'Strategic Deterrence and Information Warfare' even argued that "[high leverage options] work best with other deterrent measures such as presence, force movements (e.g. movements into theater; call up of reserves), and other direct deterrent actions that serve as a demonstration of will". Wheatley and Hayes op cit, p. 19.

[22]Annual JSTOR search results for the terms 'cyber deterrence' and 'cyberdeterrence.' The terms 'cyber deterrence' and 'cyberdeterrence' were chosen, due to JSTOR's search engine ignoring hyphens between two words as well as capitalizations. Meaning, the term 'Cyber-deterrence' returns the same search results as 'cyber deterrence.' The annual division was attained by searching for the keywords from ex. 2000/01 to 2000/12. The former number denoting the year, the latter the month. Additionally, the search was performed with the 'access type' switched to 'all content' to capture even those publications JSTOR includes in its search results that are inaccessible through the JSTOR subscription. The methodology has several shortcomings, which, although significant, we deem good enough for the rough estimation of the growth and decline of the usage of the term cyber deterrence/cyberdeterrence. The most obvious shortcoming is that JSTOR treats the search query 'cyber deterrence' also a search for the individual terms 'cyber' and 'deterrence.' Meaning, it returns hits in which both terms are used pages apart. From a statistical point of view this is a problem. From an analytical perspective it is not. Any writings on 'cyber' that touch upon 'deterrence' even in a different context are worth including. In this case, casting a wider net is more adequate than using a narrow one. The second shortcoming concerns the time lag for newer publications to make their way into the JSTOR database. Meaning the further away the year of publication, the more stable the number of search hits for that year. One could argue that this invalidates our notion of a decrease in the publications on cyber deterrence since 2016. While we do expect a rise in the numbers for the years 2017, 2018, and 2019, we are highly confident—based on the analytical part of this chapter—that these figures will not reach the level of 2016. Time will tell whether we are right. As of this writing we definitely are.

[23]Excluding results from unrelated disciplines, such as toxicology, does not significantly alter the search results.

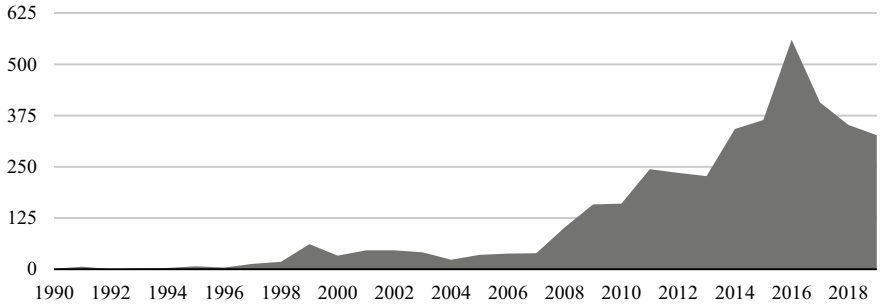

Fig. 20.1 Journal articles, book chapters, and research reports on cyber deterrence, Jan 1990—Dec 2019 (*Source* Soesanto and Smeets)

20.3 The Present

In the aftermath of the DDoS attacks against Estonia, the cyber literature turned into high gear.[24] From 2007–2008 onwards, discussion of cyber war has dominated the literature.[25] Betz and Stevens note the "popular discourse on cyberwar tends to focus on the vulnerability of the 'physical layer' of cyberspace to cyber-attack and the ways in which this may permit even strong powers to be brought to their knees by weaker ones, perhaps bloodlessly."[26] Indeed, Richard Clarke and Robert Knake wrote one of the most widely-read books on cyberwar in 2010—spurring an increase in academic literature—talking about the different ways a cyber-attack could potentially take down the United States power grid.[27] More sceptical research was published too, observing a striking absence of destructive cyber-attacks—including the article and book by Thomas Rid pushing back against the cyberwar hype.[28]

Against this backdrop, it is hardly surprising that cyber deterrence started to receive increased attention. If war and conflict are possible in cyberspace, then

[24]For a more comprehensive overview of literature topics, see Smeets and Gorwa 2019.

[25]For key works, see Rid 2012; Gartzke 2013; Liff 2012.

[26]Betz and Stevens 2011, p. 76.

[27]Clarke and Knake 2010.

[28]Rid 2012.

deterrence must be possible or needed as well.[29] By 2016, the academic discussion on cyber deterrence peaked with 480 publications that year.[30]

Today, as a military concept, cyber deterrence has at least three different meanings. First, cyber deterrence can refer to the use of (military) cyber means to deter a (military) attack. Second, cyber deterrence can refer to the use of (military) means to deter a (military) cyber-attack. Third, cyber deterrence can refer to the use of (military) cyber means to deter a (military) cyber-attack. Although not explicitly spelled out, the majority of the existing literature has focused on the latter two conceptions.[31]

Scholars currently disagree to what degree it is generally possible to deter an adversarial cyber-attack. Table 20.1 provides an overview of the distinct positions various scholars have articulated over the past few years.[32] Within this table we can roughly distinguish between three groups of scholars. The first group (denoted in the table in light grey) argues that cyber deterrence does not have distinctive problems and therefore works—or occasionally fails—like conventional deterrence. Dorothy Denning, for example, notes that cyberspace "shares many characteristics with the traditional domains," and thus deterrence can be achieved through existing regimes—e.g. norms and international agreements, better cyber security, and applying the classical deterrence by punishment logic.[33] The second group of scholars (denoted in the table in dark grey) believes that cyber deterrence encompasses a unique set of issues because cyberspace is inherently different from the traditional domains. Solving the deterrence puzzle is thus only be possible if we gain a better understanding of the underlying dynamics at play. Proponents of cyber deterrence—in either the first or second group—tend to discuss one of the following four deterrence logics: (i) Deterrence by denial, (ii) deterrence by punishment, (iii) deterrence by entanglement and (iv) deterrence by—delegitimization.[34]

First, *deterrence by denial* is essentially synonymous to cybersecurity. At its core, the conceptual idea is that better cybersecurity will decrease the probability of

[29]Having said this, Martin Libicki—discussing the Estonia DDoS attacks as the opening of his classic book 'cyberdeterrence and cyberwar'—was quick to note that the "ambiguities of cyberdeterrence contrast starkly with the clarities of nuclear deterrence" and "military cyberdefense is like but not equal to civilian cyberdefense". Libicki 2009, pp. xii–xvii.

[30]This paper focuses on academic research in the international relations field, which dominates the discussion on cyber deterrence. There are however several underdeveloped cyber deterrence research silos that have distinctly different views on the topic, such as the field of criminology (tackling cybercrime), psychology (defending against information warfare), intelligence studies (curbing digital espionage), and the computer sciences (mitigating system vulnerabilities and network disruptions).

[31]Denning 2015; Lindsay 2015; Nye 2016/2017; Kello 2017; Tor 2015; Harknett and Nye 2017. Also see William 2017; Harknett and Fischerkeller 2017; Brantly 2018.

[32]Discussion and table based on Smeets and Lin 2018a.

[33]The scholars note that "Studies of 'cyber deterrence' raise as many problems as would be raised by a comparable study of 'land deterrence'." Denning 2015.

[34]For a similar classification, see Nye 2016/2017; for a general description, see the Preface by Osinga and Sweijs in the present volume.

Table 20.1 Overview of arguments on the potential to deter cyber attacks

Scholarship	Arguments
Denning 2015	Same problems for CD as for conventional deterrence. Potential for CD through existing regimes
Gartzke and Lindsay 2015	CD suffers from problems of rationality, attribution, and secrecy. This means we have to instead focus on deception as distinct strategy
Tor 2015	We should move from 'absolute' CD to 'cumulative' CD, which is restrictive and continuous in nature
Stevens and Muller 2017	(NATO) CD seems to be viable. Yet, it should be viewed as a cumulative process, beyond military
Sulmeyer 2017	CD might be possible in theory. However, we are still unclear what activity to deter, and which tools to use to impose costs
Kello 2017	CD does not work as a strategy, but we should aim for punctuated CD instead: we should not deter individual actions but a series of actions
Healey 2017	CD is still working on the high-end—yet, nations show limited restraint. It is the aspect of 'constant cyber activity' which causes problems
Nye 2017	Conventional CD is difficult. Instead, we should focus on deterrence by economic entanglement and norms to overcome barriers
Harknett and Fischerkeller 2017	CD is impossible due to the structure of cyberspace. We need to move away from the deterrence paradigm and consider different forms of strategy
Brantly 2018	Absolute deterrence may not be possible—but a form deterrence as in criminology might be. We need to move away from deterrence only by punishment and denial

(*Source* Smeets and Lin 2018a, p. 62)

network penetration, and thus influence the cost-benefit calculations of an adversary to the degree that it either disincentives an attack or grinds an attacker to halt over time. Second, *deterrence by punishment* seeks to discourage the adversary from attacking, recognizing the costly consequences following their actions outweigh the benefits. We have seen variations of this logic being proposed as well. According to Lucas Kello, instead of trying to deter individual acts, countries should go for punctuated deterrence: "a series of actions that generate cumulative effect, rather than tit for tat response".[35] Third, *deterrence by entanglement* rests on the unresolved discussion in international relations theory on whether state-to-state interdependence mitigates interstate conflict. Fourth, *deterrence by de-legitimization* focuses on the creation of norms and rules for state behaviour in cyberspace, will over time translate into a general principle of restraint, raise the reputational costs of bad behaviour, and shrink the battlespace to only encompass military combatants.

[35]Kello 2017.

The third group (denoted in the table in white) argues that cyber deterrence is not possible. At least not in the way that the first two groups tend to believe. Jon Lindsay and Erik Gartzke, for example, put forward the idea of a comprehensive deception strategy—both on offense and defence—because the cyber domain is "a global network of gullible minds and deterministic machines."[36] In contrast Harknett and Fischerkeller make the case that the unique characteristics of cyberspace "[demand] a unique strategy, a capabilities-based strategy of cyber persistence," whose goal it is "to remove the escalatory potential from adversarial action".[37]

20.4 The Future

Figure 20.1 suggests that the writing and thinking about cyber deterrence is slowly falling out of fashion among scholars. This could be for at least three reasons: (i) everything has been said already;[38] (ii) the concept of deterrence is misapplied in cyberspace, or (iii) other strategic concepts are gaining more prominent attention. Likely a mix of these causes, it is unlikely this trend reverses itself anytime soon. Instead, we expect the debate to fork into four directions, which—although distinct and separate—do not mutually exclude each other.

The first direction will seek to increasingly incorporated cyber deterrence as an element within the broader international security and contest in a multi-domain world. Aaron Brantly for example argued back in 2018 that the main challenge of the future is not to define deterrence in cyberspace, but to "*understand the role digital technologies play in the broader scope of interstate deterrence*".[39] A recently published edited volume of Jon Lindsay and Erik Gartzke on *Cross-Domain Deterrence* has also already moved in this direction. As the scholars write, "cross-domain deterrence is not new today, but its relevance is increasing. Strategic actors have long combined capabilities or shifted domains to make coercive threats or design around them […] As a larger and more diverse portfolio of tools available for coercion complicates strategic choices, a better understanding of [cross-domain deterrence] becomes a critical asset for effective national security strategizing."[40]

Given the technical nature of the cyber domain, the second direction will primarily focus on deterrence effects that can be achieved on the operational and tactical level. Currently, there are numerous practical obstacles that hinder scholars

[36]Gartzke and Lindsay 2015.

[37]Harknett and Fischerkeller 2017.

[38]We consider this reason to be least likely given that nuclear deterrence continues to be a prolific research area despite the numerous articles published in the field over the past decades.

[39]Brantly 2018.

[40]Lindsay and Gartzke 2019, pp. 333–335; also see Futter 2018.

and strategists to explore this route, including: highly classified documents, non-access to cyber operators, and the embryonic stage of existing military cyber organizations. Over time, we expect those hurdles to slowly melt away to the extent that operational and tactical know-how on how cyber operators actually defend, fight, and win in cyberspace will increasingly make its way into open source.[41] Insights into this ground game, will also highly likely lead to a better understanding on how escalation dynamics work in cyberspace and what psychological effects can and cannot be created.

The third direction seeks to shift the attention away from deterrence, towards the other form of coercion: compellence.[42] Compellence refers to an action that persuades an adversary to stop or change an action. Compellence is conventionally considered to be more difficult. When the actor changes behaviour, there are often reputational costs. In this respect, offensive cyber operations may come with an advantage: "Its effects do not necessarily have to be exposed publicly, which means the compelled party can back down post-action without losing face. More specifically, the compelled actor can deny that the effect was caused by OCC.I[43] There are also more opportunities to reverse the effects of cyber operations, which may further encourage compliance.[44]

The final direction will explore strategic concepts that seeks to contain and blunt adversarial aggression in cyberspace that stands apart from traditional deterrence thinking. Persistent engagement is a first step into this direction—a concept also adopted by the US Cyber Command in their 2018 'Vision' document entitled "Achieve and Maintain Cyberspace Superiority".[45] Early contours of this concept are found in a 2016 article by Richard Harknett and Emily Goldman, talking about an "offense-persistent strategic environment" in which "the contest between offense and defence is continual [and] the defence is in constant contact with the enemy".[46] Harknett and Michael Fischerkeller further refined the idea a year later, arguing that "in an environment of constant contact, a strategy grounded in persistent engagement is more appropriate than one of operational restraint and reaction for shaping the parameters of acceptable behaviour and sustaining and advancing U.S. national interests."[47] Underlying this move away from deterrence thinking is a belief that the literature paid too much attention to the 'the high-and-right' cyber equivalent to an armed attack—that is, the concept of 'cyberwar', ignoring the fact that the actual behaviour of actors in cyberspace has been of a far more nuanced nature. As

[41]There is also the opportunity for more game theoretical modeling at this level. For an initial analysis, see Axelrod and Iliev 2014. For an overview, see Smeets and Work 2020.

[42]Schelling 1966.

[43]Smeets and Lin 2018a, p. 64.

[44]Ibid.

[45]United States Cyber Command 2018. For a summary, see Harknett 2018. For critical assessments, see Healey 2018; Healey 2019; Smeets and Lin 2018b; Schneider 2019; Smeets 2020.

[46]Harknett and Goldman 2016, p. 15.

[47]Fischerkeller and Harknett 2017, p. 381.

Harknett and Smeets wrote in a 2020 *Journal of Strategic Studies* article, "what has emerged are campaigns comprised of linked cyber operations, with the specific objective of achieving strategic outcomes without the need of armed attack".[48]

It is also likely we will see the emergence of alternative strategic concepts, beyond persistent engagement. Analysts from European states can be expected to promote ideas that stand in stark contrast to U.S. thinking. While most European states have absorbed early U.S. thinking of cyberspace being a warfare domain and the need for cyber deterrence, European policymakers are uncomfortable with adopting much less discussing persistent engagement, as it is perceived as overly aggressive. Similarly, most European military cyber organizations will not be able to increase their operational capacities to such a degree that they can navigate "seamlessly, globally, and continuously", as persistent engagement demands. Recognizing these limitations, EU member states will have to fill this strategic vacuum with creative conceptual thinking.

20.5 Conclusion

The purpose of this chapter was to situate the current debate on cyber deterrence within the historical evolution of deterrence thinking in cyberspace, clarify the existing conceptualizations, and comprehensively discuss whether the concept of cyber deterrence has an analytical future. Born in the 1990s, the thinking on cyber deterrence was nurtured by the U.S. Department of Defense in numerous war-gaming exercises. Hitting puberty in the aftermath of the distributed denial-of-service campaign against Estonia in 2007, we showed in this chapter that cyber deterrence matured after Stuxnet and received peak attention from policymakers and academics from 2013 to 2016 during the golden age of 'cyberwar' scholarship. Yet, it also became clear that, from 2016 onward, the interest in cyber deterrence started to fade to the extent that it is now intentionally neglected.

We argued that the future deterrence debate can move into four directions: increased incorporation of cyber deterrence as an element within the broader international security and contest in a multi-domain world. A deeper focus on the technical aspects of the cyber domain to achieve deterrence effects on the operational and tactical level. A closer analysis of compellence, as the alternative form of coercion. And an exploration of new strategic concepts that seeks to contain and blunt adversarial aggression in cyberspace that stands apart from traditional deterrence thinking.

In contrast to the evolution of deterrence theory in realspace, which has moved along four (respectively five) distinctive waves, the evolution of cyber deterrence is to some degree schizophrenic. Theory-wise it is still stuck between the first and second wave—due to absence of large empirical datasets and comprehensive case studies. As

[48]Harknett and Smeets 2020, p. 1.

a result, the three groups of scholars outlined in Table 20.1, are still interlocked in a disagreement on the very fundamentals of deterrence thinking in the cyber domain. Meanwhile, mechanism-wise, cyber deterrence is seen as an inherent part of the fourth (deterring asymmetric threats) and fifth deterrence wave (resilience and cross-domain integration). To reconcile this schizophrenic approach, scholars and practitioners need to figure out whether cyberdeterrence mechanisms can actually work without having a firm grasp on cyber deterrence theory, and whether cyber deterrence theory is actually based on evidence collected from the cyber domain rather than deduced from known behavioural outcomes in realspace. Answers to these questions will likely be found within the three future directions we have outlined.

References

Arquilla J, Ronfeldt D (1993) Cyberwar is Coming! Comparative Strategy, 12.2:141–165

Axelrod R, Iliev R (2014) Timing of Cyber Conflict. PNAS, 111.4:1298–1303

Betz D J, Stevens T (2011) Cyberspace and the State: Towards a Strategy for Cyber-Power. Adelphi Series 51:424

Borghard E D, Lonegran S W (2017) The Logic of Coercion in Cyberspace. Security Studies 26:3 452–481

Brantly A, Smeets M (n.d.) Military Cyber Operations. In: McD Sookermany A (ed) Handbook of Military Sciences. Forthcoming, Springer

Brantly AF (2018) The Cyber Deterrence Problem. 2018 10th International Conference on Cyber Conflict, CyCon X: Maximising Effects. https://ccdcoe.org/uploads/2018/10/Art-02-The-Cyber-Deterrence-Problem.pdf. Accessed 14 April 2020

Broder J M (1990) U.S. War Plan in Iraq: 'Decapitate' Leadership: Strategy: The Joint Chiefs believe the best way to oust the Iraqis would be air strikes designed to kill Hussein. https://www.latimes.com/archives/la-xpm-1990-09-16-mn-1221-story.html. Accessed 14 April 2020

Byman D, Waxman M C (2001) The Dynamics of Coercion: American Foreign Policy and the Limits of Military Might. Cambridge University Press, New York

Clarke R, Knake R (2010) Cyber War: The Next Threat to National Security and What to Do About It. Harper Collins Publishers

Denning D E (2015) Rethinking the Cyber Domain and Deterrence. Joint Forces Quarterly 77:8–15. https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-77/Article/581864/rethinking-the-cyber-domain-and-deterrence/. Accessed 14 April 2020

Derian J D (1994) Cyber-deterrence. https://www.wired.com/1994/09/cyber-deter/. Accessed 14 April 2020

Fischerkeller M, Harknett R J (2017) Deterrence is not a credible strategy for cyberspace. Orbis, 61:381–393

Futter A (2018) Hacking the Bomb: Cyber Threats and Nuclear Weapons. Georgetown University Press, Washington, D.C.

Gartzke E (2013) The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. International Security, 38.2:41–73

Gartzke E, Lindsay R J (2015) Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace. Security Studies 24(3):316–348

Harknett R J (1996) Information Warfare and Deterrence. Parameters, 26:3

Harknett R J (2018) United States Cyber Command's New Vision: What It Entails and Why It Matters. Lawfare. www.lawfareblog.com/united-states-cyber-commands-new-vision-what-it-entails-and-why-it-matters. Accessed 14 April 2020

Harknett R, Fischerkeller M P (2017) Deterrence is Not a Credible Strategy for Cyberspace. Orbis 61:381–393.
Harknett R J, Goldman E (2016) The search for cyber fundamentals. Journal of Information Warfare. https://www.jinfowar.com/journal/volume-15-issue-2/search-cyber-fundamentals. Accessed 14 April 2020
Harknett R J, Nye J S (2017) Is Deterrence Possible in Cyberspace? International Security, 42.2:196–199
Harknett R J, Smeets M (2020) Cyber campaigns and strategic outcomes. Journal of Strategic Studies 1–34
Healey J (2017) Cyber Deterrence Is Working – So Far. Cypher Brief. https://www.thecipherbrief.com/cyber-deterrence-is-working-so-far. Accessed 14 April 2020
Healey J (2018) Triggering the New Forever War, in Cyberspace. Cipher Brief. www.thecipherbrief.com/triggering-new-forever-war-cyberspace. Accessed 14 April 2020
Healey J (2019) The implications of persistent (and permanent) engagement in cyberspace, Journal of Cybersecurity, 5:1
Henderson SJ (2007) The Dark Visitor: Inside the World of Chinese Hackers. Available from https://www.lulu.com/shop/scott-henderson/the-dark-visitor-ebook/ebook/product-2420426.html
Kello L (2017) The Virtual Weapon and International Order. Yale University Press, Yale
Keuhl DT (2002) Information Operations, Information Warfare, and Computer Network Attack, Their Relationship to National Security in the Information Age. In: Schmitt MS, O'Donnell BT (eds) Computer Network Attack and International Law. Naval War College Press
Lapsley P (2013) Exploding the Phone: The Untold Story of the Teenagers and Outlaws Who Hacked Ma Bell. Grove Press
Libicki MC (2009) Cyberdeterrence and Cyberwar. RAND Corporation, Santa Monica, CA p. xii-xvii Libicki MC (2012) Crisis and Escalation in Cyberspace. RAND Corporation, Santa Monica, CA
Libicki MC (2012) Crisis and Escalation in Cyberspace. RAND Corporation, Santa Monica, CA
Liff A P (2012) Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War. Journal of Strategic Studies, 35.3:401–428
Lindsay J R (2015) Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack. Journal of Cyber Security, 1.1:53–67
Lindsay J R, Gartzke E (2019) Cross-Domain Deterrence: Strategy in an Era of Complexity. Oxford University Press
Mitnick K (2012) Ghost in the Wires: My Adventures as the World's Most Wanted Hacker. Little Brown and Company
Molander R C, Riddile A S, Wilson P A (1996) Strategic Information Warfare: The New Face of War. RAND
Ney J S Jr. (2016/2017) Deterrence and Dissuasion in Cyberspace. International Security 41.3:44–71
Nichiporuk B (1999) US Military Opportunities: Information-warfare Concepts of Operation. In: Khalizah Z, White J (eds) The Changing Role of Information in Warfare. RAND Corporation, p. 193
Rid T (2012) Cyber War Will Not Take Place. Journal of Strategic Studies, 35.1:5–32
Ronfeldt D, Arquilla J (eds) (1996) Implications for US Doctrine and Strategy. The Advent of Netwars. https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR789/MR789.ch6.pdf. Accessed 14 April 2020
Ronfeldt D, Arquilla J (1999) What Next for Networks and Netwars. In: Ronfeldt D, Arquilla J (eds) Networks and Netwars: The Future of Terror, Crime, and Militancy. RAND, Santa Monica CA, p 532. https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch10.pdf. Accessed 14 April 2020
Sartori G (1970) Concept Misinformation in Comparative Politics. The American Political Science Review, 64.4:1033–1053
Schelling TC (1966) Arms and Influence. Yale University Press, New Haven

Schneider JG (2019) Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy. *Lawfare*. https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy. Accessed: 14 April 2020

Shires J, Smeets M (2016) What Do We Talk About When We Talk About 'Cyber'? SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2860839. Accessed 14 April 2020

Slatalla M, Quittner J (1994) Gang War in Cyberspace. Wired. https://www.wired.com/1994/12/hacker-4/. Accessed 14 April 2020

Smeets M (2018) The Strategic Promise of Offensive Cyber Operations. Strategic Studies Quarterly, 12.3:90–113

Smeets M (2020) U.S. cyber strategy of persistent engagement & defend forward: implications for the alliance and intelligence collection. Intelligence and National Security, 2:444–453

Smeets M, Gorwa R (2019) Cyber Conflict in Political Science: A Review of Methods and Literature. SocArXiv Papers. https://osf.io/preprints/socarxiv/fc6sg. Accessed 14 April 2020

Smeets M, Lin H (2018a) Offensive Cyber Capabilities: To What Ends? In: Minárik T, Jakschis R, Lindström L (eds) 2018 10th International Conference on Cyber Conflict, CyCon X. NATO CCD COE Publications, Tallinn

Smeets M, Lin H (2018b) What Is Absent From the U.S. Cyber Command 'Vision'. Lawfare. https://www.lawfareblog.com/what-absent-us-cyber-command-vision. Accessed 14 April 2020

Smeets M, Work J D (2020) Operational Decision-making or Cyber Operations: In Search of a Model. Cyber Defense Review 95–112

Stevens T, Muller LP (2017) Upholding the NATO cyber pledge. Cyber Deterrence and Resilience: Dilemmas in NATO defence and security politics. Norwegian Institute of International Affairs, Policy Brief 5/2017. https://nupi.brage.unit.no/nupi-xmlui/handle/11250/2442559. Accessed 14 April 2020

Sulmeyer M (2017) Which Cyberattacks Should the United States Deter, and How Should It Be Done? CFR. https://www.cfr.org/blog/which-cyberattacks-should-united-states-deter-and-how-should-it-be-done. Accessed 14 April 2020

Theohary C A (2018) Information Warfare: Issues for Congress. https://fas.org/sgp/crs/natsec/R45142.pdf. Accessed 14 April 2020

Tor U (2015) 'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence. Journal of Strategic Studies, 40.1–2:92–117

United States Cyber Command (2018) Achieve and Maintain Cyberspace Superiority. https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM-23-Mar-18.pdf. Accessed 14 April 2020

Wheatley G F, Hayes R E (1996) Information Warfare and Deterrence. NDU Press

William B D (2017) Meet the scholar challenging the cyber deterrence paradigm. The fifth domain. https://www.fifthdomain.com/home/2017/07/19/meet-the-scholar-challenging-the-cyber-deterrence-paradigm/. Accessed 14 April 2020

Stefan Soesanto is a Senior Researcher in the Cyberdefense Project with the Risk and Resilience Team at the Center for Security Studies (CSS) at ETH Zurich.

Max Smeets is senior researcher at the Center for Security Studies (CSS) at ETH Zurich. He is also an Affiliate at Stanford University Center for International Security and Cooperation and Research Associate at the Centre for Technology and Global Affairs, University of Oxford, UK.

Chapter 21
New Technologies and Deterrence: Artificial Intelligence and Adversarial Behaviour

Alex Wilner and Casey Babb

Contents

Abstract Offering a critical synthesis of extant insights into technological developments in AI and their potential ramifications for international relations and deterrence postures, this chapter argues that AI risks influencing military deterrence and coercion in unique ways: it may alter cost-benefit calculations by removing the fog of war, by superficially imposing rationality on political decisions, and by diminishing the human cost of military engagement. It may recalibrate the balance between offensive and defensive measures, tipping the scales in favour of pre-emption, and undermine existing assumptions imbedded in both conventional and nuclear deterrence. AI might altogether remove human emotions and eliminate other biological limitations from the practice of coercion. It may provide users the ability to collect, synthesize, and act upon real-time intelligence from several disparate sources, augmenting the certainty and severity of punishment strategies, both in theatre and online, compressing the distance between intelligence, political

A. Wilner (✉) · C. Babb
The Norman Paterson School of International Affairs, Carleton University, Ottawa, Canada
e-mail: alex.wilner@carleton.ca

C. Babb
e-mail: caseybabb3@cmail.carleton.ca

F. Osinga and T. Sweijs (eds.), *NL ARMS Netherlands Annual Review of Military Studies 2020*, NL ARMS, https://doi.org/10.1007/978-94-6265-419-8_21

decisions, and coercive action. As a result, AI may quicken the overall pace of action across all domains of coercion, in conflict, crisis, and war, and within the related subfields of national security, counterterrorism, counter-crime, and counter-espionage.

Keywords Artificial intelligence · pre-emption · human emotions · instability · hyper-coercion · autonomous weapon systems

21.1 Introduction

Artificial Intelligence (AI) is influencing national defence in several important ways. It alters the way states plan and conduct military engagements, collect and use intelligence, and protect their domestic national security. Traditional notions of state power are also increasingly intertwined with national expertise and investment in AI; an arms race is thought to be developing between the United States and China as a result. And in some states, private sector AI research is increasingly pitted against the defence sector's interest in integrating AI into national security; ethical considerations abound. Despite these developments, researchers have yet to fully explore the way AI intersects with deterrence. The academic literature on the subject is particularly slim; very few studies have yet to unpack the various ways in which the technology might intersect with deterrence logic, theory, and practice writ large.[1] The dearth of knowledge is surprising given the expectation that the future of defence will likely be autonomous.[2] As this chapter will show, AI risks influencing military deterrence and coercion in unique ways: it may alter cost-benefit calculations by removing the fog of war, by superficially imposing rationality on political decisions, and by diminishing the human cost of military engagement. It may recalibrate the balance between offensive and defensive measures, tipping the scales in favour of pre-emption, and undermine existing assumptions imbedded in both conventional and nuclear deterrence. AI might altogether remove human emotions and eliminate other biological limitations from the practice of coercion. It may provide users the ability to collect, synthesize, and act upon real-time intelligence from several disparate sources, augmenting the certainty and severity of punishment strategies, both in theatre and online, compressing the distance between intelligence, political decisions, and coercive action. As a result, AI may quicken the overall pace of action across all domains of coercion, in conflict, crisis, and war, and within the related subfields of national security, cybersecurity, counterterrorism, counter-crime, and counter-espionage.

This chapter is an exercise in structured speculation: given what we know about the current state of the technology underpinning artificial intelligence and machine

[1]The recent exceptions include: Huh Wong et al. 2020; Wilner 2019; Horowitz 2019.

[2]Coker 2015; Scharre 2018b; Wittes and Blum 2015.

learning, and related innovations, what does the future of deterrence in the 21st century look like?[3] How will the use of AI in military and strategic affairs, counterterrorism, intelligence, and national security alter the way states practice deterrence? The chapter builds on Professor Wilner's previous research on updating deterrence theory for non-traditional threats,[4] but is also largely derived from the authors' ongoing research program on *AI Deterrence*.[5] The larger goal of the *AI Deterrence* project is to provide a systematic theoretical and empirical overview of how AI influences the practice of coercion, deterrence, compellence, denial, and influence across various domains, both in physical and cyber space, and across the disciplines (e.g. Criminology, IR, Terrorism and Intelligence Studies). The purpose of this chapter is more narrowly focused on exploring the way AI might intersect with interstate military deterrence and coercion more specifically. The chapter unfolds in six sections. Sections one to five explore several different ways in which AI and deterrence intersect, with specific discussions on hyper-war and hyper-coercion, scientific development and commercialization, autonomous weapons systems and tactical innovation, ethical constraints and asymmetries, and coercive credibility. The concluding section suggests avenues for further research on developing and empirically testing AI deterrence theory.

21.2 The Promises and Pitfalls of Hyper-Coercion

AI will shorten the distance from intelligence gathering and assessment to decision-making and coercive action. It will do so by making better sense of huge amounts of data, detecting minute anomalies in adversarial behaviour, automating physical and cyber tasks, and providing super-human speed, precision, reliability, patience, and vigilance.[6] On the question of intelligence assessment, Boaz Ganor explains that rather than making the intelligence officer's role redundant, AI makes their "work significantly more efficient". He illustrates how AI will help human

[3]Some authors are less sanguine about the utility AI will have in national security, suggesting the current technology is easily duped, spoofed, or exploited, does not easily lend itself to very simple cross-domain tasks, and cannot often explain how outputs were produced. Other scholars note that technological innovation does not necessarily lead to conflict escalation and novel deterrence outcomes. Horowitz 2018c; Altmann and Sauer 2017, pp. 119–120; Talmadge 2019, pp. 867–869.

[4]Wilner and Wenger 2021; Wilner 2015; Wenger and Wilner 2012; Wilner 2020; Long and Wilner 2014.

[5]The project received two grants from Canada's Department of National Defence's Innovation for Defence Excellence and Security (IDEaS) program (2018/19, and 2020/2021), and a third from DND's Mobilizing Insights in Defence and Security (MINDS) program (2019/2020).

[6]Horowitz et al. 2018.

analysts make better sense of data, highlighting important (but obscure) relationships between singular points of information.[7] It will help turn disparate pieces of information into intelligence quickly, useful to decision-makers and soldiers on the frontline alike. For similar reasons, AI might likewise improve a state's capacity in military planning, logistics, communications, recruitment, training, deployment, and so on. The back-office AI that better coordinates the machinery of warfare may make some especially complex coercive threats—like largescale international military operations—more robust, persuasive, and feasible. The automation of live-data analysis will provide states and militaries with an exploitable advantage over adversaries. Together, these factors may lead to "hyperwar", in which data will be "sifted in near real time—if not eventually in real time", providing decision-makers with greater awareness and more options far more quickly.[8]

The factors encouraging hyperwar may lend themselves to the development of hyper-coercion: the ability to foresee and forestall an adversary's next move. In the near term, by providing decision-makers with alternative tactical and strategic options based on a wide-ranging assessment of an unimaginably large trove of data and intelligence, AI may convince decision-makers to delegate some tasks (including targeting) to machines under specific time-sensitive conditions and constraints, ultimately forcing some states to re-evaluate current military assumptions, narratives, and plans regarding automation in warfare. In the long term, by providing unique advice to decision-makers that supersedes human innovation, AI may prove its value in providing situational awareness that dips into *predictive* analytics.[9] By melding an improved analysis of what adversaries have done in the past to what they are currently doing today (indeed, this very minute), AI may provide users with the ability to anticipate an adversary's next move; defenders can pre-emptively respond accordingly and influence and deter adversarial behaviour to their liking.[10] Over time, once a challenger comes to believe that a defender can rely on sophisticated AI to properly anticipate its behaviour, it may be altogether dissuaded from pursuing certain actions. Something akin to AI-enhanced general deterrence might result.

Conversely, hyperwar and hyper-coercion may lead to deterrence failure and strategic instability instead. At least five dilemmas present themselves. First, on this theme, the RAND Corporation held several workshops in 2017 exploring future U.S. security challenges, circa 2040, illustrating the way AI might interfere with strategic (i.e. nuclear) deterrence.[11] They argue that if AI creates the perception among nuclear states that one country has the ability to detect, locate, and target all of another state's nuclear weapon launchers—an infeasibility today but a possibility tomorrow given technological developments—then vulnerable states may be

[7]Ganor 2019.

[8]West and Allen 2018.

[9]Morstatter et al. 2019.

[10]Lappin 2017; Solls 2020.

[11]Geist and Lohn 2018.

especially inclined to use these weapons more quickly at the risk of losing them altogether.[12] Other states may calculate that many more such weapons may be needed to offset an adversary's ability to locate and target stockpiles, leading to an increase in both horizontal and vertical nuclear proliferation.

Second, as Keith Payne argues, AI will "change power balances" between rivals and should, all told, favour offence over defence, given the technology's "speed, precision, and acquisition and analysis of unbiased … knowledge".[13] These conditions may bolster deterrence by punishment strategies over deterrence by denial, in a repeat of Cold War dynamics.[14]

Third, letting machines dictate the speed of warfare may inadvertently augment the effect of minor algorithmic glitches, inviting the development of accidental, and entirely AI-generated, deterrence failures.[15] Within an environment in which both challengers and defenders come to rely on AI to help guide behaviour, the systems themselves will interact with each other in unique (and uncertain) ways. Autonomous but unintended chain reactions may result; think of the market's "flash crash" in 2010. The equivalent might be an unwanted "flash war" in either physical or digital space, an unintended conflict that results from the cascading effects of automated processes and responses between two opposing AIs. This is precisely the future scenario Matthew Price and colleagues contemplate, fictionalizing a two-hour long, AI-triggered war between the U.S. and China (circa 2024).[16] As the RAND study cautions, the conflagration ends in unintended and avoidable nuclear exchange. Price et al. use the narrative to explore how human decision-makers, who they suggest are "poor judges of risk under complexity", might come to inherently rely on AI advice in order to ameliorate the "time pressures" endemic to periods of crisis. They note that deterrence, when put into practice, takes "the mind of the adversary", and their "motivation" into consideration, such that failures of deterrence are failures "to understand an adversary". By replacing human rationality with opaque computations of what human rationality looks look, AI risks obfuscating and undermining the traditional deterrence process.

Fourth, fighting at "machine speed" may change the calculus of taking action. If AI-based decision-making provides one side of a conflict an advantage in responding quickly and decisively, then others, where and when feasible, will eventually mimic and come to rely on these processes, too. But as both sides of a contest come to rely on machines for insights, the very rationale of these AI-generated insights may degrade more quickly over time, as one side's AI responds and reacts to another's, at a speed beyond human capacity (or control). Put

[12]For a similar argument centred on the effects of "non-kinetic left-of-launch capabilities" (i.e. cyber and missile defence) on the stability of current nuclear deterrence structures, see Wasson and Bluesteen 2018.

[13]Payne 2018a.

[14]Wilner and Wenger 2021.

[15]Scharre 2018a, b.

[16]Price et al. 2018, pp. 92–105.

another way, an AI-generated insight may have a short shelf life, and windows of opportunity may prove fleeting. If so, the logic and value of striking first, and fast, may prevail, upending long-standing coercive and escalatory calculations.

Finally, correctly gauging a country's prowess in AI is open to misinterpretation, inviting coercive miscalculation along the way. A challenger, looking in, may be unable to properly gauge an adversary's power when that power is itself derived from AI. Compared to traditional notions of power—like economic output, military leadership, or type and number of armaments—AI power is less measurable. If a challenger does not know what a defender is capable of, it may have less reason to restrain its behaviour. The conundrum, however, is that from a signalling perspective, even if a defender wanted to, it would be hard-pressed to accurately and clearly communicate its AI capability. How do you communicate a capability when that capability is a computer program?[17] Sharing the contents of an especially potent algorithm with an adversary to prove a point is a non-starter. If AI is to have a coercive effect, defenders will have to find creative ways to demonstrate or signal their capability, otherwise they invite adversarial miscalculation and, in certain cases, avoidable deterrence failures.

21.3 Commercial Dual-Use AI as Coercive Offset

AI is not a weapon; it is a technology with myriad and diverse uses. Michael Horowitz categorizes AI as the "ultimate enabler", an all-purpose "technology with a multitude of applications".[18] While it will certainly prove useful to states and militaries engaged in conflict and warfare, AI's development is largely driven by other, often commercial, functions. And unlike other technological innovations that have weighed upon deterrence theory and practice over the century (i.e. nuclear weapons, submarines, ballistic missiles, missile defence), AI is a general-use technology largely driven by software developments and data collection. Competition for AI excellence will be broad as a result, uniquely combining the efforts of countries and corporations alike.[19] Horowitz argues further that the way AI develops in the coming years will help dictate the utility and advantage it might lend to its early military adopters. If AI advancements are led by the private sector, for instance, AI might more quickly "diffuse" to militaries around the world, who purchase it for their own use. That would reduce the original developer's "first-mover advantage", and could narrow the balance of power between innovators, purchasers, and adopters. But, conversely, if AI—or certain types of AI useful to defence—is developed primarily by states, government laboratories, and their

[17]With thanks to the participants of the AI Deterrence Stakeholder Meeting, May 2019, Ottawa, Canada.

[18]Horowitz 2018a.

[19]Horowitz 2018b.

militaries, the technology will be slower to spread between countries because of market restrictions, and innovators may retain a technological edge that translates into a longer-lasting coercive advantage. And yet, to date, there is no public evidence suggesting that any military in the world controls cutting-edge AI more sophisticated than that which is being developed or employed by leading technology firms, like Google or SenseTime.[20] Private tech appears to be leading the way.

These assertions are explored further by M. L. Cummings, who suggests that private sector innovation in AI currently has the advantage because top engineering talent find more lucrative careers in the commercial applications of AI than they do in the more narrowly-focused aerospace and defence industry. This is especially true in the U.S., Canada, and Europe. "The global defence industry", she warns, "is falling behind its commercial counterparts in terms of technology innovation".[21] Bridging the gap may be difficult. This sentiment is shared by Lieutenant General John Shanahan, Director of the U.S. Joint Artificial Intelligence Centre (JAIC), who explained in 2019 that unlike other forms of dual-use technology, "the barriers to entry" for AI are low. Shanahan explains:

> Unlike most big weapon systems … that were dominated by the Defence Industrial Base, many if not almost all AI-enabled capabilities start in commercial industry. We are seeing a true democratization of technologies that, like so many other emerging technologies in history, are as capable of being used for bad as they are for good. It is going to be increasingly difficult to prevent the use of AI-enabled capabilities by those who are intent in causing harm.[22]

The commercialization of AI presents traditionally weak states with a strategic (and coercive) opportunity. The dual-use nature of AI along with private-sector developments in the technology, suggests that smaller states and non-state actors, too, may eventually be able to purchase the technology for their own use. While weak actors may face other limitations, like acquiring access to appropriate training data, AI might nonetheless help level the playing field with more powerful actors. If so, diffusion of the technology may diminish how the strong deter or compel the weak, and might otherwise provide the weak with new avenues for coercing the strong. The weak can leverage the widespread availability of AI tools and techniques to develop new and imaginative ways to coerce, counter-coerce, or altogether defeat traditionally stronger military adversaries. Imagination and a willingness to experiment with AI at both the tactical and strategic level will prove useful here.

For illustration, Alina Polyakova's introduces "AI-driven asymmetric warfare". With Russia in mind, she shows how weaker adversaries might "co-opt existing commercially available" AI technology to challenge stronger states with AI-enhanced cyberattacks and AI-generated disinformation campaigns. She

[20]Author Interview, Brookings Institution, Washington DC, January 2019.

[21]Cummings et al. 2018.

[22]Rassler 2019.

suggests that "deep fake" technology—which allows a user to swap one person's face for another in synthetic video content[23]—can produce highly realistic and customized content useful for strategically shifting narratives and perceptions in target societies and (when done right) changing individual and government behaviour. By manipulating public information through deep fakes and other related processes, AI might provide users with new forms of deterrence by delegitimization.[24] The threat, in this case, is the ability to create, release, and disseminate fake video or audio material threatening or embarrassing to a target. Think of Russia surreptitiously threatening a U.S. congressional or presidential nominee with engineered content that could influence the candidate's standing among the electorate. Because determining the veracity of AI-manipulated content and attributing its source is difficult to do, countering these types of coercive misinformation campaigns may prove difficult.[25] Or consider other as-of-yet developed but no less unique applications for AI in physical space. Autonomous CBRN weapons—aerial or underwater "doomsday" drones—could be deployed by a weaker state to dissuade a stronger challenger from launching a debilitating first strike, augmenting the credibility of new-age second strike weapons.[26] Fanciful, perhaps, but worth imagining in both theory and practice when contemplating the future of deterrence.

21.4 Autonomous Weapons and the Advent of Saturation Tactics

If AI is narrowly defined as "machine learning", then it might be argued that some militaries have been using AI techniques and statistical learning models for years in order to improve weapons and signal processing systems. The difference today, however, is the dramatic improvement in the quantity of data and quality of processing power available for use. Countries or militaries that can combine these two elements will broaden the boundaries of what they can currently accomplish with AI technology, likely acquiring a noticeable (and potentially significant) edge over adversaries and allies alike.[27] Of all the debates surrounding AI and warfare, greatest popular and media concern is reserved for Lethal Autonomous Weapons Systems (LAWS). For the latest popular iteration of this movement, simply Google "Slaughterbots". By broadest definition, critics present LAWS as any weapon platform that has the ability to select, target, and engage an adversary

[23]Wilner et al. 2019.

[24]For an exploration of *deterrence by delegitimization*, see Long and Wilner 2014.

[25]Knight 2018.

[26]Geist and Lohn 2018.

[27]Author Interview, Brookings Institution, Washington DC, January 2019.

autonomously.[28] While important ethical, practical, and legal concerns have been levied against fully autonomous offensive weapons,[29] the purpose of this chapter is centred on exploring the coercive effect, rather than the moral consequence, of AI, including those married to robotic systems.

For clarity, weapon systems can be provided different levels of autonomy. As Scharre describes in *Army of None*, if a human remains "in the [Observe, Orient, Decide, Act (OODA)] loop deciding which target(s) to engage", the system in question should be considered a semiautonomous weapon. In this case, the search and detection of a target may be autonomous, but a human decides to engage and destroy a target. Contemporary drone warfare follows this pattern of behaviour. Conversely, with autonomous weapon systems, the entire process of identifying, detecting, and engaging a target is done autonomously. That is the battlefield of the near future. Yet even here, autonomous weapons can be further sub-subdivided. On one hand, *supervised* autonomous weapons, like those widely used to defend naval ships, bases, and other potential targets from missile or rocket attack, engage autonomously with a target (usually an incoming projectile), though humans remain in the loop and supervise the weapon's use. A human can intervene if and where needed. *Fully* autonomous systems, on the other hand, perform the entire decision process autonomous and human intervention is not possible. Using the loop analogy, Daniel Hoadley and Nathan Lucas (and others) suggest that humans can be *in* the loop (semi-autonomous), *on* the loop (human supervised autonomous systems), and *out* of the loop (fully autonomous systems).[30]

While Scharre argues that very few contemporary weapon systems have crossed into the fully autonomous category, some have, and more are expected to.[31] Contemporary examples include the Israeli Aerospace Industries' Harpy—a drone-like weapon that can loiter above a prescribed location for hours until it engages with a specific target. As Scharre explains, while a human decides to launch the Harpy in order to "destroy any enemy radars" within a proscribed geographic area and timeframe, the Harpy itself "chooses the specific radar it destroys".[32] In this case, the human does not know in advance, even when launching the weapon, which specific target the weapons will choose to destroy; the weapon determines who to kill. There is a distinction, then, between a machine ordered by a human to target something or kill someone, and a machine deciding on its own to target something or kill someone. At issue, for both opponents and proponents of these systems, is that fully autonomous and offensive weapons systems are being developed and are likely to be more widely used in future conflicts and wars.

[28]International Committee of the Red Cross n.d.

[29]iPRAW 2017; Conn 2018; European Parliament 2017.

[30]Hoadley and Lucas 2018, pp. 24–26.

[31]PAX for Peace 2019.

[32]Scharre 2018b, ch. 3; Author Interview, CNAS, Washington DC, January 2019.

In this case, autonomous weapons will lead to the potentially rapid development of new military tactics, shifting the traditional divide between offense and defence and punishment and denial, altering coercive calculations along the way. In this vein, saturation tactics have been given the most attention, in which thousands of miniature, cheaply made, and disposable autonomous systems are used to swarm and overwhelm a target.[33] The tactic usually references unmanned aerial vehicles (UAV; i.e. drones), but could just as well eventually involve unmanned ground vehicles (UGV; i.e. self-driving or—walking machines) and unmanned underwater vehicles (UUV; i.e. underwater drones). On its own, a single unmanned and autonomous unit is no match for a fighter jet or destroyer, but algorithmically lassoed together, a fleet of thousands might well overwhelm these larger and more cumbersome platforms. The tactic lends itself to both offensive and defensive processes. Horowitz suggests that low-cost, autonomous drones, coordinating their actions at machine speed, might undermine high-cost, high-quality legacy weapon systems.[34] Michael O'Hanlon adds further that these tactics might end "the kind of impunity that U.S. forces have enjoyed for decades".[35] Here again, innovation in imagination—rather than simply access to these sorts of autonomous platforms—may provide a nimble adversary with a coercive advantage.

21.5 Leveraging Moral Asymmetries for Coercive Gain

Ethical, political, and legal limitations on how AI is used in warfare may dictate how some countries behave and others respond. Some countries, notably the United States and several European allies, are (currently) openly against providing AI with the right or the means to kill individuals without human intervention—while promoting his country's AI innovation strategy, French President Emanuel Macron retorted that he was "dead against" the idea.[36] But other states, including U.S. adversaries, warn Darrell West and John Allen, are "not nearly so mired in this debate", or hamstrung by these concerns.[37] China, Russia, Israel, and others may be more willing to delegate decisions to AI. The emerging moral asymmetry introduces several interesting quandaries for thinking through the future of deterrence.

First, allies with asymmetric AI capabilities, uneven AI governance structures, or different AI rules of engagement, may find it difficult to work together towards a common coercive goal. Interoperability is central to collective defence and alliance

[33]Scharre 2014; Altmann and Sauer 2017.
[34]Horowitz 2018a.
[35]O'Hanlon 2018.
[36]Thompson 2018.
[37]West and Allen 2018.

coercion.[38] States with uneven development in AI may find it problematic to collaborate in theatre; the AI have-nots (and AI choose-nots) may function at a lower speed of operation, dragging the coalition's ability and credibility down with it. An inability to find common ground on when or how (or even whether) to use AI in strategic affairs may lead to a similar dilemma. Allies who differ on AI ethics might be unwilling to share useful training data or to make use of shared intelligence derived from AI. Without broader consensus, then, AI may weaken political cohesion within alliances, making them less effective as a result.

Second, lowering the bar on ethics and AI may become a strategic advantage: some challengers may derive a coercive advantage by signalling or communicating a willingness to develop, use, and rely on AI in warfare in ways that defenders have openly agreed against.[39] A belligerent, for illustration, might communicate a readiness to provide its AI with greater control over target engagement, or to field certain autonomous weapons systems, in order to compel or influence an adversary's behaviour. Some states might respond by purposefully shrouding their ethical standards when it comes to their own use of AI if only to safeguard against other's taking advantage of a known moral position, a twist on Thomas Schelling's "threat that leaves something to chance" (mis)appropriated to the AI era.

Third, and closer to home, ethical standards and considerations might likewise influence the very development of AI and the nature of alliance politics. This may be especially true in liberal democracies. To some, private sector considerations are a strategic consideration; the AI "commercial ecosystem" is small (less than ten thousand people, globally, determine the next generation of AI).[40] To a certain degree, then, the political and ethical preferences of the commercial American, Canadian, and European AI community will help determine how AI will be used within a military context among trans-Atlantic allies. The question "these folks ought to ask themselves is: What if we just don't utilize our expertise and cede this field to other countries; what if we just walk?"[41] The ramifications could include a strategic imbalance that favours NATO adversaries—notably China—who are purposefully building public-private collaborative AI hubs to ensure the full diffusion of the technology from the private sector to the public sector.

For the U.S., Europe, and Canada, deriving military or security benefit from AI developments taking place in the private sector will require generating incentives for public-private collaboration that meets the evolving standards of firms and/or attracts experts who might otherwise find employment at tech companies. Other states face fewer such constraints. Chinese corporations, for instance, appear far more eager, or are outright compelled, to work with the government; AI innovations are all but certain to trickle into military, intelligence, and security application.

---

[38]With thanks to the participants of the AI Deterrence Stakeholder Meeting, May 2019, Ottawa, Canada.

[39]Author Interview, CNAS, Washington DC, January 2019.

[40]Author Interview, Brookings Institution, Washington DC, January 2019.

[41]Ibid.

Thus, while Canada, parts of Europe, and the U.S. are ahead of China in terms of generating AI research, "China is crushing in the actual application of AI".[42] Other countries provide alternative lessons: Israel's model uniquely links industry, academia, and the state together, all working towards a complementary goal in support of each other.[43] Ultimately, embedding national AI strategies with the right balance of ethics and use may well lend itself to future deterrence calculations.

21.6 Enhancing the Credibility of Military Action

AI introduces a range of opportunities to combat environments, making some coercive threats more credible as a result.[44] By providing military systems with greater autonomy, for example, AI replaces humans in dangerous, complex, and labour-intensive jobs; the notion of a suicide mission may cease to influence decision-makers.[45] AI might likewise make "long-duration tasks that exceed human endurance" more feasible to plan and pursue.[46] Making sense of a huge quantity of data from disparate sources, AI might also provide military planners with suggested solutions that allow them to outpace an adversary's own assessment of and ability to strategically react to a situation if left to human analysis alone. Further, AI might provide out-of-the-box and unpredictable tactical advice that stretches the human imagination and experience. AI might likewise boost the productivity and capability of intelligence and military personnel, frontline soldiers, and of entire military institutions.

All told, AI might sufficiently alter the way conflict and war unfold, influence how states and militaries rely on and utilize both deterrence by denial and deterrence by punishment. On the former, by improving the speed and accuracy of some defensive weapons, and by subsequently improving the reliability of defending infrastructure and territory against certain kinetic attacks, AI might deter some types of behaviour by altogether denying their utility. The same holds when pairing AI to cyber deterrence: by denying aggressors access to information or networks more persistently, a defender's AI might compel a challenger not to bother attacking in the first place. In this vein of thinking, AI augments a defender's capability to defend, stripping away a challenger's ability to acquire what it hopes to accomplish. By denying success, AI deters behaviour. On the latter, however, and under other conditions, AI may augment the feasibility of certain types of offensive attack,

[42]Author Interview, CNAS, Washington DC, January 2019.

[43]Author Interview, Brookings Institution, Washington DC, January 2019.

[44]Hoadley and Lucas 2018.

[45]Conversely, Erik Gartzke argues that "automatic combat reduces the costs faced by the technological power", thus reducing its ability to demonstrate resolve: it appears to have less (of value) to lose: Gartzke 2019.

[46]Ibid.

altogether favouring punishment over denial. Autonomous swarming robotic platforms, as noted, have garnered the greatest attention: when refined, swarming bots may provide challengers with a unique coercive tool not easily deflected or defeated. Saturation tactics that rely on thousands of disposable robotic platforms working together may tip the balance towards offensive measures and the promise of punishment strategies.

Importantly, Zachary Davis makes a distinction between AI's application at the tactical and operational level of warfare—"the way wars are fought"—and the strategic level—actions that relate to the balance of power and "major conflicts between great powers", suggesting that adoption of AI in the former may lead to changes in deterrence in the latter. Davis explains that AI is already being used in military logistics, planning, and transportation, intelligence analytics and object identification, and in war gaming and training. Put together, these advancements might alter strategic calculations. He argues that AI might provide a state with the appearance of having the ability to conduct both a "disarming counterforce strike" against an adversary's retaliatory forces, and to shoot down remaining retaliatory capabilities with augmented defensive systems.[47] What counts, here, is perception: an adversary's belief in another's superior capabilities, which invites instability in the form of misperception, miscommunication, and miscalculation.[48] As Keith Payne reminds us in *Strategy, Evolution, and War* (2018), "strategy…is an intensely psychological activity".[49] It requires an actor to properly judge an adversary's motivation, beliefs, and thought. Deterrence, then, is applying pressure on an adversary such that you alter his intention. Payne, taking a biological, cognitive, sociological, and historical perspective on strategy, suggests that social life entails an ability to gauge, anticipate, and respond to an adversary's behaviour. He finds, ultimately, that AI may influence these processes, undermining the traditional expectation that defensive measures outweigh offensive ones in deterrence.

21.7 Conclusions: Next Steps for AI and Deterrence

Deterrence has been around a long time; it has repeatedly proven its theoretical flexibility in responding to shifting international dynamics and emerging technologies. As this volume suggests, this evolution has occurred within the context of distinct "waves" of scholarship, with a fifth now emerging. While AI will certainly shape this emerging wave in novel and unique ways, the actual study of AI and deterrence and coercion has only just begun. The emerging scholarship is necessarily speculative: not only is AI still an imperfect technology, but its application to

[47]Davis 2019, pp. 118–121.

[48]For Davis, AI poses a challenge to current thinking on coercion because of its effect on surprise attacks and on "mutual strategic vulnerability". Ibid.

[49]Payne 2018b.

warfare, intelligence, and national security is uneven and uncertain. Significant ethical, legal, and political considerations have yet to be hashed out. And a robust research program on AI deterrence has yet to be concretely conceived. What follows are suggestions for next steps in further developing and empirically testing AI deterrence theory.

From a theoretical perspective, a broadening of the conceptual field of research is needed. IR scholarship does not own deterrence. Scholars of psychology, criminality, terrorism studies, and computer science have made recent advancements in developing deterrence theory for countering crime, terrorism, and cybersecurity by applying insights from their distinct disciplines. These insights have proven useful to scholars of IR and military deterrence despite their interdisciplinary origins. Something similar should take place with the study of AI deterrence, which has all the hallmarks of requiring a cross-disciplinary lens. While this chapter—and much of the literature cited within it—explores how traditional IR intersects with AI deterrence, lessons from other fields where AI is making inroads and shaping individual and group behaviour, would provide a more fulsome theoretical picture.

For illustration, ubiquitous AI real-time surveillance is deterring criminal behaviour; China's experiment in deterring jaywalkers is informative.[50] Facial recognition cameras snap pictures of pedestrians breaking the law, matching the offender to photo IDs stored in a database. The individual's personal information can then be displayed online and on roadside screens—deterrence by embarrassment?—and fines can be issued automatically. In the city of Ji'Nan, the technology reduced jaywalking by 90%. What lesson might this criminological application of AI hold for IR deterrence and defence? If a state where to establish AI-powered surveillance of urban centres, border crossings, and other sensitive locations to generate biometric identification and behavioural analytics—notwithstanding concerns over personal privacy—and if it were to publicly announce its use of these tools, it might convince others besides jaywalkers, like organized criminals, terrorists, insider threats, and foreign spies, that their plans are unlikely to succeed, deterring other forms of unwanted behaviour.[51] Similar insights relevant to IR might be culled from cybersecurity's application of AI to behavioural dynamics in cyberspace. A multi-pronged approach will prove useful for developing robust theories of AI deterrence across the disciplines.

From an empirical perspective, qualitative case studies—and where applicable, quantitative analysis—should be conducted, testing the integrity and strength of the emerging theoretical propositions. Very little empirical work on AI and deterrence has taken place to date. Professor Wilner's research in this area, as part of his multi-year *AI Deterrence* project, does provide some early and preliminary empirical lessons however, suggesting avenues for further exploration. One of the

[50]Han 2018.

[51]Mosur 2019.

project's case studies explores the coercive effects AI might have on European border security.[52] Several scientific explorations are ongoing in Europe, testing the use and utility of applying AI to border and national security considerations. For illustration, the EU's iBorderCtrl program, field tested in 2019, uses AI avatars at select border crossings in Greece, Hungary, and Latvia to facilitate more thorough border control. In essence, travellers interact with the AI avatar, which is a computer-generated human-like figure displayed on a computer screen. The avatar asks the traveller questions, analysing responses by scanning the individual's facial characteristics for "micro-expressions" of stress, useful for detecting deception. Micro-expressions are indistinguishable to humans, so machines make a first assessment of an individual's overall risk. iBorderCtrl suggests the project is meant to "speed up the border crossing at the EU external borders and at the same time enhance the security and confidence regarding border control checks".

Wilner's *AI Deterrence* research team uses the border case study to explore the ramifications of experiments like iBorderCtrl on the future of physical coercion. Early results from the empirical work help situate deterrence continuity and change in an age of AI, with insights useful across the disciplines, including in IR. First, AI deterrence is a function of a process, not the immediate result of the technology itself. Second, AI deterrence is ultimately about finding the right balance between communicating, signalling, or illustrating capabilities and safeguarding those technological advantages. Third, AI deterrence may lead to deflection, displacement, and adversarial adaptation, undermining presumed deterrence successes. Fourth, and relatedly, actually measuring AI deterrence success requires fabricating a complicated counterfactual, definitively linking the technology itself to behaviour that ultimately did not take place. And fifth, ethics will play an oversized role in AI deterrence, driving the process of justification and applicability and informing the technology's use and utility. As AI becomes more fully integrated into society, policing, cybersecurity, intelligence, national security, and defence, other empirical lessons from a diverse set of circumstances will lend themselves to the scholarly evaluation and improvement of AI deterrence theory.

[52] A series of expert interviews were held at the Border Security AI Research Observatory, Frontex; GCHQ; Royal United Services Institute; European Union Institute for Security Studies; Université Libre de Bruxelles; Alan Turing Institute; Darktrace; and Stiftung Neue Verantwortung (SNV), Germany. Interviews took place between January and March 2020. Data were anonymized, in accordance with the project's research ethics protocol (Carleton University, 2021).

References

Altmann J, Sauer F (2017) Autonomous Weapons Systems and Strategic Stability. Survival 59.5:119–120

Brookings (n.d.) A Blueprint for the Future of AI. https://www.brookings.edu/series/a-blueprint-for-the-future-of-ai/

Coker C (2015) Future War. Polity

Conn A (2018) The Risks Posed by Lethal Autonomous Weapons. Future of Life Institute (September 2018)

Cummings M L et al (2018) Artificial Intelligence and International Affairs. Chatham House Report 7–18

Davis Z (2019) Artificial Intelligence in the Battlefield. PRISM 8.2:118–121

European Parliament (2017) Towards an EU Common Position on the Use of Armed Drones

Ganor B (2019) Artificial or Human. Studies in Conflict & Terrorism

Gartzke E (2019) Blood and Robots: How Remotely Piloted Vehicles and Related Technologies affect the Politics of Violence. Journal of Strategic Studies 15

Geist E, Lohn A (2018) How Might Artificial Intelligence Affect the Risk of Nuclear War? RAND

Han M (2018) AI Photographs Chinese Jaywalkers; Shames them on Public Screens. Medium, 9 April 2018

Hoadley D, Lucas N (2018) Artificial Intelligence and National Security. Congressional Research Service, pp 24–26 (April 2018)

Horowitz M (2018a) Artificial Intelligence, International Competition, and the Balance of Power. Texas National Security Review (May 2018)

Horowitz M (2018b) The Algorithms of August. Foreign Policy (September 2018)

Horowitz M (2018c) The Promise and Peril of Military Applications of Artificial Intelligence. Bulletin of the Atomic Scientists

Horowitz M (2019) When Speed Kills: Lethal Autonomous Weapon Systems, Deterrence, and Stability. Journal of Strategic Studies 42:6

Horowitz M et al (2018) Artificial Intelligence and International Security. CNAS

Huh Wong Y et al (2020) Deterrence in the Age of Thinking Machines. RAND

International Committee of the Red Cross (n.d.) Autonomous Weapons: Decisions to kill and destroy are a human responsibility. https://www.icrc.org/en/document/statement-icrc-lethal-autonomous-weapons-systems

iPRAW (2017) Focus on Computational Methods in the Context of LAWS

Knight W (2018) The Defense Department Has Produced the First Tools for Catching Deep Fakes. MIT Technology Review

Lappin Y (2017) Artificial Intelligence Shapes the IDF in Ways Never Imagined. The Algemeiner (October 2017)

Long J M, Wilner A (2014) Delegitimizing al-Qaida. International Security 39:1

Morstatter F et al (2019) SAGE: A Hybrid Geopolitical Event Forecasting System, Proceedings of the Twenty- Eighth International Joint Conference on Artificial Intelligence (August 2019)

Mosur P (2019) One Month, 500,000 Face Scans. New York Times, 14 December 2019

O'Hanlon M (2018) The Role of AI in Future Warfare. Brookings

PAX for Peace (2019) Slippery Slope: The Arms Industry and Increasingly Autonomous Weapons (November 2019)

Payne K (2018a) Artificial Intelligence: A Revolution in Strategic Affairs? Survival 5

Payne K (2018b) Strategy, Evolution, and War. Georgetown UP

Price M, Walker S, Wiley W (2018) The Machine Beneath. PRISM 7.4:92–105

Rassler D (2019) A View from the CT Foxhole. CTC Sentinel 12.11

Scharre P (2014) Robotics on the Battlefield, Part II. CNAS

Scharre P (2018a) A Million Mistakes a Second. Foreign Policy (September 2018)

Scharre P (2018b) Army of None. W.W. Norton

Solls B (2020) Now Hiring AI Futurists. ZDNet, 20 May 2020

Talmadge C (2019) Emerging Technology and Intra-war Escalation Risks. Journal of Strategic Studies 42:6
Thompson N (2018) Emmanuel Macron Talks to Wired about France's AI Strategy. Wired (March 2018)
Wasson J, Bluesteen C (2018) Taking the Archers for Granted: Emerging Threats to Nuclear Weapon Delivery Systems. Defense Studies 18:4
Wenger A, Wilner A (2012) Deterring Terrorism. Stanford University Press
West D, Allen J (2018) How Artificial Intelligence is Transforming the World. Brookings Institution (April 2018)
Wilner A (2015) Deterring Rational Fanatics. University of Pennsylvania Press
Wilner A (2019) Artificial Intelligence and Deterrence: Science, Theory, and Practice. NATO Science and Technology Organization (STO), MP-SAS-141-14
Wilner A (2020) US Cyber Deterrence: Practice guiding Theory. Journal of Strategic Studies 43.2
Wilner A et al (2019) The Threat of Digital Foreign Interference: Past, Present, and Future. Macdonald Laurier Institute
Wilner A, Wenger A (2021) Deterrence by Denial: Theory and Practice. Forthcoming, Cambria
Wittes B, Blum G (2015) The Future of Violence. Basic Books

Prof. Alex Wilner is an Associate Professor of International Affairs at the Norman Paterson School of International Affairs (NPSIA), Carleton University, Ottawa, Canada. His research updates deterrence theory and practice for contemporary and emerging security concerns. Prof. Wilner's books and volumes include *Deterring Rational Fanatics* (University of Pennsylvania Press, 2015), *Deterring Terrorism: Theory and Practice* (Stanford University Press, 2012), and *Deterrence by Denial: Theory and Practice* (Cambria Press, 2021).

Casey Babb is a Ph.D. Candidate at the Norman Paterson School of International Affairs (NPSIA), Carleton University, Ottawa, Canada. He is also a Junior Affiliate at the Canadian Network for Research on Terrorism, Security and Society (TSAS) and an Associate Fellow with the Royal United Services Institute (RUSI) in London, U.K. His research explores state strategy in cyberspace, as well as the nexus between emerging technologies and the future of conflict.

Part V
Rationality, Psychology, and Emotions

Chapter 22
Nuclear Deterrence in the Algorithmic Age: Game Theory Revisited

Roy Lindelauf

Contents

Abstract Commonly used game and decision theoretic models fail to explain the empirics of deterrence. This has unjustly led many theorists to criticize the (rationality and other) assumptions underpinning of such models. No serious game theorist will contend that his theoretic model will possibly take account of all the peculiarities involved in decision making and therefore be an accurate model of such situations. Games are an aid to thinking about some of the aspects of the broader situation. Game theory models prescribe what a decision maker *ought* to do in a given situation, not what a decision maker actually *does*. To maintain nuclear strategic stability, it is of paramount importance to understand the dynamical interplay between all players involved in decision making processes with regard to nuclear strategy. History has shown some progress in understanding nuclear deterrence by the use of initial game- and decision theoretic models to alleviate the burden of human cognitive biases. Since it is highly likely that (semi-)autonomous systems will in some way participate in the future nuclear strategic landscape, combined with the fact that the nuclear deterrent decision-cycle will also be based

R. Lindelauf (✉)
TU Delft, Delft, The Netherlands
e-mail: rha.lindelauf.01@mindef.nl

R. Lindelauf
Netherlands Defence Academy, Breda, The Netherlands

F. Osinga and T. Sweijs (eds.), *NL ARMS Netherlands Annual Review of Military Studies 2020*, NL ARMS, https://doi.org/10.1007/978-94-6265-419-8_22

on algorithmic analysis, rational deterrence theory is and should be an integral element of strategic thinking about nuclear deterrence. That, or it might as well be *game over*.

Keywords rationality · chicken games · tit-for-tat · autonomous weapon systems · artificial intelligence · algorithms · stability

22.1 Introduction

As discussed in the chapters by Bijlsma (Chap. 23), and Zilincik and Duyvesteyn (Chap. 24) in this volume, humans consistently and systematically make poor decisions as Nobel prize winning research on human decision making under uncertainty has shown.[1] Kahneman taught us that human thought processes as representations of the real world (so-called mental models) suffer from a multitude of cognitive biases. The mental models that humans employ are incomplete and unstable, our ability to mentally run mental models is limited and those models do not have firm boundaries and are parsimonious.[2] To avoid all out nuclear destruction the human calculus of deterrence should be protected from such shortcomings; deterrence theory sprang from this well. In addition, analytic techniques have been developed to alleviate the burden of cognitive biases that lead to fallacious arguments and inconsistent conclusions and should therefore be part of deterrence theoretic frameworks. A large subset of these methods entail quantitative prescriptive, descriptive and predictive models that consist of logical consistent frameworks that proceed from explicit assumptions to coherent conclusions. This chapter provides a coarse introduction into such quantitative models used to understand deterrence, with a specific focus on game- and decision theory.

During World War II quantitative modelling developed as a formal method of decision support for operations.[3] The field of operations research (sometimes referred to as decision theory) and game theory that emerged from this development is rich in methods and techniques that aid higher level decision makers regarding problems concerned with the operations under their control. Simply put, operations research (OR) is the science of decision making and game theory provides an explicit normative framework on optimal decision making in either conflicting or cooperative settings. Game theory is concerned with modelling strategic interaction, hence encompasses more than one 'player' (whereas OR or decision theory focus on unilateral decision frameworks). For several decades such frameworks have been successfully deployed in a multitude of military strategic and operational settings. Think of the identification of resource limited interdiction actions that

[1] See for instance Gilovich et al. 2002.

[2] Norman 1983.

[3] Washburn and Kress 2009.

maximally delay completion time of a proliferator's nuclear weapons project,[4] dynamic task assignments for multiple unmanned combat aerial vehicles,[5] submarine warfare,[6] search theory[7] and combat models,[8] to name just a few. The application of game theory is not limited to the military but includes many sectors, be it government, business, manufacturing, healthcare, service operations, evolutionary biology, experimental sociology, psychometrics, economics or others. Game- and decision theory encompasses many different decision making situations, such as optimization of resource allocation, task allocation, coalition formation, bargaining situations, elections, signalling, pricing and of course choosing deterrent strategies.

Game theoretically speaking: deterrence equals one player threatening another player with the goal of preventing him to conduct an aggressive action that it has not yet taken (but appears willing to do). In other words, the aim of deterrence is to influence perceptions and the decision calculus of the opponent to prevent him o doing something undesired.[9] Deterrence is therefore based on the psychological principle of a threat of retaliation. For instance, a nation wants to prevent nuclear first strikes or cyber-attacks and a company aims for the non-entry of competitors to their market. A key point in deterrence theory is *credibility*: are the threats credible or not. This depends on the attacker's beliefs on the capabilities of the defender. Clearly, any decision maker with enough concern for tomorrow is likely to be moved by deterrent threats.[10] Therefore it is not surprising that deterrence is a major theme of game theory, both in economics and political science game theory plays a role in modelling deterrence. Pioneers in the application of game theory such as Thomas Schelling resorted to game theory in their discussion of nuclear deterrence even though such leading scientists were not technical game theorists per se, they simply used concepts and insights from game theory to sharpen their thinking about deterrent situations.

On the other hand, deterrence theorists trace the origin of their theories to the aftermath of World War I and classify their realist classical theory of deterrence into several strands: structural deterrence theory and decision-theoretic deterrence theory.[11] It is the latter theory that applies game theoretic methodology to reasoning about deterrence. In this chapter, after first introducing some basics of game theory, we will present some of the game theoretic arguments—and critiques thereof—that arise in classical deterrence theory. Next we will mention some more advanced game theoretic models that are designed to take those critiques into account. Since

[4]Brown et al. 2009.

[5]Duan and Yu n.d.

[6]Danskin 1969.

[7]Alpern et al. 2013.

[8]Washburn and Kress 2009.

[9]See Chap. 1 by Freedman and Chap. 2 by Mazarr in the present volume.

[10]Langlois and Langlois 2006.

[11]Quackenbusch and Zagare 2016.

game theory also enters into the design and application of algorithms (of semi-autonomous systems) we will end this chapter with some observations on the recent exponential developments in computer science and the effect thereof on nuclear stability and deterrence.

In this chapter, a short introduction to normative decision making is given by presenting the basic framework of game theory. This will provide the reader with a better understanding of the standard ideas and assumptions with regard to this theory and also with some of its goals. Next several applications, including its shortcomings and advantages, of the game theory within deterrence theory are presented and discussed. The development of information technology and AI will have a large effect on nuclear security issues in the next quarter century, therefore this chapter concludes with a short outlook on future developments of nuclear deterrence with respect to algorithmic game theory in computer science in general and of artificial intelligence in particular.

22.2 Game Theory Basics

The mathematical theory of games can be divided into games of several types depending on whether,

A. players can negotiate and form alliances or not, i.e. cooperative versus non-cooperative games,
B. players know everything about the game (payoffs) and the other players (strategies) or not, i.e. games of (in)complete information,
C. players act concurrently or sequentially (where each player is aware of the other player his action) or not, i.e. simultaneous versus sequential games,
D. all the players have the same goals (are symmetric) such that only their choice of strategy determines who wins (chess) or not, i.e. symmetric versus asymmetric games,
E. all the players have perfect information about the game (observe all the other players' moves) or not, i.e. perfect versus imperfect information games,
F. one player's loss equals the other's gain (zero sum) or not, zero sum versus non-zero sum games.

Basically, a game involves players, strategies, payoffs and an information structure. The most well-known games are non-cooperative two player zero sum games. In general, a non-cooperative game is a sequence of moves, at each of which one of the players chooses from among several possibilities.[12] Note that some such moves may involve chance (for instance throwing a die) or are random acts of nature. At the end of the game there is some sort of payoff to all of the players. This for instance can be money, satisfaction, or any other quantifiable variable. In

[12]Owen 2001.

general, non-cooperative games are modelled either in *extensive-* or *normal* form. The former includes the possibility of alternation of moves by players and situations where players can have less than perfect information such as not knowing other player's payoffs or possible moves. The latter involves the assumption that, given knowledge of the game and its payoffs, each player has already decided what he will do before the game starts, i.e. each player chooses a strategy before the game and they do so simultaneously. This may be a restrictive assumption at first, but it encapsulates the idea of devising a plan ('strategy' in game theoretic nomenclature) for a coming situation.

Most often the game theorist is interested to devise the best possible plan for a given game, i.e. to find optimal strategies for each player. Optimality consists of maximizing the payoff to the respective players and looking for equilibrium situations. Simply put, an equilibrium occurs if each player is satisfied. Below simple examples of an extensive form game and a normal form game are given. The main difference between a game in extensive form or normal form is in the sequentially to a player's moves. The former allows for players to move after each other such that players can observe the other's moves, the latter assumes that players decide upon optimal strategies before the game commences.

In Fig. 22.1 an example of an extensive-form game with two players (player 1 and player 2) is shown. Many examples in international relations theory are modelled by simple extensive-form games.[13] The game in Fig. 22.1 commences at the root of the tree where player 1 can choose between option Z or W. Depending on player 1's moves, player 2 can either choose between A and B or between C and D. In the former case player 1 again is presented with two options: X or Y. The dotted line indicates an *information set*, i.e. it exemplifies a situation of incomplete information: player 1 (noted above the dotted line) cannot distinguish between the states in the information set, that is, he does not know whether player 2 will choose A or B. Finally, the numbers denoted at the terminal vertices indicate the payoff to the respective players.

To infer optimal options for the players in this game, to 'solve' an extensive-form game, several solutions concepts exists in game theory. The most well-known solution to an extensive game is called backward induction where one reasons backward in time to solve each subgame, reasoning from the optimality of the previous solved subgame.[14] It is a theorem in game theory that a subgame perfect Nash equilibrium can always be obtained by backward induction in finite perfect information games. Even though the game in Fig. 22.1 is not of the perfect information type, it still can be solved using this procedure (due to its payoff structure). In the game in Fig. 22.1, starting at player 1 in his choice between X or Y it can be seen that X always favors Y ($5 > 3$ and $4 > 2$) even though player 1 does not know player 2's choice between A and B. Player 2 then (knowing that player 1 will choose X) favors B over A ($6 > 0$), additionally player 2 prefers C over D ($4 >$

[13]See Langlois and Langlois 2006 regarding the Cuban missile crisis.

[14]Neumann and Morgenstern 1944.

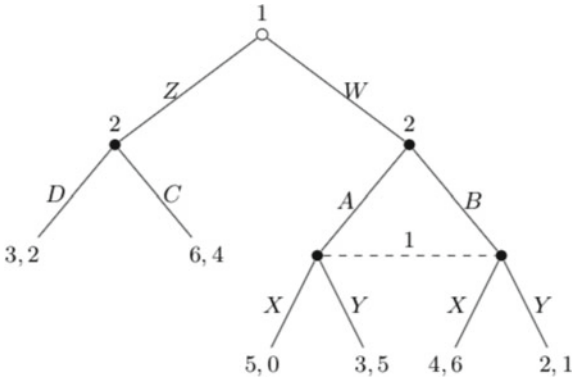

Fig. 22.1 An example of an extensive-form game (*Source* Roy Lindelauf)

2). Finally, player 1's choice at the root is between Z (which will yield 6) or W (which will yield 4). Hence the solution obtained by backward induction yields player 1 choosing Z, X and player 2 choosing C, B. Clearly more realistic games contain more players, more moves and more options per player. If the game has a finite horizon and is of perfect information the solution procedure as sketched above remains the same (and can be computed algorithmically).

Another very common approach to model strategic interaction with game theory is according to the *normal-form*. Informally a normal-form game consists of players each of which have strategies that after selection are played *simultaneously*. Each strategy selection for all players results in payoffs (to each player) that can be observed by all players. Those payoffs are denoted in a *payoff matrix* (see Fig. 22.2) which can be analysed using well defined concepts (such as dominating strategies, pure or mixed Nash equilibria, etc.). Solutions of a normal-form game then consist of *good* strategy prescriptions for each player. When the game situation repeats over time and/or space those solutions come in the form of probability distributions over the set of pure strategy options for each player. The most well-known such solution is the Nash equilibrium which consists of the strategy profile for all players such that no player can unilaterally benefit from deviation from that profile. If the game is of complete information (each player knows all the options of every player and all corresponding payoffs) all players can compute the optimal strategy of each player. However, even though each player thus knows the optimal play of the other players, he/she still does not know the actual option those players will play (because those strategies are given probabilistically). Hence normal-form games provide optimal plays that are rational but unpredictable.

Consider the following simplified introductory example. Somewhere on a remote island drug smugglers regularly drop off small shipments of illegal drugs at either one of two locations, A or B. The police unit on the island has very limited resources and can observe only one location at a time. Knowing that the drop-off capacity at location A is twice that of B, the question arises which location should be observed more often (and how often). Similarly, the smugglers wonder at which location to drop their drugs and with what frequency.

Fig. 22.2 An example of a normal-form game (*Source* Roy Lindelauf)

		Smugglers	
		A	B
Police	A	2,-2	0,0
	B	0,0	1,-1

The Nash equilibrium to this game equals the Police observing location A with probability 1/3 and location B with probability 2/3 (due to the symmetry of the game the same holds for the smugglers). In practice this translates to the police throwing a regular dice before each observation and when it lands on either 1, 2, 3 or 4 the observation takes place at location B, otherwise at location A (similar for the smugglers). The expected average capacity (kilos of cocaine) of seized drug shipments then equals 2/3, i.e. if the police did 100 observations (and each shipment contained either 1 or 2 k of cocaine) according to this strategy then on the average there would be a total of about 66 k of cocaine seized. Cleary normal-form games that model reality more realistically contain more than two options or two players. The normal-form game theoretic framework however has been very successful and applied in a plethora of applications.

22.3 Nuclear Deterrence and Basic Game Theory

Initial game theoretic models of deterrence are extreme simplifications of the complicated reality of deterrent situations. In general, this contention holds for many normal and extensive form games used in international relations theory. Often such text book models are two person games with both players only having two options (the normal-form as presented in the previous paragraph). Perhaps the most well-known game in IR theory is the prisoner's dilemma, used to model the Cuba crisis for instance, developed in the 1950s by RAND researchers.[15] Such two-by-two games serve as gentle introductions into the ideas and concepts of basic game theory, but lack depth and structure for modelling realistic situations.

An example of a two-by-two game to model nuclear crisis is the *chicken game*.[16] This game represents the situation where two teenagers are speeding towards each other in their cars at the middle of the road, i.e. representing two nuclear belligerents threatening each other with all-out nuclear war. Each player only has two options: to swerve (S; not attack) or to non-swerve (NS; attack). The corresponding payoff structure is modelled as follows: the first player to swerve loses. However, this loss is not as bad as both players not swerving (resulting in mutual destruction).

[15]Dresher 1961.

[16]Kahn 1960.

Clearly, a player prefers the situation of both players swerving above the situation where he swerves and the other does not (better to have no nuclear strikes than to be destroyed by one). This results in the following ordinal preference structure (for player 1): (NS, S) > (S,S) > (S,NS) > (NS,NS). Because the game is completely symmetric the same holds for the second player and it can easily be seen that only if both players cooperate a compromise could emerge. Otherwise, if only one player cooperates (agrees not to strike) the other player can exploit this (by striking). This game theoretic equilibrium outcome does not represent reality.[17]

It is easy to argue that the chicken game abstracts away too much aspects of a nuclear crisis. The game assumes that both players only have two options, that they determine their strategy beforehand, that there is no observation of others' actions and that each player has complete information about the game. Additionally, empirical evidence shows that, in the case of approximately equal opponents, it is better for a player to escalate when challenged with a nuclear strike than to submit.[18] Chicken games do not allow for such step-by-step iterations.

In Quackenbusch and Zagare (2016) a simple extensive-form game to model deterrence is introduced, the rudimentary asymmetric deterrence game (RADG). This game consists of two players (challenger and defender) and both players have two options at their disposal: cooperate and defect for challenger and concede and deny for defender. Challenger moves first. It is stated that the assumption that conflict is the worst outcome is 'the defining assumption of decision-theoretic decision theory', translated into the lowest payoff for both players in case of 'conflict'. Then it is reasoned that, by use of RADG, this leads to the paradox of deterrence: the contention that bilateral relationships between nuclear equals are stable even though the 'solution' of the RADG does not equal the status quo. The solution of the RADG as presented by Quackenbush and Zagare, i.e. the Nash equilibrium obtained by backward induction, equals the situation where challenger chooses 'defect' and defender chooses 'concede'. Indeed, this is not a stable bilateral situation between nuclear equals. This paradox is easily resolved by changing the payoff structure of the game, hence it is not a shortcoming of decision theory but rather of modelling choice.

Summarizing, early game theoretic models used by modellers of deterrence lack complexity to include,

1. situations of escalation, i.e. players react to each other inducing continuous iterations of developing situations,
2. attackers and defenders (almost always) are not exactly aware of each other's strategy options and utility calculations (and there can be more than two players), i.e. incompleteness of information dominates international political decision making regarding deterrence,

[17]Another (mixed) strategy equilibrium exists in chicken games but that is not mentioned here because it does not add to the discussion.

[18]Zagare 1987.

3. attackers and defenders are not exactly aware of the moves other players have made (and there can be more than two options per player).

Research in game theory—outside of the scope of deterrence—recognized all of the restrictions mentioned above.

22.4 Moving beyond the Limitations of Basic Game Theory Models

A plethora of advancements have been made to overcome those limitations. The easiest: having more than two options for each player and having more than two players. Additionally, iterated games (also called 'repeated games') were developed to analyse series of decisions that are not 'one-shot'; they overcome the first objection as mentioned above. Knowing that a game will continue indefinitely will impact how players choose their strategies because players have knowledge of the past behaviour of their rivals (they observe their choices). The Soviet-US arms race for instance has been most commonly modelled as an iterated prisoners' dilemma [IPD] (Majeski 1984). This led to the famous TIT-FOR-TAT (TFT) decision rule that consists of choosing 'cooperate' during the first iteration and then copying what the other player did in the previous round thereby rewarding cooperative behaviour and punishing otherwise. It turned out that this decision rule did surprisingly well in many comparisons of strategies for the IPD because of its properties of niceness, forgiveness and retaliatoriness. This results in a model where on any given trial both superpowers are better off arming regardless of what the other side chooses, but if both sides arm the outcome is less desirable than had both sides reduced their supply of weapons.[19]

Several extensive form models have been introduced, such as Hawks and Doves games that include incomplete information situations and elements of nuclear brinkmanship by introducing escalation ladder models[20]. However, this model still suffers from many of the shortcomings mentioned above. It was John Harsanyi who first developed game theoretic models to deal with situations of incomplete information.[21] With respect to deterrence for instance the attacker's beliefs on the credibility concerning the defender's deterrent threat are uncertain. Such incomplete information could be about the other player's motivations, strategy options, resolve, beliefs about the other player and others aspects.

Clearly the problem of deterrence has also inspired more advanced forms of game theory. Nobel Prize winner Robert Aumann together with Michael

[19]Plous 1993.

[20]See for instance Langlois' online chapter three of *Applicable Game Theory.*

[21]Harsanyi 1967.

Maschler[22] wrote a book on the application of mathematical utility theory to disarmament. They formulated repeated two-player games in which one (or both) of the players lack complete information on the payoffs in the stage-game matrix. They showed that when one of the two players has special information not available to the other, then he can use this information to his advantage only to the extent that he reveals it. Using several theorems, they showed that optimal strategies in repeated games of incomplete information contain certain interesting peculiarities which are best illustrated by the following analogy: consider player 1, a policy maker who does not play the game himself, he uses a negotiator to play the game for him instead. Aumann and Maschler showed that the optimal strategy for the policy maker is to fool his negotiator to the extent that he reveals him a certain amount of information on how to negotiate (the type of negotiator he is) according to some probability distribution (determined by mathematical analysis). The interesting fact is that complete disclosure nor complete concealment of secret information from one's negotiator is in general an optimal strategy and that there exists a random mechanism that describes exactly what partial information should be disclosed to the negotiator.[23]

22.5 Nuclear Deterrence—Games and Decisions

The preceding paragraphs illustrated that commonly used game and decision theoretic models fail to explain the empirics of deterrence. This has unjustly led many theorists to criticize the (rationality and other) assumptions underpinning of such models.[24] Next to the reasons already mentioned, no serious game theorist will contend that his theoretic model will possibly take account of all the peculiarities involved in decision making and therefore be an accurate model of such situations. Games are an aid to thinking about some of the aspects of the broader situation. The corresponding conclusions therefore will reflect general insights that can be useful in the weighing of multiple criteria upon making a decision. Game theory models prescribe what a decision maker *ought* to do in a given situation, not what a decision maker actually *does*.

Much in the same way, decision theory for instance has taught us by mathematical analysis that commonly accepted beliefs about decision procedures with three or more candidates will *always* lead to a dictator; by listing basic properties of decision methods satisfied by all (democratic) election methods Arrow showed this

[22]Aumann and Maschler 1995.

[23]For a much more in-depth analysis of these assertions, we refer to Aumann and Maschler 1995.

[24]Lebow and Stein 1989.

in his famous theorem.[25] This shows the fallacy of human reasoning and the necessity of logical consistent thinking; informal arguments can lead to seemingly correct conclusions which in reality contain falsehoods. Such contentions in all likelihood also hold for arguments in deterrence theory. The theories of games and decisions are therefore of innumerable value to provide a coherent explicit framework and to alleviate the burden of cognitive biases in decision settings such as deterrence. No framework, be it quantitatively motivated or not, will ever explain all the peculiarities encompassed in complex deterrence settings. 'All models are wrong, but some are useful' as famous statistician George Box used to say.[26] So what then is the future of game theory in deterrence?

First, game theory can help to lay an axiomatic foundation under the theory of deterrence, much as decision theory did for the theory of democratic elections (see our earlier mention of Arrow's theorem). Second, the world is witnessing unprecedented technological innovations in information technology. Algorithms are entering each and every aspect of our lives, from choosing which movie to watch at night to predicting poaching of wildlife. The exponential growth of processor speed, data storage, computational analysis and technology in general are changing the future battlefield. Systems embedded with algorithms that make decisions on its behaviour are commonplace and are expected to proliferate in the future. It comes as no surprise that these advancements in computer science enable *rational* decision making within the field of deterrence along another avenue of approach. The future battlefield will see a mix of (semi-)autonomous weapon systems with manned systems.[27] It is highly likely that these systems will deploy game- and decision theory based algorithms to coordinate and control.[28] Autonomous weapon systems base their decisions on all kinds of algorithms. These artificial intelligence and autonomous systems have the potential to dramatically affect nuclear deterrence and escalation.[29] The speed of decision making, its differences from human understanding, the willingness of many countries to use autonomous systems, our relative inexperience with them, and continued developments in these capabilities are among the reasons.[30] A similar situation has already been witnessed in the field of stock trading where high frequency automatic trading algorithms are deployed to conduct autonomous trading. This contributed to the flash crash of the stock market in 2010 where computers in fast automated markets made buy-sell decisions in fractions of seconds.[31]

Game and decision theoretic concepts often translate directly into such algorithms. Actually game- and decision theory is an integral element of artificial

[25]Saari 2001.

[26]Box 1976.

[27]Wong et al. 2020.

[28]Marden and Shamma 2018; Morgan et al. 2018.

[29]See Chap. 21 by Wilner and Casey in the present volume.

[30]Wong et al. 2020.

[31]Kirilenko and Samadi 2017.

intelligence.[32] Machine learning classifiers such as a support vector machine for instance can be seen as strategic two player games, i.e. one player is challenging the other in finding the optimal hyperplane by giving him the most difficult points to classify. Many algorithms implemented by (semi-)autonomous systems are based on rational decision making. In multi-agent reinforcement learning for instance agents *learn* by interacting with the environment and with other agents. Often the Nash equilibrium represents the collaboration point between the different agents (players). In short, this forces game theory in the future of nuclear deterrence along several avenues of approach. Below we exemplify three of them.

A. The design of nuclear weapon decision support algorithms, for instance with respect to the detection and tracking of adversary launchers for counterforce targeting;
B. With respect to coordination and competition between (semi-)autonomous nuclear systems, for example consider Russia's nuclear powered undersea drone that can carry a thermonuclear warhead and that should be able to operate autonomously for prolonged periods of time;[33]
C. Regarding (adversarial attacks on) algorithms used in the nuclear infrastructure, for instance by data poisoning corresponding SCADA systems.[34]

First, consider one of many nuclear weapon decision processes: the targeting process. This is the practice that aims at achieving specified effects on and beyond the battlefield that employs classic kinetic lethal actions as well as non-military, non-kinetic, and nonlethal activities. The process consists of six phases of which the second phase—*target analysis, vetting, validation, nomination and prioritization*—is clearly of interest to automation of (nuclear weapon) decision support. With the massive increase of data in the Intelligence Surveillance and Reconnaissance (ISR) domain comes the need of automated analysis simply because the amount of data exceeds the timely analysis capacity of human analysts. The second phase of the targeting process can benefit from the use of automated analysis since it provides opportunities to deal with the complexity, scope and scale of the targeting process.[35] Decision support algorithms for nuclear weapon targeting come in many shapes and forms and can benefit from game theoretic approaches. Target prioritization for instance consists of ranking targets because resources are scarce. This is related to solution concepts in cooperative game theory such as the Shapley value that axiomatically defines a formula to derive the power of 'players' that create value upon cooperation. With respect to nuclear targeting this relates to the importance of a target with respect to the value of a subset of targets that can be engaged given cost and capacity restrictions. Power indices in cooperative game

[32]Norvig and Russell 2016.
[33]Geist and Lohan 2018.
[34]Terziyan et al. 2018.
[35]Ekelhof 2018.

theory provide a sound basis to support such decisions and are applied in a plethora of security domains.[36]

Second, consider coordination and competition between (semi-)autonomous systems, i.e. the field of multi-agent systems (MAS)—an area in distributed artificial intelligence—that consists of multiple autonomous interacting units each with their own sensory systems and goals. Based on resources and agents skills MAS systems will either be in cooperation and collaboration or competition.[37] Military applications of MAS frameworks for instance consist of surveillance, navigation and target tracking and are clearly also beneficial in nuclear settings. Future systems like the Russian undersea drone for instance have to operate autonomously to achieve individual goals over long periods of time and are expected to interact with other agents that influence each other's decisions. One advantage of such a drone system is its capability for ultra-long loitering periods as there is no human crew that needs time to recuperate and recover. Therefore, it also needs to be equipped with smart decision procedures. One possible approach to develop such protocols is by multi-agents reinforcement learning, a research area within AI that uses game theory to learn optimal behaviour of agents through trial and error interaction with the environment and with other agents. In such a setting agents are assumed to be players in a normal-form game which is played repeatedly.[38] The importance of understanding the dynamics of such game theoretic algorithms is evident and still an active field of open research.

Third, future AI developments might put the nuclear infrastructure even more at risk in various ways. Inadvertent nuclear escalation is being driven by the fact that nuclear command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) capabilities are entangled with nonnuclear weapons.[39] Cyber operations, empowered by AI algorithms, magnify and aggravate the challenges associated with C4ISR as military cyber offensives threaten the elimination of C4ISR capabilities.[40] Hence dual-use C4ISR capability could become under attack during a conventional conflict and prove escalatory in the nuclear domain. Protecting such critical infrastructure can be done by assisting decision systems using game theoretic models that compute optimal defender strategies in near real-time, thus providing efficient ways of allocating scarce resources for defence. An example of such a model for instance consists of power grid defence against malicious cascading failures.[41] Another area where game theory meets artificial intelligence is the field of generative adversarial networks. Here deep learning tasks

[36]Van Campen et al. 2018.

[37]Parker 2008.

[38]Nowé et al 2012.

[39]Acton 2018.

[40]Futter 2016; Li 2018; Sweijs and Osinga 2020.

[41]Shakarian and Lindelauf 2014.

can be viewed as strategic games.[42] Such models have also been used in data poisoning attacks that target machine learning algorithms by injecting malicious data-points into the training dataset.[43] Modern communication technologies used in SCADA systems that operate nuclear infrastructure introduce security vulnerabilities such as data poisoning of their AI driven decision support algorithms.[44]

To maintain nuclear strategic stability, it is of paramount importance to understand the dynamical interplay between all players involved in decision making processes with regard to nuclear strategy.[45] History has shown some progress in understanding nuclear deterrence by the use of initial game- and decision theoretic models to alleviate the burden of human cognitive biases. Since it is highly likely that (semi-)autonomous systems will in some way participate in the future nuclear strategic landscape,[46] combined with the fact that the nuclear deterrent decision-cycle will also be based on algorithmic analysis, rational deterrence theory is and should be an integral element of strategic thinking about nuclear deterrence. That, or it might as well be *game over*.

References

Acton J M (2018) Escalation through Entanglement. International Security, 43.1:56–99

Alpern S, Fokkink R, Gasieniec L, Lindelauf R, Subrahmanian VS (2013) Search Theory: A Game Theoretic Perspective. Springer, New York

Aumann R J, Maschler M B (1995) Repeated Games with Incomplete Information. MIT Press, Massachusetts Institute of Technology

Box GEP (1976) Science and Statistics. Journal of the American Statistical Association 71.356:791–799

Brown G et al (2009) Interdicting a Nuclear-Weapons Project. Operations Research 57.4

Danskin JM (1969) A Helicopter versus Submarine Search Game. Operations Research, Vol. 16, No.3

Dresher M (1961) The Mathematics of Games of Strategy: Theory and Applications. Prentice-Hall, Englewood Cliffs NJ

Ekelhof M (2018) Lifting the fog of targeting. Naval War College Review, 71.3. US Naval War College Press

Futter A (2016) Cyber Threats and Nuclear Weapons. New Questions for Command and Control, Security and Strategy. RUSI Occasional Paper

Geist E, Lohan A J (2018) How Might Artificial Intelligence affect the Risk of Nuclear War? RAND Corporation, Santa Monica CA

Gilovich T, Griffin D, Kahneman D (2002) Heuristics and biases: The psychology of intuitive judgment. Cambridge University Press, New York

[42]Tambine 2019.

[43]Munoz-Gonzalez et al. 2019.

[44]Munoz-Gonzalez et al. 2019.

[45]Morgan et al 2017.

[46]Horowitz 2019.

Gomez Rivera AO et al (2019) Towards Security and Privacy of SCADA Systems through Decentralized Architecture. International Conference on Computational Science and Computational Intelligence (CSCI), IEEE Xplore
Haibin D et al (2015) A Predator Prey Particle swarm optimisation approach to multiple UCAV air combat modeled by dynamic game theory. IEEE/CAA 2.1
Harsanyi JC (1967) Games with incomplete information played by "Bayesian players", I-III. part I. The Basic Model. Management Science 14.3:159–182
Horowitz M C (2019) When speed kills: Lethal autonomous weapons systems, deterrence and stability. Journal of Strategic Studies 42.6
Kahn H (1960) On thermonuclear war. Routledge, New York
Kahneman D, Tversky A (1974) Judgement and Uncertainty: Heuristics and Biases. Science, 27.185
Kirilenko A S, Samadi M (2017) The flash crash: High-frequency trading in an electronic market. The Journal of Finance, Wiley Online Library
Kopelman S (2020) Tit for Tat and Beyond. The Legendary Work of Anatol Rapoport. Negotiation and Conflict Management Research 13.1:60–84
Langlois J P, Langlois C (2006) Bargaining and the Failure of Asymmetric Deterrence: Trading off the Risk of War for the Promise of a Better Deal" (with Catherine Langlois), Conflict Management and Peace Science 23:159–180
Lebow N R, Stein J G (1989) Rational Deterrence Theory: I Think, Therefore I Deter. World Politics 41.2:208–224
Li J (2018) Cyber security meets artificial intelligence: a survey. Frontiers of Information Technology & Electronic Engineering 19:1462–1474
Majeski SJ (1984) Arms races as iterated prisoner's dilemma games. Mathematical Social Sciences 7(3):253–266
Marden JR, Shamma JS (2018) Game Theory and Control. Annual Review of Control, Robotics, and Autonomous Systems 1:105–134
Morgan FE et al (2018) Military Applications of Artificial Intelligence. Ethical Concerns in an Uncertain World. RAND Corporation, Santa Monica CA
Morgan GP et al (2017) Sociocultural Models of Nuclear Deterrence. IEEE Transactions on Computational Social Systems 4.3
Munoz-Gonzalez L et al (2019) Poisoning Attacks with Generative Adversarial Nets. arXiv:1906.07773v2
Neumann J, Morgenstern O (1944) Theory of Games and Economic Behavior. Princeton University Press, Princeton
Norman DA (1983) Some Observations on Mental Models. In: Gentner D, Stevens A (eds) Mental Models. Lawrence Erlbaum Associates Cognitive Science Series, Mahwah NJ
Norvig P, Russell S (2016) Artificial Intelligence: A Modern Approach. Pearson Education Limited
Nowé A, Vrancx P, De Hauwere YM (2012) Game Theory and Multi-agent Reinforcement Learning. In: Wiering M, van Otterlo M (eds) Reinforcement Learning. Adaptation, Learning, and Optimization, vol 12. Springer, Berlin/Heidelberg
Owen G (2001) Game Theory. Academic Press
Parker L E (2008) Distributed Intelligence: Overview of the field and its application in multi-robot systems. J. Phys. Agents 2.1:5–14
Plous S (1993) The nuclear arms race: Prisoner's dilemma or perceptual dilemma. Journal of Peace Research
Quackenbusch S L, Zagare F C (2016) Modern Deterrence Theory: Research Trends, Policy Debates, and Methodological Controversies. Oxford Handbooks Online
Saari DG (2001) Decisions and Elections; Explaining the Unexpected. Cambridge University Press, Cambridge
Shakarian S, Lindelauf R (2014) Power Grid Defense Against Malicious Cascading Failure. 13th Conference of Autonomous and Multiagent Systems, AAMAS-14
Sweijs T, Osinga F (2020) Maintaining Nato's Technological Edge. Whitehall Papers 95.1

Tambine H (2019) Deep Learning Meets Game Theory: Bregman-Based Algorithms for Interactive Deep Generative Adversarial Networks. IEEE Transactions on Cybernetics 50.3
Terziyan T et al (2018) Industry 4.0 Intelligence under Attack: From Cognitive Hack to Data Poisoning. In: Dimitrov K (ed) Cyber Defence in Industry 4.0 Systems and Related Logistics and IT Infrastructures. IOS Press, Amsterdam
Van Campen T, Hamers H, Husslage B, Lindelauf RA (2018) New approximation method for the Shapley value applied to the WTC 9/11 attack. Social Network Analysis and Mining 8.3
Washburn A, Kress M (2009) Combat Modeling. Springer, New York
Wong YH et al (2020) Deterrence in the Age of Thinking Machines. RAND Corporation, Santa Monica CA
Zagare F (1987) The Dynamics of Deterrence. University of Chicago Press, Chicago

Roy Lindelauf is assistant professor of Quantitative Intelligence Analysis at the Department of War Studies of the Netherlands Defence Academy. A former Apache Attack Helicopter pilot, his research includes Quantitative Intelligence Analysis, Game Theory, Network Analysis, Data Mining and Algorithms. He obtained his PhD from Tilburg University.

Chapter 23
What's on the Human Mind? Decision Theory and Deterrence

Tom Bijlsma

Contents

Abstract Indeed, deterrence, as Freedman and Mazarr recount in this volume in respectively Chaps. 1 and 2, aims to dissuade an opponent from taking undesirable actions. Clear communication of demands (a red line for instance), coupled with a credible threat to inflict pain if necessary, and demonstration of resolve are some obvious essential elements for creating effective deterrence. Success crucially also depends on whether the opponent receives the intended signal, interprets it as intended, and has the perception that the message is congruent with reality, i.e., that the opponent can make good on her threats. Success furthermore assumes that the demands communicated are acceptable. If those prerequisites exist, theory suggests a rational actor will back down, after weighing the benefits of the envisioned actions

T. Bijlsma (✉)
Netherlands Defence Academy, Breda, The Netherlands
e-mail: T.Bijlsma.01@mindef.nl

F. Osinga and T. Sweijs (eds.), *NL ARMS Netherlands Annual Review of Military Studies 2020*, NL ARMS, https://doi.org/10.1007/978-94-6265-419-8_23

versus the potential costs that may result when the threat is executed. This chapter offers a synthesis of insights that have appeared since the 1980s that fundamentally challenge that assumption of rationality. This contribution about the workings of the human mind concerns the various filters and cognitive shortcuts that colour the incoming stream of information and the processes to digest it and come to a decision.

Keywords Rationality · heuristics · biases · culture · religion · ideology · prospect theory

23.1 Introduction

Deterrence revolves around the mind; in essence, it is a psychological game that is played to influence the decision-making process of another actor. Patrick Morgan defined the nexus of deterrence and psychology succinctly as follows: 'Deterrence is undoubtedly a psychological phenomenon, for it involves convincing an opponent not to attack by threatening it with harm in retaliation. To "convince" is to penetrate and manipulate the thought processes of the opposing leaders so that they draw the "proper" conclusion about the utility of attacking'.[1] Indeed, deterrence, as Freedman and Mazarr recount respectively in Chaps. 1 and 2 of this volume, aims to dissuade an opponent from taking undesirable actions. Clear communication of demands (a red line for instance), coupled with a credible threat to inflict pain if necessary, and demonstration of resolve are some obvious essential elements for creating effective deterrence. Success crucially also depends on whether the opponent receives the intended signal, interprets it as intended, and has the perception that the message is congruent with reality, i.e., that the opponent can make good on their threats. Success furthermore assumes that the demands communicated are acceptable. If those prerequisites exist, theory suggests a rational actor will back down, after weighing the benefits of the envisioned actions versus the potential costs that may result when the threat is executed.

This chapter offers a synthesis of insights that have appeared since the 1980s that fundamentally challenge that assumption of rationality. This contribution about the workings of the human mind concerns the various filters and cognitive shortcuts that colour the incoming stream of information and the processes to digest it and come to a decision. Just as the human body and mind are closely tied to each other, emotion too is integrally connected to one's way of thinking and behaviour. The logic of affect, or emotional choice theory, states that decision-making is based on the dynamic interplay between one's emotions, norms, and identity.[2] The emotional part of the mind I will leave to Zilincik and Duyvesteyn in Chap. 24 of the present book as well as to many other researchers.

[1] Morgan 1985.

[2] Markwica 2018.

This chapter benefits from ongoing research in, at one end of the war-coercion-deterrence-spectrum, Peace Psychology, which is a division within the American Psychological Association (APA). The full name of this Division 48 is Society for the Study of Peace, Conflict, and Violence. Peace psychology has as its focus the application of psychology to issues of peace, conflict, and violence, often in the context of international politics. Second, it builds on insights from political psychology, which is not (yet) an independent and distinctive tag in the field of psychology, yet in the last decades, it has contributed quite significantly to research on international studies, international relations and foreign policy.[3] This contribution is welcomed because of the integrated approach required for the understanding of political problems, an understanding that also requires the disciplines of, for example, political science, sociology, history and economics. Moreover, the annual meeting of the International Political Psychology Association in 1982 formed the cradle of the seminal work *Psychology and Deterrence*.[4]

While this chapter focuses on the deterring person and the individual receiver, the deterred, it is absolutely of value for understanding decision-making processes at higher aggregate levels (groups, military organizations and governments).[5] In her standard work *Foreign Policy Analysis*, Valerie Hudson deprives the reader right from the start of some illusions. The field of international relations is basically about … understanding how humans perceive and react to the world around them, and how humans shape and are shaped by the world around them….[6] The first two levels of the nine major levels of analysis in foreign policy analysis she constructed are about the individual: cognitive processes and leader personality and orientation —all basic aspects in this contribution.

After a short preface about the historical developments in deterrence research, the stage is set for the deterring mind, and the corresponding eye of the beholder: six of the most common heuristics related to deterrence are discussed. Framing as a major bias is then introduced, followed by prospect theory. Finally, some of the consequences of using heuristics, defensively as well as offensively, are discussed.[7] The final conclusion can be summarized as follows: when deterring, know yourself well, very well, as well as your opponent, and work in a team.

[3]McDermott et al. 2011.

[4]Jervis et al. 1985.

[5]Allison and Zelikow 1999.

[6]Hudson 2014.

[7]Among others, Payne 2001; Jervis et al. 1985; Tetlock et al. 1991.

23.2 Rationality and the Evolution of Deterrence Theory

Jeffrey Knopf usefully introduced the idea of four waves in the deterrence literature. The first wave took shape after the invention of the atomic bomb and the setting of the new power blocks, right after World War II.[8] The second wave emerged in the 1950s and 60s. Fuelled by research in the RAND think tank and a steady involvement by their researchers in policy and strategy development (Wohlstetter, Schelling, Kahn, Kaufman), during the Cold War at least the Western military and policy makers embraced the rational actor model (RAM) to plan the strategies of nuclear deterrence. This classic deterrence theory, at the end in practice worked out till MAD, is a bold tit-for-tat-game without an option to transform a competitive relation into a cooperative one. With regard to the USSR, this strategy was developed under the assumption Soviet leaders would think and act as reasonable, rational humans as well.

From the 1970s on, new insights from the psychological, economical, and decision-making literature made the shortcomings of RAM more prominent. Graham Allison's study on the Cuba Crisis which became a bestseller, showed how organizational and political interests, processes and routines, and group think all brought the US and Russia to the brink of a nuclear exchange. Robert Jervis in turn noted that a state can rationally choose to fight a war it thinks it will probably lose if the gains of winning and/or the costs of alternative policies are great enough. Statesmen may also adopt deterrence policies that are not in the national interest because they are acting on the basis of their domestic or personal interest, so the external threat focus assumption is invalid. Third, states may create a confrontation or go to war, not in the hope of making positive gains, but in order to avoid the losses that are foreseen unless they do so. Moreover, deterrence may fail because of misperception: one side would launch a first strike not because it was aggressive or believed that war was preferable to peace, but because it was sure that the other side was about to attack and believed that striking first was better than striking second. Jervis also argued that, because the world is very complex and people's information-processing capabilities are sharply limited, we must all employ a number of short-cuts to rationality (the topic that will be discussed more fully below). For instance, people tend to act in accordance with theories they already subscribe to rather than to fresh data. Second, beliefs tend to be strongly influenced by historical analogies to recent important cases that the person or his country has experienced first-hand. The role of accidents and confusion tends to be underestimated too and other states and alliances tend to be seen as being much more centralized than they actually are. And rather than integrating many values, people often decide on the basis of a single important value dimension.[9] In the 1990s, prospect theory claimed decisions are influenced by how the issue is interpreted or

[8] E.g. Brodie 1959.

[9] E.g. Jervis 1976; Jervis et al. 1985.

framed: gaining or losing.[10] Such insights suggest that real world decision-making deviates significantly from the RAM. Rationality is where you stand (for).

In this third wave the fundaments of nuclear deterrence strategies remained. The last decades these fundaments started crumbling.[11] There are asymmetric threats (by e.g. rogue states, terrorists, refugees), paired with a new dimension: cyber, and a new constellation (at least in theory): hybrid deterrence or hybrid war. Military force and (nuclear) deterrence is no longer the sole factor. Because of this, a 'tailored deterrence' is adopted, a multidisciplinary contingency strategy for each state apart. Decision-making theory has developed as well. Physiological research on e.g. brains, and endocrinology made progress. From psychology, for example, it became clear it is not rationality, or emotion and intuition, but in decision-making they are intertwined and multi-layered.[12] Clearly research and experience has moved us well beyond the assumptions embedded in the first wave deterrence theory, and this certainly pertains to the rather simplified rationality assumption.

23.3 Rationality and the Eye of the Beholder

When trying to influence the mind of the other, it is essential to know how the mind is composed, will think and can possibly be affected. As Jervis pointed out; *it is hard to find cases of even mild international conflict in which both sides fully grasp the other's views. Yet all too often statesmen assume that their opposite numbers see the world as they see it, fail to devote sufficient resources to determining whether this is actually true, and have much more confidence in their beliefs about the other's perceptions than the evidence warrants*.[13] Aware of this trap, General De Kruif. Former commander of Regional Command South (RC-S) of the International Security Assistance Force (ISAF) in Afghanistan, stated that he therefore preferred anthropologists over country experts to explain the Afghan tribal culture.[14] Knowing how they think and what they mean by their expressions is of great help in the regular discussions with the politicians and governors. De Kruijf was involved in planning and commanding operations and worked at the locations concerned. For politicians and policymakers working in their own familiar environments, with their confidence-inspiring processes, cultures and thinking habits, it is hard to picture the party/individuals on the other side (of the world).

Even in Europe, the ways in which people in different countries think and act, and even the type of communication and language politicians use, can differ markedly. Miscommunication is a constant possibility, and the greater the cultural

[10]Tversky and Kahneman 1979.
[11]Knopf 2010.
[12]E.g. Markwica 2018.
[13]Jervis 1982.
[14]De Kruif 2018.

differences between countries, the greater the probability of misunderstanding and distortion with respect to communication and action in the context of deterrence. This can be a problem from the outset: in terms of urgency and political nuances, for example, is the sender's message attuned to the culture of the party being addressed? Moreover, many interpretations are made by all of the parties involved already in the run-up to a conflict. These interpretations are also based on assumptions about culture, strategies, policies and the personalities of the leaders. The work of, for example, Hofstede about cultural differences between countries is a bare essential.[15] Therefore, seen from a rational actor model perspective, building a deterrence strategy in a dynamic world and achieving objectives in relation to the parties involved is a blurred and befogged game. Rationality begins to fade, or rather, as Paul explains,[16] the common assumption of "instrumental rationality" is, meaning a rationality which solely looks at weighing costs and benefits. Instead, or in addition, we need to acknowledge the workings of "value rationality", values which may differ for each individual, group, or (failed) state, and which are based on ideology, religion or psychology.

The terrorist attacks of 9/11 for instance demonstrated the impact of religious fervour. As Payne observed, religion may undermine deterrence effectiveness. For instance, the superiority of an opposing force may be an insufficient deterrent against a religiously motivated actor and blind obedience to what is seen as divine will may actually compel battle with even a superior opponent. The faithful may be spurred on by a belief that providence will make them invulnerable and victorious and fighting against the odds may be considered a necessary demonstration of faith. Somewhat similarly, again following Payne, ideology may cause a state to fall victim to "mirror-imaging" and assume that an adversary's behaviour is as predictable as its own, because the adversary is motivated by the same or similar logic, values, and objectives. Mistaken threat perceptions can arise from ideological influences, leading states to perceive dangers where none exist or ignore threats with an objective reality. Significant ideological differences between two states can result in miscommunication, both in words and in actions (force deployments and exercises, for example) intended to convey intent. Some ideologies may also encompass or produce absolute goals, the attainment of which may be worth virtually any price to an adversary, something that would undermine deterrent strategies based on the opponent weighing the costs and benefits of a course of action.[17] Any deterrence strategy should therefore be based on a proper understanding of the interplay of such intangible factors such as religion, history, culture, and ideology and their impact on individual and collective cognitive processes.

[15]Hofstede et al. 2005

[16]Paul 2009.

[17]Payne 2011.

23.4 Our Thinking Patterns: Heuristics and Biases

As Janice Gross Stein already noted, neuroscience is a very important factor when translating deterrence theory into practice.[18] Indeed, research in the fields of psychology and behavioural economics during the last three decades has shed light on the dynamics at play affecting rational choice processes, in particular in high stakes contexts,[19] suggesting heuristics, biases, stereotypes, mental models and psychological fallacies in general are omnipresent. Taking advantage of the epic work of Tversky and Kahneman,[20] which should be compulsory literature for every decision maker, the following section offers a brief sketch of heuristics (rules of thumb, to put it simply) and biases (systematic errors). In our normal mode we make System 1 decisions; that is, we make decisions quickly without deliberation. To do so, relying on experience, an expert uses his skilled intuition. An amateur, not knowing the answer to a complex issue, reframes the problem in simpler terms, falling back on a heuristic. There are certain kinds of heuristics (see below). These are based on intuition, built on recognition. However, because the complex issue is redefined as a simple question and the stored recognition differs (completely) from the actual context, heuristics are by definition biased. System 2, on the other hand, is the analytical process. This takes time and energy, but the outcome is more objectively argued, even though this process does not provide the certainty that the outcome is right, or at least more right than the System 1 solution. These thinking-modes are common for deterrence as well. It is about interpretation, building the situation assessment, based on objective and/or subjective stimuli. Because both time and energy are scarce in times of crisis, System 1 is tempting. First, let us explore heuristics and biases.

Heuristics, those rules of thumb, are strategies derived from experience with similar problems, using readily accessible, though loosely applicable, information to control problem solving in human beings, machines, and abstract issues.[21] People use heuristics and biases to survive in our complex and challenging world. The automatic pilot functions to enable a person to focus on activities that require brainpower. We use heuristics in our work as well as in our daily social lives, and we start creating them from babyhood onwards. These rules work well under most circumstances, but in certain cases lead to systematic errors or cognitive biases. A heuristic is used more or less unconsciously. We have to use brainpower to identify a heuristic and discover its rationale, roots and specific construction.

Biases, on the other hand, are inclinations or prejudices for or against something or somebody. Once we have adopted one (unconsciously), there is almost no clear rational track leading from our thinking and acting back to causes or persuasions. To increase the complexity, most biases are emotionally loaded. Below six of the

[18]Stein 2009.

[19]Stein 2017.

[20]Kahneman 2011.

[21]Pearl 1983.

most common heuristics are introduced (anchoring, confirmation, availability, representativeness, affect and fluency heuristics), which will be followed by a discussion of biases that affect decision-making processes.

23.4.1 Anchoring

The anchoring heuristic is the common human tendency to rely too heavily on the first piece of information offered (the "anchor") when making a decision. We give disproportionate weight to the first information that we receive, especially when we have no clue (in chaotic and dynamic times or about an unknown area). Sometimes the anchor is in our memory, something that was once stored and is now possibly outdated or inaccurate in the current context. The given information, serving as an anchor (at least for the target of deterrence), can be deliberately inserted by the deterring party, leading to the framing heuristic (see below). In times of stress and chaos, the effect is difficult to avoid. It is like the instruction "Don't think about a pink elephant".

23.4.2 Confirmation

The confirmation heuristic is a psychological tendency to confirm evidence. It involves seeking information that supports one's existing point of view and neglecting or ignoring signs that can lead to contrary evidence. It is about assimilating new information into one's pre-existing beliefs, resulting in seeing only what one expects to be present. Ambiguous or even contradicting information is ignored, misperceived or reinterpreted so that it does minimum damage to one's own mental model. It is sometimes hard to change one's mental model of the situation and exchange it for a worse or vaguer one. In a blurred context, swapping the reliable straw that a person keeps for another straw requires mental energy and courage. The confirmation heuristic is vulnerable to biases and can evolve into tunnel vision.

An example of a confirming heuristic is the US attitude towards Japan before the start of the Pacific War in December 1941. In those days, the US military was somewhat dismissive regarding the professionalism of Japanese fighter pilots and the machines that they were flying in. In addition, the US navy expected a traditional naval war with surface ships and gave little to no attention to air raids. In the period prior to 7 December, the US Department of War, Navy headquarters and Washington, DC, received many weak signals

about Japanese plans for a massive surprise air assault on the air and naval assets at Pearl Harbor.[22] These signals, however, were not in line with existing ideas about the potency of the Japanese air force and did not confirm the US naval strategy.

A detail worth noting in this case is that the Japanese attacked Pearl Harbor from the north. The nearest Japanese naval base was to the south at Truk Lagoon. This was why the Americans conducted aerial reconnaissance only to the south. This information was provided by a collaborator from the Japanese consulate. He drove every morning to a hill to observe the direction in which the reconnaissance units flew, and it was never to the north.[23]

23.4.3 Availability

This heuristic operates on the basis of a mental shortcut that occurs when people make judgments about the probability of events according to the ease with which examples come to mind. The recognition tends to colour situational awareness and decision-making by making information that is already stored easier to recall. Because of this, some can argue that travelling by plane is far more dangerous than driving a car; almost every plane crash is newsworthy. Deterring with an action already used by some party in the past is more powerful than deterring with an action never done before, although it might have more impact when executed. Even so, the impression the events made determine how they are stored in our minds. That is why our memories are more strongly excited by a hijacked plane and the threat of the plane being flown into a building than by a hijacked cruise ship and the threat of the ship being sunk to the bottom of the ocean. The deterrence impact depends on memory. Because of this, the press, television broadcasts, newspapers and social media are instruments for mass influencers.

A special form of influencing is priming, making use of strong points of reference stored in the brain. The point of reference makes it easier for the brain to think of associated topics. For example, exposing someone to the word "yellow" will make him more likely to think of "banana" instead of "apple" when asked to name a fruit. The associations are automatic routines in the brains, individually and culturally embedded, and open to conditioning (like a Pavlov reaction).

[22]Johnson 1987.
[23]Ogilvie 1995.

The image of the drowned Syrian three-year-old boy on a Turkish beach on 2 September 2015 is a strong primer. Everyone felt a strong sense of pity for him and his family. The image forced us to think about the real problem, whether it was the war in the Middle East, the refugees or migrants, the people smugglers, or the attitude of the countries involved. These rational thoughts were nevertheless based on emotion. Priming by striking an emotional chord is a strong weapon. Think about the images of the Boeing flying into the Twin Towers, or the screaming, naked Vietnamese girl after a US napalm attack.

In several countries, billboards along roads display graphic, real-life images of the results of drunk or distracted driving. The purpose is to deter by confrontation.

23.4.4 Representativeness

This heuristic resembles the previous one. Where the availability heuristic recalls memories, the representative heuristic compares a situation with mental models in our minds. These representations are stored in our minds, based on our experiences, and are used to make our daily lives easier because they do not require energy. Stereotyping and profiling are forms of this heuristic. We all have our first impressions and immediate opinions regarding Americans, Chinese, criminals, terrorists, military personnel, crime fighters or fire fighters. Reasoning by historical analogy is an example of this heuristic as well, and the heuristic is the foundation of the proverb that the military fights a current war with the doctrine, attitude and mindset of the last war. In their own contexts, would not politicians act in the same heuristic way?

For military personnel, well-known skills and drills are examples of this live-saving heuristic. In this military context, Eikmeier even refers to acronyms as being powerful heuristics. *Acronyms used as recognition heuristics have two functions: storage and recall*.[24] In the fields of aviation, hospitals, and the military, checklists are used to ensure that protocols are carefully followed and tracked. Without doubt, checklists improve safety and enhance the quality of the processes involved. There is usually a huge world behind each item of a checklist and the person putting a checkmark is himself a subject matter expert. In this sense, one can see a checklist as a formalized memory aid, like a rule of thumb in that they are largely considered important tools to condense large quantities of knowledge in a concise fashion, reduce the frequency of errors of omission, create reliable and

[24]Eikmeier 2019.

reproducible evaluations and improve quality standards and use of best practices.[25] Returning to the subject of deterrence, checklists and lists, stereotypes and analogies can aid in recognizing the threat as real, but false analogies and hostile stereotyping can result in unnecessary escalation.

23.4.5 Affect

The affect heuristic describes the psychological process we are more positively inclined to what we like. Current emotion, possibly intentionally generated, influences decisions. In other words, it is a type of heuristic in which the emotional response, referred to as "affect" in psychological terms, plays the leading role. Deterring always gives rise to an emotional dimension. Connected with this dimension is the level of interaction and nature of the interpersonal relationship. For instance, it pertains to the distance between two persons, seated or standing, how they shake hands or react to other physical contact, poker faces and eye contact. The first impression is important, something referred to as the halo or horn effect. Music and scents play on two other senses and are used in shops, bars or restaurants to seduce.

The meetings between Vladimir Putin and Donald Trump, the two most powerful leaders in the world, are examples of talks where two completely different styles clash. Putin is a rather muscled but small person. His stone-faced behaviour betrays not a single emotion. His voice is muted and during discussions he waits for his moments to make eye contact. His background—and because of this partly his attitude and capabilities related to deterrence—is in the secret service; in working under the radar.

The US president is always physically present. When greeting he thrusts out his big right hand, grabbing the right arm of the other with his left hand and pumping it enthusiastically for rather longer than is comfortable. With this move Trump pulls the other into his personal space regardless of the values and norms and cultural descent of the other. He is aware of his length, width, weight and tanned skin and uses these to impress. His speech is always firm and loud. Not being accustomed to silence during talks (he repeats his short sentences) is perhaps linked to a lack of listening.

Introvert meets extrovert: two protagonists of completely different worlds thinking about and acting on mutual deterrence.

[25]Hales et al. 2008.

23.4.6 Fluency

The fluency heuristic is closely related to the affect heuristic. It is a mental heuristic in which, if one object is processed more fluently, faster or more smoothly than another, the mind infers that this object has the higher value with respect to the question being considered. In other words, the more skilfully or elegantly an idea is communicated, the more likely it is to be considered seriously, whether or not it is logical.

Mohammed Saeed al-Sahhaf is known for his daily press briefings in Baghdad during the 2003 invasion of Iraq, the second Gulf War. He was the Iraqi Information Minister under President Saddam Hussein. His colourful and overly convincing appearances caused him to be nicknamed "Baghdad Bob".[26] He continually spoke with theatrical sentences and made over-the-top, even absurd, claims about enormous American losses in their cowardly missions and about Iraqi courage and heroic victories. Because of his performances, he made a living caricature of himself or, to put it more strongly, became the archetype of an obvious liar. The summit in this regard was the news broadcast in which he denied that there were any American tanks in Baghdad, when in fact they were only a few hundred metres away from the press conference at which he was speaking. The combat sounds of these approaching American troops could already be heard in the background of the broadcast.

For some people, Al-Sahhaf triggered their affect and fluency heuristics. At a more abstract level, this power play in mass media is an example of deterrence, in this case luckily without teeth. He was the personified precursor of fake news.

23.5 Biases

Two types of biases are generally recognized. Framing is an example of cognitive bias in which people react to a certain stimulus. A communicator frames by stressing certain elements and omitting less effective ones, and associates some cause and effects to make his point. It concerns the presentation of the stimulus, the description, the context it is placed in and the words and medium used. The content and packaging of the message are deliberately designed to convince the receiver to accept a specific perception. When framing, one can make use of all of the

[26]Pierce and Coon 2007.

heuristics mentioned. These mental shortcuts are basically already easy prey. Framing techniques make them even more vulnerable to manipulation.

When the sender crosses a certain boundary or enters a grey zone, framing becomes fake news. In the case of deterring, fake news can be a serious weapon if the other party does not know whether the sender is serious or otherwise. Because of this obscuring move, the receiver cannot look into the mind of the sender and loses some clues in relation to the bigger picture or situational awareness regarding the sender. In a hybrid war, for example, given the speed and quantity of social media, framing is an effective tool to plant suspicion and doubt in people's minds. Framing is also the cornerstone of a successful stratagem. A magician makes use of the same psychological effect. He primes his audience by unnoticeably transferring certain stimuli. Framing is basically a marketing technique. For instance, in the case of product selling, advertisers try with the help of music, photos, movies and text to create an ideal context for each of their target audiences. The way that a product, and even a problem or an issue, is framed can profoundly influence the choices that one makes.

Soon after the two planes flew into the skyscrapers in New York on 9/11, CNN showed live broadcasting with "America under Attack" constantly visible on the screen; quite a statement, even in the chaotic "fog of attack". These written words or short sentences have a direct impact on TV viewers. With speech it is more apparent, but every written word evokes emotion as well; resonates in terms of our feelings or affect; for example, "chaos" versus "disorder" or, in the case of the 9/11 example, "America under Attack" versus "Four planes hijacked: aiming for selected buildings". One of the lesser-known changes of 9/11 was that the attacks prompted news networks to introduce the scrolling news ticker at the bottom of the screen—a powerful medium for a big audience. Since being elected as president, the same applies with respect to Trump's tweets. It is a weapon that the current US president uses very regularly for deterrence by presenting complex and interrelated challenges as straightforward, single-dimension issues. Intentionally or otherwise, he is a master of framing.

23.5.1 Prospect Theory

A second bias concern how leaders deal with risk and an overview of biases and heuristics as related to deterrence would not be complete without prospect theory. Introduced by Tversky and Kahneman, and explored further by Jack Levy, this is a behavioural economic theory that describes the way people choose between probabilistic alternatives that involve risk, where the probabilities of outcomes are

known. The theory states that people make decisions based on the potential value of losses and gains rather than the final outcome, and that people evaluate these losses and gains using certain heuristics. In contrast to rational choice, prospect theory finds that decision makers do not maximize in their choices, are apt to overweight losses with respect to comparable gains, and tend to be risk averse when confronted with choices between gains while risk acceptant when confronted with losses.[27]

Recently McDermott wrote an interesting book about this theory with some historic examples from US foreign policy decisions made by the president.[28] These cases all involve time pressure, high stakes, conditions of uncertainty and secrecy. When balancing and acting between deterring and coercing, one of the parties might interpret the situation at hand as a negative and losing one. In this scenario, prospect theory assumes that there is an increasing chance that the inferior party will execute more risky and probably unforeseen actions. Emotions such as fear of losing the conflict, shame, honour, or loss of face, losing credibility and status may play a role here. Fear leads to the three coping mechanisms: freeze, flight or fight.[29]

In a deterrence context, this can result in unforeseen actions that have a strong escalatory effect.[30] Risk-acceptant and non-maximizing behaviour, together with the effects of fear, is not automatically integrated into traditional models of deterrence that assume the rational actor perspective. In short, echoing Jack Levy, applied to deterrence dynamics, the result is that leaders are inclined to take more risks to maintain their positions, reputations etc., than they are to enhance their positions. Having suffered losses, leaders will display an aversion to accommodate to those losses but instead are willing to engage in excessive risk taking behaviour to recover lost territory. This also explains why in principle it is easier to deter an adversary from taking an action than to compel him to terminate an action or undo what he has already done. Similarly, it is easier to deter an adversary from making gains than to deter him from recovering losses.[31]

23.6 Conclusion: You Think, Therefore I Can Deter You?

Everybody is prone to these heuristics. The biggest advantage of heuristics is the fact that these pre-programmed processes in the brain are fast and frugal. Heuristics are snapshots of the mind. But when there is no hurry, how can one hold one's horses and take time to make an analytical sweep? Or, when in stress and chaos, how can one being alarmed to take a deep breath and count till three? Or, climbing out of the foxhole with skills, drills and an automated thinking pattern, switch to a

[27]Berejikian 2002.

[28]McDermott 2001.

[29]Steimer 2002.

[30]A beautiful example is Janice Gross Stein's detailed analysis of the tensions between and deterrence strategies of Israel and Egypt between 1969 and 1973: Stein 1985.

[31]Levy 1996.

more rational state? A valuable observation in relation to decision-making is: At every stage of the decision-making process, misperceptions, biases, and other tricks of the mind can influence the choices we make. Highly complex and important decisions are the most prone to distortion because they tend to involve the most assumptions, the most estimates, and the most inputs from the most people. The higher the stakes, the higher the risk of being caught in a psychological trap.[32] Therefore, forewarned is forearmed.

In face-to-face negotiations, the whole spectrum of affective behaviour, language and setting can be used to create a pressing or relaxing ambiance; from a poker face, not giving away any clue, to acted, fake emotion to provoke pity or, on the contrary, to deter seriously. A famous example of the latter is this cased ascribed to Hitler. When a British emissary arrived in July 1938, Hitler was not in the mood yet: "*Gott im Himmel*! Don't let him in yet. I'm still in a good humour." According to his assistants he proceeded "to work himself up until his face darkened, he was breathing heavily, and his eyes were glazed."[33]

Richard Nixon had played with the idea of pretending that he was going to lose his reason because of the domestic and international pressure to end US military involvement in Vietnam and end the war. One day, on a walk along a beach in California, he told Bob Haldeman, his chief of staff: *I call it the Madman theory, Bob. I want the North Vietnamese to believe I've reached the point where I might do anything to stop the war. We'll just slip the word to them that, "for God's sake, you know Nixon is obsessed about Communism. We can't restrain him when he's angry — and he has his hand on the nuclear button" — and Ho Chi Minh himself will be in Paris in two days begging for peace*.[34]

We should be aware of these heuristics and biases and that we are by nature not rational beings. One should read about, listen to, watch and learn about these psychological processes. System 2 is more analytical, but it remains unreliable because of the reality of the workings of the human mind. Working with and reflecting in a group is a second line of defence. Not only because of this pitfall, but striving for professionalism as a whole, former US president Barack Obama took steps to minimize the potential for "groupthink" to affect his political decision-making. As Coile observed, for his national security council, Obama was deliberately seeking strong personalities and strong opinions. He insisted he wanted advisers who would push back and challenge his assumptions. 'I think that's how the best decisions are made,' he said. 'One of the dangers in the White House, based on my reading of history, is that you get wrapped up in 'groupthink', and everybody agrees with everything, and there is no discussion and there are no dissenting

[32]Hammond et al. 1998.

[33]Markwica 2018.

[34]McDermott et al. 2017.

views'.[35] On the offensive side of deterrence, one has to influence the (unconscious) mind of the opponent. This requires a good understanding of the individual personalities of the leaders, their potential biases, their historical frames of references, the frames they have been using in the media to signify the nature of the crisis, and their relative power position vis a vis potential political domestic rivals. Similar information needs to be obtained concerning the group of officials included in the decision-making process. In short, awareness of heuristics and biases, one's own and those within the leadership of the opponent is essential for coping with the challenges of deterrence.

References

Allison G T, Zelikow P D (1999) Essence of Decision: Explaining the Cuban Missile Crisis, 2nd edn. Pearson

Berejikian J D (2002) A cognitive theory of deterrence. Journal of Peace Research 39.2:165–183

Brodie B (1959) The Anatomy of Deterrence. World Politics 11.2:173–191

Coile Z (2009) The Presidency in Transition: A Challenge Obama Chose. San Francisco Chronicle (11 January 2009)

Eikmeier D C (2019) Simplicity. A Tool for Working with Complexity and Chaos. Joint Forces Quarterly 92.1:30–35, 33

Hales B, Terblanche M, Fowler R, Sibbald W (2008) Development of medical checklists for improved quality of patient care. International Journal for Quality in Health Care 20.1:22–30

Hammond J S, Keeney R L, Raiffa H (1998) The Hidden Traps in Decision Making. Harvard Business Review 76.5:47–58

Hofstede G, Hofstede G J, Minkov M (2005) Cultures and Organizations: Software of the Mind, revised and expanded 3rd edn. McGraw-Hill, New York

Hudson VM (2014) Foreign policy analysis: classic and contemporary theory. Rowman & Littlefield Publishers, MD

Jervis R (1976) Perception and Misperception in International Politics. University Press, Princeton

Jervis R (1982) Deterrence and perception. International Security 7.3:3–30

Jervis R, Lebow R N, Stein J G (1985) Psychology and deterrence. Johns Hopkins University Press, Baltimore, MD

Johnson T (1987) What Every Cryptologist Should Know about Pearl Harbor. Cryptologic Quarterly 6.2:58–65

Kahneman D (2011) Thinking, fast and slow. Farrar, Straus, and Giroux, New York

Knopf J W (2010) The Fourth Wave in Deterrence Research. Contemporary Security Policy 31.1:1–33

Levy J S (1996) Loss Aversion, Framing, and Bargaining: The Implications of Prospect Theory for International Conflict. International Political Science Review 17.2:179–195

Markwica R (2018) Emotional choices: How the logic of affect shapes coercive diplomacy. University Press, Oxford

[35]Coile 2009.

McDermott R (2001) Risk-taking in international politics: Prospect theory in American foreign policy. University of Michigan Press, Michigan
McDermott R, Wernimont N, Koopman C (2011) Applying Psychology to International Studies: Challenges and Opportunities in Examining Traumatic Stress. International Studies Perspectives 12.2:119–135
McDermott R, Lopez A C, Hatemi P K (2017) Blunt Not the Heart, Enrage It: The Psychology of Revenge and Deterrence. Texas National Security Review 1.1:68–88
Morgan P M (1985) Saving Face for the Sake of Deterrence. In: Jervis R et al (eds) Psychology and Deterrence. Johns Hopkins University Press, Baltimore
Ogilvie R (1995) Krijgen is een kunst; Omtrent krijgskunde en ondernemingsstrategie. Addison-Wesley, Amsterdam
Paul T V (2009) Complex Deterrence: An Introduction. In: Paul T V, Morgan P M, Wirtz J J (eds) Complex Deterrence, Strategy in the Global Age. The University of Chicago Press, Chicago, 1–30
Payne K B (2001) The fallacies of Cold War Deterrence and a New Direction. The University Press of Kentucky, Lexington, KY
Payne K B (2011) Understanding Deterrence. Comparative Strategy 30.5:393–427
Pearl J (1983) Heuristics: Intelligent Search Strategies for Computer Problem Solving. Addison-Wesley, New York
Pierce W G, Coon R C (2007) Understanding the Link between Center of Gravity and Mission Accomplishment. Military Review 76–84
Steimer T (2002) The biology of fear- and anxiety-related behaviors. Dialogues in Clinical Neuroscience 4.3:231–249
Stein J G (1985) Calculation, Miscalculation, and Conventional Deterrence I: The View from Cairo" and "- II: The View from Jerusalem. In: Jervis R et al (eds) Psychology and Deterrence. Johns Hopkins University Press, Baltimore, 34–89
Stein J G (2009) Rational Deterrence against "Irrational" Adversaries? No Common Knowledge. In: Paul T V, Morgan P M, Wirtz J J (eds) Complex Deterrence. Strategy in the Global Age. The University of Chicago Press, Chicago, 58–84
Stein J G (2017) The micro-foundations of international relations theory: Psychology and Behavioral Economics/ International Organization 71:249–263
Tetlock P E, McGuire C B, Mitchell G (1991) Psychological Perspectives on Nuclear Deterrence. Annual Review of Psychology 42.1:239–276
Tversky A, Kahneman D (1979) Prospect Theory: An Analysis of Decision under Risk. Econometrica 47.2:263–291

Tom Bijlsma is assistant professor in military management. A graduate of the Royal Military Academy and former army officer he obtained his Ph.D. at Tilburg University. His research focuses on team learning and decision making.

Chapter 24
Deterrence: A Continuation of Emotional Life with the Admixture of Violent Means

Samuel Zilincik and Isabelle Duyvesteyn

Contents

> "*...emotions may be slippery, but they are also by far the most salient aspect of our lives. They give meaning to everything*."
> De Waal 2019, 9–10

Abstract Deterrence is more than anything a psychological mechanism. It depends on emotions that orchestrate processes across organisms to deal with the challenges of the present and the future. However, deterrence scholarship has had a turbulent relationship with emotions. The main aim of this chapter is to review what we know and what we do not know about emotions and deterrence. The secondary aim is to

S. Zilincik (✉)
University of Defence, Brno, Czech Republic
e-mail: zilinciks@gmail.com

I. Duyvesteyn
Institute of History, Leiden University, Leiden, The Netherlands
e-mail: i.g.b.m.duijvesteijn@hum.leidenuniv.nl

F. Osinga and T. Sweijs (eds.), *NL ARMS Netherlands Annual Review of Military Studies 2020*, NL ARMS, https://doi.org/10.1007/978-94-6265-419-8_24

develop a dynamic and interactive emotion-centric model of deterrence to explain where and how emotions play a role in such a mechanism. We combine the methods of theoretical analysis and literature review to achieve these aims. Our findings indicate that emotions give a new meaning to deterrence by changing the nature of the theory and by highlighting problems of practice. More specifically, scholars should reconsider both the means and the ends of deterrence. Practitioners should be aware that deterrence efforts are hard to sustain and may produce emotional effects detrimental to their original purpose.

Keywords emotions · deterrence · psychology · perception · decision-making · fear · anger · happiness

24.1 Introduction

While traditionally seen as strategy, deterrence is, more than anything, a psychological mechanism.[1] Deterrence is commonly known to comprise the practice, the process or the situation in which one actor relies on a prospect of harm to persuade an opponent not to engage in certain specified behaviour. This notion does not do justice to the salience of the adversary's agency in the whole process. It is the adversary who decides the outcome, or, more precisely, the emotions of the adversary.

Recent research on emotions questions the traditional understanding of deterrence. Emotions are not only the consequences of the defender's actions; they emerge through the challenger's interpretation of the situation.[2] Once triggered, specific emotions affect cognitive processes and action (or inaction) in far more sophisticated ways than has been assumed.[3] Finally, emotions may spread, affecting both domestic and foreign politics and producing second-order effects unintended by the original deterrent efforts.[4] In sum, contemporary research on emotions gives a new meaning to the very nature of deterrence.

Emotions overlap with several biological and psychological processes already discussed in the mainstream deterrence literature. Hormones and other neurotransmitters are essential for emotions to emerge and their influence on deterrence has already been explored.[5] Emotions, in turn, are responsible for different kinds of

[1]Payne 2001, p. 30.
[2]Roseman and Smith 2001, p. 3.
[3]Lerner et al. 2015.
[4]Van Kleef and Fischer 2016.
[5]Payne 2011, pp. 401–403.

biases that affect decision-making and judgments.[6] Indeed, recent research indicates that this applies even to the effects of framing predicted by prospect theory.[7] Likewise, specific emotions affect perceptions and, therefore, change how the individual sees the world.[8] Similarly, emotions and stress interact in dynamic ways.[9] Finally, emotions affect thoughts and beliefs and indirectly shape what some deterrence scholars have labelled "operational codes" of decision-making.[10] Emotions are the one element that orchestrates all these processes to prepare individuals for the future.[11] Therefore, by exploring emotions, this contribution aims to enhance our understanding of the psychology behind deterrence.

What do we know and what do we not know about emotions and deterrence? Apart from answering this question, the chapter also develops a dynamic and interactive emotion-centric model of deterrence to explain where and how emotions play a role in the mechanism. The rationale behind these two aims is to develop a tool to examine deterrence from a unique, emotional perspective. The methods to do so include theoretical analysis and a literature review. We understand emotions to be "complex, organized subsystems consisting of thoughts, beliefs, motives, meanings, subjective bodily experiences, and physiological states".[12] This definition encompasses the relevant components of emotions as identified by various emotion theories. However, the definition itself is rooted in the appraisal theory of emotions, which argues that emotions emerge as a consequence of one's appraisal of reality rather than as a result of a simple interaction with the world.[13] This is a deliberate choice, because the theory has a decent track-record of success when it comes to studying emotions in social settings.[14] As such, the appraisal theory of emotions constitutes the best lens available to explore the role of emotion in deterrence.

By dissecting the emotions related to deterrence, the chapter contributes to the academic debate, as well as offering insights for practical decision-making. The academic contribution resides in the interdisciplinary synthesis of psychological research on emotion with social scientific research on deterrence. Additionally, the chapter also contributes to the literature on emotions in international relations and

[6]Engelmann and Hare 2018; Jervis et al. 1985.

[7]Druckman and McDermott 2008; Stein 2013, p. 384. For the initial work on prospect theory, see Kahneman et al. 1982.

[8]Stein 2013, pp. 379–81; Zadra and Clore 2011.

[9]Lazarus 1993. For the initial treatments of stress in deterrence literature, see Holsti and George 1975.

[10]Frijda and Mesquita 2000; George 1967.

[11]Scherer 2013; Cosmides and Tooby 2000.

[12]Lazarus 2001, p. 67.

[13]For a comprehensive overview of emotion theories, see Moors 2009.

[14]Halperin 2015; Markwica 2018.

strategic studies in general.[15] The argument contributes to political and military practice, enabling practitioners to better understand the emotional effects elicited by their (or their adversary's) use of deterrents. This, in turn, may enable states (wo)men to manipulate these effects to their advantage, or at least to negate the emotional effects desired by the adversary.

The following section introduces the main themes of contemporary emotion science and reflects on how these themes have been incorporated into the deterrence literature. Based on this assessment, we then proceed to develop a dynamic emotion-centric model of deterrence. Consequently, we examine its explanatory power by looking a case of the deterrent efforts between the United States and Iran in early 2020. The concluding section summarizes the implications of our argument.

24.2 Salient Themes of Contemporary Emotion Science as Reflected in Deterrence Literature

The psychological study of emotions has been flourishing for the last four decades. New techniques, such as magnetic resonance imaging, have enabled experts to study emotions in unprecedented ways. Scientists can now trace emotional reactions across the human brain. As a result, new emotion theories have been developed, transforming our understanding of what emotions are, how they emerge, and what their influence is. The vast pool of all these fascinating propositions far exceeds the scope of this chapter.[16] We have selected the themes which are particularly relevant for deterrence and organized the literature review around them. The themes include: the emergence of emotions through interpretation, the influence of specific emotions on cognition and action, and the issue of individual emotions within collectives (see Table 24.1). In discussing the themes, we focus mostly on the emotions of fear, anger and happiness. While we also discuss other emotions in passing, we have chosen these three because of their varied and often diverging characteristics as well as their common occurrence in everyday (political) life. Finally, these three emotions are familiar to people across the world, which makes it easier for our readers to relate to them.[17]

[15]For a good introduction to emotions in international relations, see Ariffin et al. 2016. For similar efforts in strategic studies, see Payne 2018, 2015.

[16]See for example Keltner et al. 2014.

[17]Izard 2007.

Table 24.1 Characteristics of fear, anger, and happiness

Emotion	Situation for emergence	Impact on cognition	Impact on behaviour
Fear	Appraisal of threat to one's objectives	– Risk aversion – Pessimism – Feeling a lack of control – Feeling uncertainty – Expecting high effort to improve the situation	Motivates freeze, flight, and fight responses
Anger	Appraisal of access to one's objectives being blocked by the specific other	– Risk acceptance – Optimism – Feeling in control of the situation – Feeling certain about the situation – Expecting high effort to improve the situation	Motivates punishment of others
Happiness	Appraisal of successful access to one's objectives	– Risk acceptance – Optimism – Feeling in control of the situation – Feeling certain about the situation – Expecting low effort to improve the situation	Motivates the continuation of the activity or its termination (depends on whether the goals have already been achieved or not)

We derived the data included in this Table from Druckman and McDermott 2008; Lerner and Keltner 2000; Lerner and Tiedens 2006; Smith and Ellsworth 1985; Turowski, Man, and Cunningham 2014

24.3 Emotions and Interpretation

Emotions do not "just happen" to us, nor do deterrent efforts produce the desired emotions automatically. It is a person's interpretation of the situation that determines if emotions emerge and what shape they take.[18] First, the situation has to be appraised as relevant.[19] People do not experience emotions about issues they do not care about. Furthermore, the character of the ensuing emotion depends on the meaning we derive from the situation.[20] Fear, for example, is likely to appear when an individual feels access to their objectives threatened, anger when the access to their objectives is blocked, and happiness when one feels unrestricted access to their objectives.[21] Deterrent efforts can elicit any of these emotions, as well as others, but the conversion between deterrence threats and emotions is subjective, unstable and non-linear.

Deterrence scholars have progressed considerably in their understanding of how emotions emerge. Early experts considered the link between actions and emotions to be straightforward: the defender would mount a threat and the challenger would subsequently be frightened.[22] There was little room reserved for interpretation. This (mis)understanding changed with the third wave of deterrence scholarship. Scholars such as Robert Jervis, Richard Lebow and Janice Gross Stein found that the challenger often failed to care enough or that he/she interpreted the "threats" in different ways than the defender intended.[23] As Lebow points out, threats may be interpreted as provocations and, therefore, trigger anger instead of fear.[24] Some of the recent works on deterrence have started to emphasize interpretation as the key to emotion elicitation. Robin Markwica's *Emotion Choices* is a good example, since the author specifically relied on the appraisal theory of emotions to make his argument.[25] Though not yet mainstream knowledge, the role of interpretation in deterrence practice has started to be taken seriously in recent years.

However, there is a lot more we do not know. The emergence of specific emotions on the side of the defender deserves more attention. Psychological states of defenders are rarely examined in deterrence scholarship.[26] At the same time, a defender's emotions constitute the engine for the whole deterrence process. Successful deterrent efforts may make the defender happy while ignored one may

[18]Moors 2013.

[19]Frijda and Mesquita 2000.

[20]Lazarus 2001.

[21]Smith and Ellsworth 1985.

[22]Herman Kahn, for example, emphasized that deterrents should be "frightening", as if that quality, like all the others he lists, depended on the inherent nature of the tool rather than on the interpretation of the adversary. See the table in Kahn 1961, p. 146.

[23]Jervis et al. 1985. See also Payne 2001, p. 31.

[24]Lebow 2008, p. 552.

[25]Markwica 2018.

[26]For a small set of exceptions, see Jervis et al. 1985.

make him frightened or angry. As the following section will show, the difference between the specific emotion experienced may contribute to the maintenance or to the termination of deterrent efforts. The focus on the defender's emotions is also important because emotions associated with deterrent efforts may gradually lead to institutional changes at the home front.[27] It is, therefore, necessary to know how deterrence activity affects the emotions of those who conduct it so as to minimize deterrence failures and unwanted institutional transformation.

24.4 Emotions and Influence

Specific emotions are unequal in their influence on deterrent efforts. Emotions, both those experienced and sometimes even those merely anticipated, influence cognition and behaviour in diverse ways. Psychological research is now clear that the differences go beyond the simple distinction between positive and negative emotions.[28] Anger, for example, is a negative emotion, like fear. However, while fear tends to make people more risk-averse and pessimistic, anger tends to make people feel risk-prone and optimistic.[29] In this respect, anger resembles positive emotions more, such as happiness.[30] Furthermore, the behavioural influence of emotions varies with context. Fear, for example, can motivate freezing, fleeing, or fighting.[31] Happiness may motivate both the relaxation of efforts and their pursuit, depending on whether the emotion is experienced or merely anticipated in the future.[32] Nonetheless, the research also shows that all emotions may provide a basis for rational-decision making and action if their experience is appropriate to the character of the situation.[33] Indeed, emotions are essential to take any decision, rational or not.[34] This is because emotions make us care about the consequences of our actions, which in turn enable us to choose from competing objectives in any given context.[35] The varied and sometimes contradictory influence of specific emotions makes deterrence efforts a real gamble. The odds for deterrence success may be improved by educated anticipation but not by reliable prediction.

Deterrence scholarship has progressed gradually in its understanding of emotional influence. Early deterrence scholars viewed emotions as mere adjuncts to rational calculation, without appreciating the variance in influence. Fear, for

[27]Lupovici 2018; Sauer 2015.
[28]Angie et al. 2011; Druckman and McDermott 2008; Lerner and Keltner 2000.
[29]Keltner and Lerner 2001.
[30]Lerner and Tiedens 2006.
[31]Steimer 2002.
[32]Turowski et al. 2014.
[33]Hacker 2018, pp. 71–77.
[34]Phelps et al. 2014.
[35]Damasio 2005.

example, was the only emotion discussed but its variable influence on behaviour was not appreciated.[36] It is plausible that these early scholars did not consider fear to be a real emotion.[37] Rather it was "something merely mentioned in passing, definitely not a thing to be dealt with analytically and in its own right".[38] The central assumption of initial deterrence theorists was that the defender was to use a threat of force to elicit fear, and then to rely on the rational calculation of the opponent to submit to the former's will.[39] This assumption would only be valid if fear had no influence on cognition or if it always enhanced rationality in the same ways.[40] These conditions, however, did not correspond to reality. Early deterrence experts thus believed in a psychological mechanism, which in light of today's psychological science would be untenable.

This faulty understanding has been gradually corrected from the third wave of deterrence research onward. A group of scholars in this tradition employed insights from psychological sciences to point out how emotions (through motivated biases) impede rational calculation.[41] This recognition was important progress, as it provided a basis for more elaborate treatments of the role of emotions. In this vein, Crawford, Lebow, and Stein acknowledged that fear may have a diverging influence in different contexts.[42] Some recent works have broadened the scope of the investigation to include emotions beyond fear, such as disappointment, shame, humiliation, anger or empathy.[43] Markwica went even further, as he empirically tested the influence of five different emotions (fear, anger, pride, hope, humiliation) with mixed valence. His research showed that emotions, such as fear and humiliation, can lead the target of deterrence to back down or to resist depending on the context.[44] Recent works have also acknowledged that specific emotions do not necessarily impede rationality but that they can contribute to it.[45] Overall, this strand of scholarship demonstrates considerable progress in our understanding of the emotional complexity associated with deterrence.

Similar progress relates to emotional anticipation and its relationship with deterrence. In a crude sense, the anticipation of an emotion has always been part of deterrence theory. It is the anticipated causal link between threat and fear which constitutes the theory of victory in traditional deterrence literature.[46] Recent

[36]Schelling 1966, p. 36.

[37]Crawford 2000, pp. 145–146.

[38]Sauer 2015, p. 111.

[39]Crawford 2013, p. 121.

[40]Even some four decades ago, Patrick Morgan found the assumption puzzling, see Morgan 1983, pp. 21–22; Crawford 2000, pp. 146–147.

[41]Jervis 1976; Jervis et al. 1985; Lebow and Stein 1989.

[42]Crawford 2000, 148; Lebow 2008, 91; Stein and Lotan 2019, pp. 70–71.

[43]Stein 2012, 57; Crawford 2014, pp. 545–546.

[44]Markwica 2018, 17–18.

[45]Markwica 2018, 66–67; Mercer 2005, 2010; Stein 2012, 2013; Thayer 2007, 316–318.

[46]Schelling 2008, x.

research has explored the anticipation of emotions beyond fear. For example, several scholars have argued that the anticipation of hatred and anger form the basis of credibility in deterrence by punishment.[47] The challenger may abstain from the attack if he/she anticipates that the adversary will retaliate so as to feel the pleasantness of revenge.[48] From a different perspective, Thomas Dolan argues that it is the anticipation of future negative emotions such as shame, guilt and anger that discourages challengers from violating taboos.[49] Emotional anticipation, though more complicated than often assumed, is at the heart of both deterrence theory and practice.

We still need to know more about other emotions and their relationship to deterrence. Even the more conservative emotion theorists now acknowledge the existence of more than twenty unique emotional states.[50] For instance, we know little about happiness, joy, interest, curiosity, disgust, regret, grief, hatred or guilt. The influence of some emotions may be beneficial to deterrent efforts, while the influence of others is likely to be detrimental. Happiness is particularly interesting because of its ambiguous influence on motivation. It is far from clear whether the use of inducements, as some experts advise, to make the adversary happy is a reliable recipe for deterrence success. Happy adversaries may easily grow confident and risk-prone, which is not always beneficial for the defender. What is clear is that deterrence theory needs to acknowledge the differences in influence of specific emotions. Without the ability to comprehend all the emotional variations, deterrence practitioners risk the possibility of creating effects which may undermine their own efforts.

24.5 Emotions in Collectives

Deterrence aims at individuals but it may ignite emotions in whole societies. Members of smaller groups can experience similar emotions when they interact with each other. Sharing emotions with others is contagious, as humans are good at copying each other's emotional expressions.[51] However, even members of large collectives can experience similar emotions. This can occur through shared appraisals rooted in collective identity but also through top-down emotional transmission from the political elites to the rest of the society.[52] Collective feelings of happiness are common after a national sport team achieves success, while collective anger and fear often follow terrorist attacks.[53] Importantly, the emergence,

[47]Löwenheim and Heimann 2008; McDermott et al. 2017; Jervis 2017, p. lxxi.
[48]McDermott et al. 2017, p. 71.
[49]Dolan 2013, pp. 42–43.
[50]Keltner 2019.
[51]Van Kleef and Fischer 2016, 7–8.
[52]Van Kleef and Fischer 2016, p. 6; Hall and Ross 2019, pp. 1360–1363.
[53]Hall and Ross 2015.

experience and expression of some emotions varies across cultures.[54] It follows that deterrent efforts may produce a variety of emotions, that can further transform the political landscapes of whole societies and this transformation may be influenced by cultural specifics.

Deterrence scholarship has made great progress in its understanding of emotions in collectives. The first-generation scholars of deterrence research assumed states to be unitary actors, with no difference between individual and collective emotions.[55] Recent deterrence research on collective emotions deals predominantly with so-called incidental emotions. These are the emotions present in collectives before the deterrence efforts take place and they influence the emergence of subsequent emotions.[56] Crawford and Lebow, for example, have both argued that the institutions of some polities may be inherently rooted in fear and this emotion then influences responses to deterrence.[57] Amir Lupovici argues that this kind of emotional institutionalization may lead defenders to tie their identity to deterrent efforts that protect them from the experience of undesired emotions.[58] Stein, drawing attention to the variance in strategic cultures, has argued that political elites from the so-called "honour" cultures may experience different emotions than Western thinkers assume.[59] Collective emotions in their incidental forms have been explored on both sides of the deterrence relationship.

Still, we know little about the interaction between collective emotions and strategic cultures. Since the emergence and the experience of emotions differs across cultures, this gives a whole new meaning to the idea of tailored deterrence. It means that eliciting particular collective emotions may be impossible in some strategic cultures or that the experience itself may vary considerably. It is therefore essential to know the peculiarities of specific strategic cultures to increase the chances of successful emotional manipulation by deterrence.

24.6 The Emotion-Centric Model of Deterrence

So far we have only discussed emotions in a static manner; now is the time to make them dynamic. Accordingly, we present a model (see Fig. 24.1) which explains where and how emotions play a role as related to the deterrence mechanism. The model brings together all the themes discussed in the previous sections. In

[54]Barrett 2017, pp. 145–150. For more details, see Fontaine et al. 2013, ch 20–26.
[55]Achen and Snidal 1989, p. 150.
[56]Renshon and Lerner 2012, pp. 1–2.
[57]Crawford 2009, 2013; Lebow 2008, pp. 89–92.
[58]Lupovici 2018, pp. 6, 65–69.
[59]Stein 2012, pp. 60.

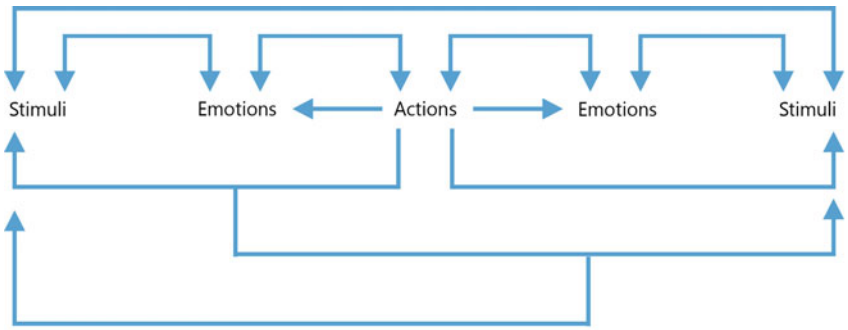

Fig. 24.1 Interactive and dynamic model of emotions and deterrence (*Source* The authors)

constructing the model, we have been inspired by similar models on emotions already developed by social scientists.[60] We argue that the model is necessary to understand the psychological factors of deterrence, but it is not sufficient—those seeking a holistic psychological understanding of deterrence should combine the model with other works on deterrence psychology.[61] The model is emotion-centric in nature; it pays attention to emotions at the expense of other psychological considerations to emphasize their importance.[62]

The model is circular rather than linear. Emotions, rooted in either domestic or political concerns, play a role even before the deterrent activity takes place. Depending on the specific emotions, the defender either chooses to launch the deterrent activity or to abstain from it. On the other side of the equation, the same motivational force of emotions influences the challenger's decision to attack. Simultaneously, both defender and challenger can be (de)motivated to act by their own anticipation of the adversary's emotions or by the adversary's expressions of emotions. The next step is the deterrence itself and the emotions it triggers on the side of defender, challenger, and potential observers. This is further complicated by the fact that few of these actors are emotionally unitary. On the contrary, different segments of populations within one polity are likely to draw diverse interpretations, based on their own biases, prejudices, opinions, desires, memories, perceptions, and incidental emotions. The emotions and their anticipation influence the further thoughts and actions of all affected actors. Emotions, therefore, complete a full circle from being an initial motivation, to being transformed through interpretation, to again being the driving force of thought and action. Thus, though emotions may change over time, they never stop being a relevant factor in the deterrence mechanism.

[60]Halperin 2015; Lerner et al. 2015; Markwica 2018.

[61]See for example Payne 2001, pp. 104–14.

[62]Roy 2016.

We now turn to explore this model further by looking at case material; the highly volatile relationship between the United States and Iran, which experienced a severe crisis in January 2020.

24.7 US–Iran Case Study

On 3 January 2020, the leader of the Iranian Revolutionary Guard Quds Force Qasim Suleimani was killed by a Hellfire missile fired from an American drone.[63] The killing of Suleimani has been justified by the United States' government as a significant reinforcement of deterrence: 'This strike was aimed at deterring future Iranian attack plans. The United States will continue to take all necessary action to protect our people and our interests wherever they are around the world'.[64] This assertion is consistent with observations of other experts.[65] We therefore use this case to illustrate where, when and how emotions played a role in the deterrence mechanism. Our focus is on a small set of the most common emotions (fear, anger, happiness) that have surfaced in the notable analyses of the case. The analysis explores the role of these emotions in the two phases delineated in the model above. To identify the presence of specific emotions we reviewed journalistic and professional commentaries of the event. In terms of coding, we searched for particular emotion words as well as words from the associated emotion families—not only fear but also worries, anxiety, horror, et cetera. Additionally, we used the characteristics of specific emotions to infer their presence by the appearance of the relevant stimuli, as well as to explain how particular emotions may have contributed to the specific choices and demonstrated behaviours. While we primarily focus on emotions within the US and Iran, the main actors in the confrontation, collateral emotions of others are also discussed.

24.7.1 Phase 1: Emotions before Deterrence

Anger (along with hatred) was certainly present in the American administration and security services. Many members of these collectives considered Suleimani responsible for American soldiers being killed during the Iraq War.[66] The American political establishment was also angry that, despite the stringent sanctions regime, Iran had been able to increase and strengthen its position in the region, in its quest for regional hegemony. Conversely, the US had been losing allies and influence in

[63] Al Jazeera 2020b.
[64] Department of Defense 2020.
[65] Seligman 2020.
[66] Jervis 2020.

the Middle East, partly by choice, e.g. withdrawal from northern Syria. It had fewer friends and more enemies, and their 'recourse to brute force is always a sign of lost legitimacy and authority'.[67] Anger at Iranian responsibility for American losses may have motivated the US president to use violence to remove Suleimani without regard for long-term consequences.

Stimuli for fear were also abundant. Before the attack against Suleimani, American credibility was perceived as being at stake. A whole series of attacks against American targets had gone unanswered.[68] In an interview with *Foreign Policy*, General David Petraeus elaborated on the weak American deterrent position: 'Many people had rightly questioned whether American deterrence had eroded somewhat because of the relatively insignificant responses to the earlier actions'.[69] In an analysis in the *New Statesmen*, Lawrence Freedman argued along similar lines, 'Iranians shooting down an American drone over the Strait of Hormuz in June 2019, and allegedly attacking a Saudi Aramco oil facility later that year; Trump refused to authorize retaliatory airstrikes. So tepid was his response that Tehran was emboldened—they saw Trump as something of a paper tiger, big on boasts but short on action'.[70] Another source of American fear may have been a perceived danger of imminent attack.[71] Attacks against the American compounds in Iraq had directly preceded the drone strike. Furthermore, the president in his public justification for the murder, mentioned intelligence reports, later retracted, of imminent threats. Fear could have motivated Trump to fight and fortify the US position.

Stimuli for happiness were also present. The establishment saw great luck in being given the opportunity to kill Suleimani. In a Hoover Institute speech, the secretary of state, Mike Pompeo, claimed that 'had we not taken that strike against Qasem Soleimani, our leadership—the recommendation that we made to President Trump—we would have been "culpably negligent" had we not made that recommendation, imposed a significant cost on the regime for their bad decision'.[72] Simultaneously, the administration also probably, and not unreasonably, anticipated large parts of the US domestic public to feel happy after hearing about the general's death. Happiness elicited in such a way could have motivated them to pursue their plan as the successful achievement of their objectives seemed at hand.

In Iran, fear was commonplace. The US policies in the region were often interpreted as threatening and dangerous.[73] The sanctions had started to hurt, and two days before the attack on 1 January, the Iranian president had gone on national

[67]Mishra 2020.
[68]Al Jazeera 2020b.
[69]Seligman 2020.
[70]Freedman 2020.
[71]Riley-Smith 2020.
[72]Pompeo 2020.
[73]Strobel et al. 2019.

television to state as much.[74] Moreover, there were probably fears about the stability of the regime. People had started taking to the streets in Iraq and Lebanon to demonstrate against Iranian influence, e.g., the attacks against the Iranian consulates in Najaf and Karbala.[75] In Iran, people had been protesting in the preceding months against rising prices for petrol.[76] Fears of domestic and foreign threats produced a powerful incidental emotion on the side of the regime.

24.7.2 Phase 2: Deterrence and the Emergence of Emotions

The attack elicited a kaleidoscopic range of emotions across the world. These, of course, depended upon the individual's and group's interpretations of the situation. Furthermore, states experienced no emotional unity in the aftermath. In the US context, some conservatives saw the drone strike as a legitimate act of defence and revenge, and thus felt happy afterward.[77] Pompeo expressed himself confidently: 'We now enjoy a great position of strength regarding Iran. It's as good as it has ever been, and Iran has never been in the place that it is today.'[78] Democrats had already despised Trump before the attack; it is understandable that they interpreted the activity unfavourably and felt angry.[79] Seeing the assassination as a dangerous precedent, some commentators felt fear as they anticipated the anger of the Iranians.[80]

In Iran, thousands felt angry, for they interpreted the attack as an act of American malevolence and an obstacle to their security.[81] The supreme leader Ayatollah Khamenei said in a statement that 'harsh revenge' would be enacted against the United States for killing Suleimani.[82] Furthermore, public demonstrations showed a measure of anger among the Iranian public.[83] However, the regime was at the same time scared of further escalation, and rightly so. Military conflict with the US would be devastating for the already fragile polity. The evidence of fear is also implied by the relatively harmless way in which Iran chose to respond: an attack against American installations in Iran without causing any casualties, which is a clear effort

[74]The speech by President Rouhani is available in Asharq Al-Awsat 2020. See also the commentary by Goldman 2020.

[75]Reimer 2020.

[76]Johnson 2019.

[77]Associated Press 2020.

[78]Seligman and Gramer 2020.

[79]Associated Press 2020; Risen 2020; Rove 2020.

[80]Ward 2020.

[81]Knights 2020.

[82]Al Jazeera 2020a.

[83]Naji 2020.

to de-escalate.[84] Furthermore, it may be that some individuals and groups were happy. After all, the US attack enhanced the cohesion of Iranian society after the weeks of unrest.[85] The regime might interpret this as a successful development in accordance with its goals and experience happiness in the aftermath.

Then there were collateral emotions experienced by many others. Some Syrians and Iraqis felt happy, as they celebrated the death of their long-time enemy.[86] Many in Europe felt scared because of the appraised threat of further escalation of violence.[87] Instead of being confined to their original locations, many of these emotions and their anticipations spread rapidly throughout the world via social media.

24.8 Conclusion

We started the chapter by observing that emotions give meaning to practically everything. Our review indicates that emotions may well give new meaning to deterrence itself. They alter our understanding of deterrence in three ways. First, emotions form the essence of deterrence. Other psychological processes, such as perception, attention, judgment, memory, or thought, are less relevant, if emotions are not taken into account. This is not to say that these cognitive processes are less important, but emotions are the one element that synchronizes all of them so as to prepare individuals to face the challenges of the present and the future. Any examination of deterrence, in theory and in practice, needs to start from an emotion-centric perspective and then move to add other psychological elements. The model we have developed in this chapter may be refined as new insights about emotions are revealed, but it could be a stepping stone for psychological understandings of deterrent efforts and their consequences.

Second, emotions give a new meaning to the content of both means and ends in deterrence theory. The fundamental causal mechanism behind deterrence, the issuing of threats to produce fear, requires refinement. Threats, even if perfectly signalled, attributed and credible, need to be interpreted as relevant and as threats. Otherwise, they do not elicit emotions at all or they may elicit ones that are detrimental to the whole effort. To alleviate the problem, we may incorporate the actual use of violence into existing deterrence theory, as illustrated by our case study and Chap. 14 by Eitan Shamir in this volume. Of course, even the use of violence is open to interpretation. However, space for interpretation is inherently smaller compared to verbal threats or positioning of weapon systems. Additionally, deterrence theory needs to expand its psychological content. Emotions other than

[84]The regime responded by first warning and then attacking American positions in Iraq but no casualties occurred in the aftermath. See BBC 2020.

[85]Esfandiary 2020; Mishra 2020.

[86]Hamid 2020.

[87]Wintour 2020.

fear may be useful for deterrent purposes. It may be that conceptual content will be enhanced gradually as more emotions prove useful for deterrent purposes. Eventually, this content expansion may in turn necessitate the re-examination of the means by which the emotional effects are to be accomplished. In short, the incorporation of varied emotions may transform the very nature of deterrence theory.

Third, deterrence practice is more complex than usually assumed. Above all, the insights from emotion sciences indicate that we have little control over emotions and, therefore, cognition and behaviour of others. Furthermore, actors from some strategic cultures may be undeterrable simply because they cannot experience the intended emotions or because they experience them differently. The tailoring of deterrence efforts to particular adversaries needs to include an assessment of the latter's emotional profiles, histories and cultures. Then there is the problem of collateral emotions. Deterrence is never an isolated act. It affects the domestic and foreign politics of direct participants and observers alike. Or, to put it in more strategically pleasing jargon, deterrence is just a continuation of emotional life with the admixture of violent means. Some of the collective emotions are beneficial, others detrimental. Deterrence practice needs to incorporate anticipation of these emotional effects so as to enable their countering. Otherwise, the failures of deterrence may not only lead to the adversary's attacks but also to the transformation of the defender's own institutions. In sum, deterrence practice is much more about the diverse nature of emotions than about simple cost/benefit calculations.

References

Achen C H H, Snidal D (1989) Rational Deterrence Theory and Comparative Case Studies. World Politics 41:143–169

Al Jazeera (2020a) Iran in Mourning, Vows Revenge for Qassem Soleimani's Killing. https://www.aljazeera.com/news/2020/01/iran-mourning-vows-revenge-qassem-soleimani-killing-200103100607193.html. Accessed 30 May 2020

Al Jazeera (2020b) US-Iran Tensions; Timeline of Events Leading to the Soleimani Killing. https://www.aljazeera.com/news/2020/01/iran-tensions-timeline-events-leading-soleimani-killing-200103152234464.html. Accessed 30 May 2020

Angie A D, Connelly S, Waples E P, Kligyte V (2011) The Influence of Discrete Emotions on Judgement and Decision-Making: A Metaanalytic Review. Cognition and Emotion 25:1393–1422

Ariffin Y, Coicaud J M, Popovski V (2016) Emotions in International Politics. Cambridge University Press, New York

Asharq A A (2020) Iran President: US Sanctions Cost Country $200 Billion. https://aawsat.com/english/home/article/2061761/iran-president-us-sanctions-cost-country-200-billion. Accessed 30 May 2020

Associated Press (2020) Here's How 2020 Democrats Are Reacting to the U.S. Assassination of Iran's Qasem Soleimani. https://time.com/5758264/qasem-soleimani-2020-democrat-reaction/. Accessed 30 May 2020

Barrett L F (2017) How Emotions Are Made. Houghton Mifflin Harcourt, New York

BBC (2020) 'Iran Missile Attack: Did Tehran Intentionally Avoid US Casualties?' BBC, 8 January 2020. https://www.bbc.com/news/world-middle-east-51042156. Accessed 30 May 2020

Cosmides L, Tooby J (2000) Evolutionary Psychology and the Emotions. In: Lewis M, Haviland-Jones J M (eds) Handbook of Emotions. The Guilford Press, New York, 91–115
Crawford N (2000) The Passion of World Politics: Propositions on Emotion and Emotional Relationships. International Security 24:116–156
Crawford N (2009) Human Nature and World Politics: Rethinking "Man". International Relations 23:280–82
Crawford N (2013) Emotions and International Security: Cave! Hic Libido. Critical Studies on Security 1:121–23
Crawford N (2014) Institutionalizing Passion in World Politics: Fear and Empathy. International Theory 6:535–57
Damasio A (2005) Descartes' Error: Emotion, Reason, and the Human Brain. Penguin Books, New York
De Waal F (2019) Mama's Last Hug: Animal Emotions and What They Tell Us about Ourselves. Norton and Company, New York
Department of Defense (2020) Statement by the Department of Defense. https://www.defense.gov/Newsroom/Releases/Release/Article/2049534/statement-by-the-department-of-defense/. Accessed 30 May 2020
Dolan T M (2013) Unthinkable and Tragic: The Psychology of Weapons Taboos in War. International Organization 67:37–63
Druckman J N, McDermott R (2008) Emotion and the Framing of Risky Choice. Political Behaviour 30:297–321
Engelmann J B, Hare T A (2018) Emotions Can Bias Decision-Making Processes by Promoting Specific Behavioural Tendencies. In: Fox et al (eds) The Nature of Emotion: Fundamental Questions. Oxford University Press, New York, 355–359
Esfandiary D (2020) By Killing Qassem Suleimani Trump Has Achieved the Impossible, Uniting Iran https://www.theguardian.com/commentisfree/2020/jan/07/qassem-suleimani-trump-uniting-iran-assassination-government. Accessed 30 May 2020
Fontaine J J R, Scherer K J, Soriano C (2013) Components of Emotional Meaning: A Sourcebook. Oxford University Press, Oxford
Freedman L (2020) Death of a Warlord. https://www.newstatesman.com/world/middle-east/2020/01/death-warlord. Accessed 30 May 2020
Frijda N, Mesquita B (2000) Beliefs Through Emotions. In: Frijda N, Manstead A, Bem S (eds) Emotions and Beliefs: How Feelings Influence Thoughts. Cambridge University Press, Cambridge, 45–64
George A (1967) The "Operational Code": A Neglected Approach to the Study of Political Leaders and Decision-Making. RAND Corporation, Santa Monica
Goldman D P (2020) How Fragile Is Iran's Regime? https://www.asiatimes.com/2020/01/article/how-fragile-is-irans-regime-2/. Accessed 30 May 2020
Hacker P M S (2018) The Passions: A Study of Human Nature. Blackwell, Oxford
Hall T H, Ross A A G (2015) Affective Politics after 9/11. International Organization 69:847–879
Hall T H, Ross A A G (2019) Rethinking Affective Experience and Popular Emotion: World War I and the Construction of Group Emotion in International Relations. Political Psychology 40:1357–1372
Halperin E (2015) Emotions in Conflict: Inhibitors and Facilitators of Peace Making. Routledge, New York
Hamid S (2020) American Self-Criticism Borders on Narcissism. https://www.theatlantic.com/ideas/archive/2020/01/the-us-isnt-as-important-as-the-left-thinks/604642/. Accessed 30 May 2020
Holsti O R, George A (1975) The Effects of Stress on the Performance of Foreign Policymakers. In: Cotter C P (ed) Political Science Annual. Bobbs-Merrill, Indianapolis, 255–319
Izard C E (2007) Basic Emotions, Natural Kinds, Emotion Schemas, and a New Paradigm. Perspectives on Psychological Science 2:260–280
Jervis R (1976) Perception and Misperception in International Politics. Princeton University Press, Princeton

Jervis R (2017) Perception and Misperception in International Politics. Princeton University Press, Princeton
Jervis R (2020) On the Current Confrontation with Iran https://warontherocks.com/2020/01/on-the-current-confrontation-with-iran/?fbclid=IwAR0-feIZoiInsBYwKzMWfAYpKnMPSV0w3i6xheYzSupd0FDsZTFP6mtH5Ro. Accessed 30 May 2020
Jervis R, Lebow R N, Stein J G (1985) Psychology and Deterrence. The John Hopkins University Press, Baltimore
Johnson K (2019) Iran Protests Suggest Trump Sanctions Are Inflicting Serious Pain https://foreignpolicy.com/2019/11/20/iran-protests-trump-sanctions-inflicting-serious-pain/. Accessed 30 May 2020
Kahn H (1961) On Thermonuclear War. Princeton University Press, Princeton
Kahneman D, Slovic P, Amos T (1982) Judgment under Uncertainty: Heuristics and Biases. Cambridge University Press, Cambridge
Keltner D (2019) Toward a Consensual Taxonomy of Emotions. Cognition and Emotion 33:14–19
Keltner D, Lerner J (2001) Fear, Anger and Risk. Journal of Personal and Social Psychology 81.1:146–159
Keltner D, Oatley K, Jenkins J M (2014) Understanding Emotions. Wiley, Hoboken
Knights M (2020) Why Iran May Not Be Satisfied with a "Slap" at Trump. https://foreignpolicy.com/2020/01/07/qassem-suleimani-iran-killing-next-move/. Accessed 30 May 2020
Lazarus R (1993) From Psychological Stress to the Emotions: A History of Changing Outlooks. Annual Review of Psychology 44:1–21
Lazarus R (2001) Relational Meaning and Discrete Emotions. In: Scherer K R, Schorr A, Johnstone T (eds) Appraisal Process in Emotion: Theory, Methods, Research. Oxford University Press, Oxford, 37–67
Lebow R N (2008) A Cultural Theory of International Relations. Cambridge University Press, New York
Lebow R N, Stein JG (1989) Rational Deterrence Theory: I Think, Therefore I Deter. World Politics 41:208–224
Lerner J, Keltner D (2000) Beyond Valence: Toward a Model of Emotion-Specific Influences on Judgement and Choice. Cognition and Emotion 14:473–493
Lerner J, Tiedens L (2006) Portrait of The Angry Decision Maker: How Appraisal Tendencies Shape Anger's Influence on Cognition. Journal of Behavioural Decision Making 19:115–37
Lerner J, Li Y, Valdesolo P, Kassam K S (2015) Emotion and Decision Making. Annual Review of Psychology 66:799–823
Löwenheim O, Heimann G (2008) Revenge in International Politics. Security Studies 17:685–724
Lupovici A (2018) The Power of Deterrence: Emotions, Identity, and America and Israeli Wars of Resolve. Cambridge University Press, Cambridge
Markwica R (2018) Emotional Choices: How the Logic of Affect Shapes Coercive Diplomacy. Oxford University Press, Oxford
McDermott R, Lopez A C, Hatemi P K (2017) "Blunt Not the Heart, Enrage It": The Psychology of Revenge and Deterrence. Psychology of War 1:68–88
Mercer J (2005) Rationality and Psychology in International Politics. International Organization 59:77–106
Mercer J (2010) Emotional Beliefs. International Organization 64:1–31
Mishra P (2020) Hardliners in the U.S. and Iran Are Each Other's Best Friends https://www.bloomberg.com/opinion/articles/2020-01-07/hardliners-in-the-u-s-and-iran-are-each-other-s-best-friend. Accessed 30 May 2020
Moors A (2009) Theories of Emotion Causation: A Review. Cognition and Emotion 23:625–62
Moors A (2013) On the Causal Role of Appraisal in Emotion. Emotion Review 5:132–40
Morgan P M (1983) Deterrence: A Conceptual Analysis. SAGE Publications, Beverly Hills
Naji K (2020) Soleimani: Why Huge Crowds Turned Out for Iran Commander's Funeral https://www.bbc.com/news/world-middle-east-51021854. Accessed 30 May 2020

Payne K B (2001) The Fallacies of Cold War Deterrence and a New Direction. The University Press of Kentucky, Lexington
Payne K B (2011) Understanding Deterrence. Comparative Strategy 30:393–427
Payne K (2015) The Psychology of Strategy: Exploring Rationality in the Vietnam War. Hurst and Company, London
Payne K (2018) Strategy, Evolution, and War. Georgetown University Press, Washington
Phelps E A, Lempert K M, Sokol-Hesner P (2014) Emotion and Decision Making: Multiple Modulatory Neural Circuits. Annual Review of Neuroscience 37:263–288
Pompeo M (2020) The Restoration of Deterrence; the Iranian Example https://id.usembassy.gov/the-restoration-of-deterrence-the-iranian-example/. Accessed 30 May 2020
Reimer J (2020) Iran Claws Back Its Regional Influence. RAND Corporation, Santa Monica
Renshon J, Lerner J (2012) Decision-Making, the Role of Emotions in Foreign Policy. In: Christie D J (ed) The Encyclopedia of Peace Psychology. Blackwell Publishing, Oxford, pp 1–6
Riley-Smith B (2020) US Says Attack Planned by Qassim Soleimani Was "days" from Happening. https://www.telegraph.co.uk/news/2020/01/07/us-says-attack-planned-qassim-soleimani-days-happening/. Accessed 30 May 2020
Risen J (2020) Donald Trump Murdered Qassim Suleimani. https://theintercept.com/2020/01/09/donald-trump-iran-suleimani-murder/. Accessed 30 May 2020
Roseman I, Smith C (2001) Appraisal Theory. In: Scherer K R, Schorr A, Johnstone T (eds) Appraisal Process in Emotion: Theory, Methods, Research. Oxford University Press, Oxford, pp 1–20
Rove K (2020) The Politics of Killing Soleimani. https://www.wsj.com/articles/the-politics-of-killing-soleimani-11578528322. Accessed 30 May 2020
Roy J M (2016) From Intersubjectivity to International Relations: The Relevance of the "Emotive Turn" of Cognitive Science. In: Ariffin Y, Coicaud J M, Popovski V (eds) Emotions in International Politics. Cambridge University Press, New York, pp 80–111
Sauer F (2015) Atomic Anxiety: Deterrence, Taboo and the Non-Use of US Nuclear Weapons. Palgrave Macmilllan, New York
Schelling T C (1966) Arms and Influence. Yale University Press, New Haven
Schelling T C (2008) Arms and Influence. Yale University Press, New Haven
Scherer K J (2013) Measuring the Meaning of Emotion Words: A Domain-Specific Componential Approach. In: Fontaine J J R, Scherer K J, Soriano C (eds) Components of Emotional Meaning: A Sourcebook. Oxford University Press, Oxford, pp 7–30
Seligman L (2020) Petraeus Says Trump May Have Helped "Reestablish Deterrence" by Killing Suleimani. https://foreignpolicy.com/2020/01/03/petraeus-on-qassem-suleimani-killing-says-trump-helped-reestablish-deterrence/. Accessed 30 May 2020
Seligman L, Gramer R (2020) Nervous U.S. Allies Brace for Iran Fallout. https://foreignpolicy.com/2020/01/14/nervous-allies-trump-iran-fallout-middle-east-tensions-suleimani-killing-conflict/. Accessed 30 May 2020
Smith C, Ellsworth P (1985) Patterns of Cognitive Appraisal in Emotion. Journal of Personality and Social Psychology 48:813–838
Steimer T (2002) The Biology of Fear- and Anxiety- Related Behaviours. Dialogues in Clinical Neuroscience 4:231–249
Stein J G (2012) Deterring Terrorism, Not Terrorists. In: Wenger A, Wilner A (eds) Deterring Terrorism : Theory and Practice. Stanford University Press, Stanford, pp 46–66
Stein J G (2013) Threat Perception in International Relations. In: Huddy L, Sears D O, Levy J S (eds) The Oxford Handbook of Political Psychology. Oxford University Press, Oxford, pp 364–394
Stein J G, Lotan M (2019) Disabling Deterrence and Preventing War: Decision Making at the End of the Nuclear Chain. In: Harrington A I, Knopf J W (eds) Behavioural Economics and Nuclear Weapons. University of Georgia Press, Athens, pp 56–77

Strobel W P, Youssef N A, Salama V (2019) Intelligence Suggests U.S., Iran Misread Each Other, Stoking Tensions. https://www.wsj.com/articles/trump-told-aides-he-doesnt-want-war-with-iran-11558036762. Accessed 30 May 2020

Thayer B (2007) Thinking about Nuclear Deterrence Theory: Why Evolutionary Psychology Undermines Its Rational Actor Assumptions. Comparative Strategy 26:311–323

Turowski T K, Man V Y, Cunningham W A (2014) Positive Emotion and the Brain: The Neuroscience of Happiness. In: Gruber J, Moskowitz JT (eds) Positive Emotion: Integrating the Light Sides and Dark Sides. Oxford University Press, Oxford, pp 95–115

Van Kleef G A, Fischer A H (2016) Emotional Collectives: How Groups Shape Emotions and Emotions Shape Groups. Cognition and Emotion 30:3–19

Ward A (2020) The US Killed Soleimani. What Will Iran Do Next? https://www.vox.com/2020/1/10/21058430/iran-crisis-war-soleimani-response-trump-war. Accessed 30 May 2020

Wintour P (2020) European Leaders Call for De-Escalation of Crisis after Suleimani Killing. https://www.theguardian.com/world/2020/jan/03/qassem-suleimani-killing-may-spell-end-iran-nuclear-deal-europe-fears. Accessed 30 May 2020

Zadra J R, Clore G L (2011) Emotion and Perception: The Role of Affective Information. Wiley Interdisciplinary Review of Cognitive Sciences 2:676–685

Samuel Zilincik is a doctoral student of Security and Strategic studies at Masaryk University and a teaching assistant at the University of Defence in the Czech Republic. He also has conducted internships at the Hague Centre for Strategic Studies in the Netherlands), at the Centre for Security and Prevention in the Czech Republic, and at the Strategic Policy Institute in Slovakia.

Isabelle Duyvesteyn is a Professor of International Studies and Global History at the Institute of History at Leiden University in the Netherlands. Prior to joining the History Institute, she held a special chair in Strategic Studies at the Institute of Political Science at Leiden. She has been a member of the National Advisory Council for International Affairs and is a member of the Scientific Advisory Board of the Netherlands Defence Academy.

Chapter 25
The Missing Component in Deterrence Theory: The Legal Framework

Paul Ducheine and Peter Pijpers

Contents

Abstract This chapter takes the starting point that the power to deter consists of three components: (physical) capacities, concepts (strategy, plans, decision-making procedures) and will (moral, determination, audacity). In case one of these com-

P. Ducheine (✉) · P. Pijpers
Netherlands Defence Academy (NLDA), Breda, The Netherlands
e-mail: p.a.l.ducheine@uva.nl

P. Pijpers
e-mail: b.m.j.pijpers@uva.nl

P. Ducheine
University of Amsterdam, Amsterdam, The Netherlands

F. Osinga and T. Sweijs (eds.), *NL ARMS Netherlands Annual Review of Military Studies 2020*, NL ARMS, https://doi.org/10.1007/978-94-6265-419-8_25

ponents is underdeveloped or not in place, (coercive) power fails. Modern technologies (e.g. ICT, AI) and strategic insights (e.g. the utility of soft and smart power) urge for a reinterpretation of the 'physical' component, and include cyber capacities as well as culture, knowledge or law(fare) as capacities (or power instruments), too. Moreover, and taking cyber capabilities as a test case, these developments put even more weight on the conceptual and moral components of power. This chapter focusses on the legal framework as a key, but underrated, conceptual element of deterrent power. Using cyber threats as a case, it offers a legal framework enabling decision-makers to effectively generate deterrent power by showing which legal bases (should) undergird the employment of the variety of responses available to States. In democratic rule-of-law States, the principles of legitimacy and legality demand that the use of power (instruments) by States must be based on a legal basis and should respect other institutional features too. Through two illustrative vignettes the generic value of the framework will be illustrated for the potential use of power instruments—diplomacy, information, military, economy, culture, legal, knowledge—in its various modalities, including cyber operations. This legal framework, though tailored to cyber capabilities, may be used as a starting point for conceptualising the legal framework for so-called cross domain and cross dimensional, or full spectrum deterrence.

Keywords Legal framework · legal bases · deterrence · cyber operations · attribution · cyberspace

25.1 Introduction

"*The supreme art of war is to subdue the enemy without fighting.*"

Sun Zsu, 6th century BC

25.1.1 East Meets West

Western States traditionally focus on the physical military instrument when conceptualising deterrence as a strategic function. The threat of military force, or its actual use, is a preferred *modus operandi* in Western strategic culture.[1] For Asian States such as China, force may be perceived differently in terms of instruments used, as well as in its modalities, and in concepts. Force and power may have an economic or diplomatic face, whilst the actual threat or use of military force is less

[1]See Kitzen 2012a, b; Ducheine and Osinga 2017.

prominent or takes virtual or symbolic shapes. Looking at China's Belt and Road Initiative, trade relations, loans, (lease) contracts, embassies, harbours, education, culture and indeed the positioning of armed forces, play important roles. Quite early, Chinese strategic thinkers like Sun Zsu, and more recently Qiao Liang and Wang Xiangsui, have stressed the importance of the information environment in strategic issues such as deterrence.[2] Although rather late, Western strategic interest —accelerated by ever growing opportunities and threats in cyberspace – in this sphere is growing fast.[3]

25.1.2 Cyberspace as a Strategic Opportunity?

Cyberspace has been described in many ways,[4] ranging from 'a consensual hallucination'[5] to a 'networked information infrastructure'.[6] In short, cyberspace covers 'all entities that are or may potentially be connected digitally'.[7] Cyberspace is central to the information environment, the sphere where information is presented, found, communicated, processed, handled and used upon which decision-making is based, followed by (in)action. The information environment entails a physical, a cognitive and a virtual dimension. To enable digital connections, cyberspace, as part of the information environment consists of three elements: (1) cyber identities, (2) cyber objects (i.e. software, data and protocols), and (3) the physical network layer entailing cyber infrastructure (i.e. hardware and (electromagnetic) connections).

Cyberspace may be used in a number of ways. First of all, it offers a medium for information and communication. Secondly, it entails capacities that may be used as instruments of power: data, applications, procedures. Thirdly, these instruments may be directed at, or can engage with other actors in cyberspace. In military terms, one may find both weapons and targets, as well as a vector to connect weapons with

[2]Qiao Liang and Wang Xiangsui 1999, p. 199.

[3]Smeets and Soesanto 2020.

[4]Most elaborate by Kuehl 2009, p. 28, who describes cyberspace as a 'global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies'.

[5]Gibson 2018, p. 51.

[6]Koh 2012, p. 6.

[7]See Netherlands Defence Cyber Strategy 2012 (UK version) "Cyberspace is understood to cover all entities that are or may potentially be connected digitally. The domain includes permanent connections as well as temporary or local connections, and in all cases relates in some way to the data (source code, information, etc.) present in this domain", (original Dutch) in: *Parliamentary Papers II 2011–2012*, 33 321, no. 1.

the targets. In generic terms: cyber capacities may be used as instruments to engage with other cyber capacities in or through cyberspace.[8]

Not surprisingly, cyberspace has become the 5th domain of operations.[9] In effect, the potency of cyberspace is related to the threat or use of (military) force, but also to the deliberate undermining of the understanding and autonomous decision-making of actors, hence the informational instrument of power.[10]

25.1.3 Conceptual Considerations for Deterrence in Cyberspace

Is deterrence possible in cyberspace? Cyberspace is not an instrument of power in itself, but an engagement 'arena' similar to the land or air domain. However, unlike land, sea and air, people are absent in cyberspace[11] and 'only' the virtual reflections of humans—cyber identities—engage in cyberspace. The dominant academic thinking tends to conclude that cyberspace is not fit for deterrence as a strategic function for States,[12] a view that appears at odds with the actual effects of on-line activities of numerous (State sponsored) Advanced Persistent Threats (APTs),[13] or the considerations of US Cyber Command.[14]

But maybe the question is not whether cyberspace is fit for deterrence, but whether the constituent components of deterrent capabilities are fit for contemporary engagements. Power projection in cyberspace, whether for deterrence purposes or otherwise, is no longer merely focusing on military power, but on all instruments of power, including diplomacy, informational, cultural, financial or legal instruments.

---

[8]Whilst this generic view describes so-called hard cyber activities or operations, the present authors also recognize so-called soft cyber operations, where cyberspace is merely used a vector to communicate virtual or digitalised information (content) via cyber identities to real persons, in an effort to affect their psyche and consequently their autonomous decision-making process, individual or collective preferences and values.

[9]See NATO Warsaw summit NATO 2016, Bulletin no. 70.

[10]Ducheine and Pijpers 2020.

[11]Delerue 2019.

[12]Borghard and Lonergan 2017; Fischerkeller and Harknett 2017, p. 393; Taddeo 2018, pp. 352–353; Whyte 2016, pp. 100–101.

[13]For an overview of these APTs, see the list produced by Mitre-Attack, at https://attack.mitre.org/groups/; Booz Allen 2020.

[14]US Cyber Command 2018.

Applying the instruments of power, including military power, (in deterrence contexts) requires the (demonstrated) capacity to perform, the will to act,[15] but moreover a manner how to channel these capacities.[16] These commonplace elements—capacities, concepts and will—are also encapsulated in military doctrine.[17] Creating power presumes the existence and effectiveness of these three components. In case one of these components is underdeveloped or not in place, power fails.

For democratic States, the conceptual component includes an applicable legal framework which enables the use of these power instruments. Their common values[18] dictate to respect and promote international law in their international relations,[19] and respect for law in general when interacting with non-state actors.

This legal framework however, is an area that seems undervalued and less researched, at least in war studies and security studies, despite the fact that the legal framework is a crucial element of the conceptual component for (deterrence) operations in cyberspace or any physical domain. For the purpose of this treatise, the legal framework is considered an integral part of the holistic approach towards deterrence in operations as it should be when conducting research in these areas. Therefore, States will need to organise and structure their legal and institutional framework in order to deter others from engaging, threatening or attacking vital interests, in or through cyberspace.

25.1.4 Aims and Structure

The primary aim is to supplement the conceptual component of power by adding a concise legal framework for the use of all power instruments, be they military or otherwise, classic or modern. The approach taken departs from the premise that when the legal framework is not in place or underdeveloped, the conceptual component of power is flawed which in turn will have deteriorating impact on power itself. E.g., when offensive cyber capabilities are in place, but actual legal bases have not been analysed, realistic decision-making procedures are lacking, or competent bodies authorising the use of capabilities in response of threats have not been designated, deterrence by punishment is illusive. For deterrence to be

[15]Jakobsen 1998, ch 1; Jakobsen 2007, pp. 225–247.

[16]Biddle 2006, pp. 190–191.

[17]Fighting power comprises of (1) capacities, most often the so-called physical component (i.a. manpower, means), (2) a conceptual component (strategy, doctrine, planning), and (3) a moral component (will, resilience, determination). See: NATO 2017, p. 1–16; UK Ministry of Defence 2017, p. 3–2; NL Defence Staff 2019, pp. 66 ff; applied in Ducheine and Van Haaster 2014, p. 305.

[18]See e.g. the Preamble to the Treaty of the European Union (6 October 2012); and the Preamble to the NATO Treaty (4 April 1949).

[19]See e.g. the Preamble to the Charter of the United Nations (26 June 1945); and the Netherlands' position as expressed in *Parliamentary Papers II*, 2006–2007, 29 521 no. 41.

effective, credibility and clear communication demonstrating the will and ability to use capabilities is essential. Hence, without a legal framework in place, a deterrence strategy, with whatever means, will not be effective.

While such a framework is essential for the employment of all instruments of power, and certainly in a context of cross domain deterrence (see Chap. 8 by Sweijs and Zilinck), this chapter focuses on the nexus of deterrence and cyberattacks. Taking deterrence against cyber threats as a case, a succinct matrix of options will be presented serving as a conceptual component to generate capabilities to dissuade opponents, offering insight in the available legal bases for each of the power instruments, recognizing the different faces or modalities that may be envisioned. Although at first glance, this approach may appear to focus on deterrence by punishment, it will become evident that deterrence by norms and/or entanglement may also be of relevance.[20]

In addition, to the legal basis, other institutional elements, such as governance issues, will be addressed, involving questions such as 'who has the authority to decide to make use of the instrument', who is responsible for the execution, who is accountable (for what part), how is oversight guaranteed, will be (briefly) addressed. As Jakobsen argued, effective coercion requires the demonstrated ability to quickly generate coercive power. Having thought through the appropriate governance framework is instrumental to that. To this end, the situation in the Netherlands' national legal framework will be used as a demonstration using so-called vignettes.[21]

Combining the international legal bases with the applicable national institutional or governance framework for the use of power instruments, also serves as a demonstration explaining the legal framework outside threats in cyberspace. In fact, it is argued, that the core of this legal framework may be used to prepare for deterrence in cross domain or full dimension situations. Hence, deterrence against opponents using military, economic or other threats, may benefit from this contribution supplementing or reinforcing the conceptual component of deterring power.

This chapter first briefly sets out the instruments of power (Sect. 25.2). Secondly, the components of power and the legal framework as a conceptual element therein are covered (Sect. 25.3). Next, the legal framework itself is analysed in two parts: the legal bases (Sect. 25.4) building on international law and other relevant elements (Sect. 25.5) building on the Netherlands' institutional arrangements, after which a matrix is presented offering legal options related to the instruments of power (Sect. 25.6).

[20]Nye 2016, pp. 58–62.

[21]As States will have different institutional and constitutional arrangements, this part of the legal framework using the Netherlands as a case in fact, serves as a demonstration.

25.2 Power Instruments

Power instruments are often briefly summarized as DIME: diplomacy, information, military and economy.[22] In deterrence literature the military and diplomatic instruments have been dominant in the past. However, contemporary strategic theorists increasingly make use of concepts such as hybrid threats, unrestricted warfare, grey zone activities, information warfare, financial or economic warfare, cultural, ideological, political, virtual and cyber warfare. Other instruments, such as financial, intelligence, legal,[23] or culture and knowledge, might be added,[24] to fully grasp the instruments used to exert power in today's geopolitical arena.

Diplomacy is linked to foreign relations, it is generally about communicating and advocating national or international interests and values. Diplomacy gets a face through the work of diplomats, international governmental organisations but also through international agreements, resolutions, cooperation, coordination, norm development, alliances, treaties, customary law and soft law.[25]

The military instrument, armed forces, may be used in various ways, from (treaty based or ad hoc) peaceful cooperation based on shared values and norms, to armed conflict. The modalities used, the means and methods, may range from classic physical weaponry, to non-kinetic[26] (e.g. training and advisory capacity)[27] and new information related capabilities, including hard and soft cyber operations.[28]

Economic power, as an instrument may also take various shapes, ranging from consensual (loans) to compulsory (sanctions),[29] and can be enlarged with the financial instrument of power. It covers both passive elements, e.g. a State's macro-economic characteristics as well as active measures (assets freeze, investments, etc.). On the institutional side, international economic relations, such as common markets, with its mechanisms and procedures in place, would be another facet.

---

[22]Mann 2013, p. 502; Schroeder 2015, p. 2; UK Ministry of Defence 2011, pp. 1–6; US Joint Chiefs of Staff 2013, p. 1–12.

[23]Van Haaster 2019, p. 64; Rodriguez et al. 2020.

[24]Nye 2013, pp. 7–10.

[25]See e.g. the Group of Governmental Experts on advancing responsible State behaviour in cyberspace in the context of international security (UNGGE) at https://www.un.org/disarmament/group-of-governmental-experts; and the Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security (OEWG), at https://www.un.org/disarmament/open-ended-working-group.

[26]Ducheine 2015a.

[27]Wiltenburg 2019.

[28]Ducheine et al. 2017.

[29]Giumelli 2017.

Next to classic DIME instruments, others come to the fore: culture as a (soft) power element is often seen in action,[30] expressions of which are Radio Free Europe, China's Confucius institutes,[31] Soros' Open Society Foundation.[32] Lawfare, law used strategically as an alternative for the military instrument[33] in conflict situations,[34] is used in legal action: e.g. the US' indictments of foreign cyber operators,[35] or litigation between States.[36]

Last but certainly not least, information as a power instrument—including intelligence—can be understood in several ways. First of all, it involves the relative value of information sources itself, whether physical, cognitive or virtual.[37] These sources may be observed by men and/or machine, upon which understanding and decision-making are based.[38] Large data sets containing personal information related to (large) groups, or traffic data, are also examples of power resources. This substantive facet may be used to affect other actors, e.g. through marketing.[39] Secondly, it entails structures to communicate, both in terms of procedures and as a medium or vector. This could be the World Wide Web as part of cyberspace, or the internet and the dark web. (Entry) control over these structures, may be used to exert power. One may think of communication channels (old media), Great Firewalls, but also Internet Exchanges, 5G networks, the glass fibre cable network covering the globe, satellites offering mobile internet to places without physical (cable) connectivity. Thirdly, institutions overseeing, designing, contributing to the flow of information may offer a powerbase as well, e.g. the Internet Corporation for Assigned Names and Numbers (ICANN), or the Internet Engineering Task Force. Fourthly, information has a productive aspect as well: to generate debate, to reproduce and reinforce discourse or messaging, to construct and disseminate new information, whether malevolent or benevolent. Consider the (alleged) role of

[30]Nye 2013, pp. 10–14.

[31]Young 2009; Łoś 2019.

[32]See https://www.opensocietyfoundations.org/who-we-are.

[33]Sari 2020.

[34]Voetelink 2017.

[35]See i.a. US DOJ 2018b (GRU Indictment) and 2018a (IRA Indictment); New York Times 2018, 2019; Bellinger 2020.

[36]ICJ, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Judgment (Merits), [1986] ICJ Rep 14, 27 June 1986; ICJ, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, [1996] ICJ Rep 226, 8 July 1996.

[37]See UK Ministry of Defence 2010, p. 2–5; and *supra* n 28.

[38]See *supra* n 28.

[39]In the terminology used by Bets and Stevens 2011: compulsory power. See the four categories by Barnett and Duvall 2005, p. 43: compulsory, structural, institutional and productive power.

Facebook, Twitter and WikiLeaks in elections, or ordinary marketing.[40] As demonstrated, cyberspace is used to gather, transfer, handle and produce information, whilst virtual information (i.e. data, software, protocols) is also used as an instrument, as a vector and as a target to generate effects.

25.3 The Underrated Conceptual Component: Legal Framework

> *The commonplace understanding of power is as a capacity or attribute with which an actor is endowed, or as a resource to be exploited to achieve particular end.*
>
> David Betz & Tom Stevens

Power, described by Betz and Stevens,[41] may be applied to promote and to protect the vital interests of States.[42] As described in Sect. 25.1.3 and mindful of earlier academic and doctrinal work,[43] power requires (1) capacities, most often the so-called physical components (i.e. manpower, means), (2) a conceptual component (strategy, doctrine, planning), and (3) a moral component (will, resilience, determination) to ensure effectiveness, and thus to be regarded a capability.[44] Power requires instruments, and capacities, that may only be effective when 'unlocked' through strategy.[45]

One essential part of the conceptual component, embedded in strategic notions, democratic principles and procedures, is the legal framework accompanying the foreseeable use of power instruments. In democratic rule-of-law States, the principles of legality demand that the use of power (instruments) by States must be

[40]It is signalling that the seven largest publicly traded companies having the greatest market capitalization, are ICT companies (Microsoft, Apple, Amazon, Alphabet, Alibaba, Facebook and Tencent). As on 31 March 2020. Market capitalization is calculated from the share price (as recorded on the selected day) multiplied by the number of outstanding shares. See Van Haaster 2019, p. 78, based on the Financial Times Global 500.

[41]Betz and Stevens 2011, p. 42.

[42]See *supra* n 10, p. 8.

[43]See Jakobsen 2011; NL Defence Staff 2019.

[44]The difference between *capacities* and *capabilities* is essential in this contribution. See by analogy NDD 2019, p. 66: "Fighting power is the ability to conduct military operations in an optimum NDD cohesive totality of functionalities and components. It is more than just the availability of means (capacities); there must also be the willingness and ability to deploy these means (capability). If this is properly developed, it then becomes fighting power, and capacities are elevated to capabilities."

[45]Betz and Stevens 2011, p. 40: "strategy is the art of unlocking the power inherent in national capacities to effect outcomes in the national interest in contest with other strategists acting in their own national interests".

based on such a legal framework. A first element in this legal framework is the legal basis for the legitimate employment of power instruments.[46] In addition, the legal framework, will also entail decision-making procedures describing the (legal and political) authority for the decision to use the designated assets,[47] the applicable legal regimes when these assets are used (i.a. rules of engagement),[48] and accountability and oversight mechanisms.[49]

25.4 Legal Bases

Without a proper legal bases international action, law abiding, and legitimacy seeking States run the risk of producing (or threatening with) non-credible, thus non-deterrent action. Within the limits posed by international law, States are permitted to use power instruments in their international relations. When the use of these instruments falls short of the threshold on the use of force as defined in Article 2(4) of the UN Charter,[50] interstate action is governed by the general principles of territorial sovereignty,[51] and respect for the political independence and territorial integrity, and inviolability of States.[52]

Within this international law framework, various bases for non-forceful and forceful action indeed exist. The legal basis for *non-forceful action* (e.g. economic sanctions, or declaring diplomats *persona non grata*) is an essential part of the conceptual component as it offers three legitimate avenues for interaction with other States (and non-state actors). As States will generally seek to secure the (perceived) legitimacy of their acts, they will offer some form of clarification for non-consensual behaviour. Most often, these clarifications, or in other terms, legal bases, will be based on in the international law phenomena such as retorsion, countermeasures, or a plea of necessity.

Though the use of force itself is forbidden, international law relevant to interstate force, the *jus ad bellum*, offers another three exceptions to this rule that provide a

[46]Ducheine and Pouw 2009, 2012a.

[47]Ducheine et al. 2020.

[48]See e.g. Ducheine and Pouw 2009, 2012b.

[49]Ducheine et al. 2010.

[50]Article 2(4) UN Charter: "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."

[51]On this principle in cyberspace: Ziolkowski 2013; and Pirker 2013. See also Tallinn Manual 2013, Rule 4.

[52]On this principle in cyberspace: Gill 2013.

legal basis for *forceful* (individual or collective) actions:[53] consent,[54] UN Security Council authorization, or self-defence (see below).[55] The legitimacy of these actions strengthens the conceptual component of power as it invigorates the normative justification for the action and moreover, it enhances the will the act. The various legal bases for response action will be described below.

25.4.1 Consent

Paradoxically as it may seem when considering deterrent capabilities, in some cases States might rely on a consensual basis to make use of its power instruments in international relations. This could be both non-forceful and forceful. International law enforcement cooperation might for instance provide for extraterritorial enforcement mechanisms,[56] enabling States e.g. to locate or attribute threats. When this information is made public, it could contribute to the legitimacy of the use of other instruments and modalities. A consensual basis could also be envisioned through treaty-based conflict-resolution or enforcement mechanisms, for which the treaty provides. For example, through international law enforcement cooperation to obtain forensic evidence from a foreign internet service provider's cloud server. Another example could be a Status of Forces Agreement, enabling armed forces operating abroad, to act in designated ways in response of e.g. threats to its forces.[57]

25.4.2 Retorsion

A second basis States might select is retorsion which is defined as unfriendly, but internationally lawful acts, that do not require a prior violation of international law

[53] *Argumentum a maiore ad minus*.

[54] See e.g. the Tallinn Manual 2013, Rule 1, para 8, following the notion of sovereignty, States 'may consent to cyber operations conducted from its territory or to remote cyber operations involving cyber infrastructure that is located on its territory'.

[55] See e.g. Gill and Fleck 2015, Part II.

[56] Ducheine 2015b, p. 469: "Cross-border law enforcement responding to illegal (cyber) activity could be undertaken with respect to the territorial sovereignty of other States with the consent of that State", with reference to Gill 2013, p. 229.

[57] See Boddens Hosang 2015; and Voetelink 2015.

per se.[58] Unfriendly refers to the fact that retorsion is "wrongful not in the legal but only in the political or moral sense, or a simple discourtesy".[59] Retorsion may be used to enforce (international) law, in case the triggering act was indeed a violation of the law. It may also be used to enforce soft law arrangements.[60] Notwithstanding its use in interstate relations, retorsion can also be used by and against qualified international organizations.[61]

State practice presents a great variety of measures of retorsion: each legislative, executive, administrative, etcetera measure that is permissible under international law and that "seems suitable to a State to redress the unwelcome, unfriendly, or illegal behaviour of another State".[62] Common forms can be found within various power instruments: protest; cancelling State visits; denying ships access to ports or to the exclusive economic zone; summoning ambassadors; declaring diplomats persona non grata;[63] "downgrading diplomatic intercourse to the technical level; recalling ambassadors for consultations of indefinite duration; severing diplomatic relations; terminating the payment of development aid or the provision of military assistance; unilaterally imposing legally permissible economic sanctions such as an arms embargo; [..] suspending, terminating, or refusing to prolong a treaty; and withdrawing from an international organization in order to protest this organization's political activities."[64]

Retorsion by using cyber capabilities would be an option in a response to unfriendly (or unlawful) acts by other States,[65] e.g. by "limiting or cutting off the other state's access to servers or other digital infrastructure in its territory",[66] or by

[58]Max Planck Encyclopedia of Public International Law [MPEPIL]. Based on the Articles on State responsibility, chapeau to Chapter II of Part 3, para 3 of the Commentary.

[59]MPEPIL, para 2. As stressed by (inter alia) the Netherlands' Cabinet: "This option is therefore always available to states that wish to respond to undesirable conduct by another state, because it is a lawful exercise of a state's sovereign powers. States are free to take these kinds of measures as long they remain within the bounds of their obligations under international law." See *Parliamentary Papers II* (House of Representatives) 2018–2019, 33–649, no. 47 (annex), p. 7. Via https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace.

[60]Soft law being non-binding international arrangements, see MPEFIL, para 37: "a complex of norms lacking binding force, but producing significant legal effects nevertheless".

[61]To the extent that the latter have international legal personality and the capacity to act in the international sphere, see: MPEPIL, para 1.

[62]MPEPIL, para 10.

[63]As was the case in response to Russia's meddling with the 2016 US Presidential elections, see: US White House 2016; Sanger 2016.

[64]MPEPIL, para 10.

[65]Gill 2013, p. 230 and the accompanying notes; and Gill 1992, p. 105.

[66]*Parliamentary Papers II* (House of Representatives) 2018–2019, 33 649, no. 47 (Annex), p. 7, stressing: "provided the countries in question have not concluded a treaty on mutual access to digital infrastructure in each other's territory".

"misleading a prospective intervening party by providing it with bogus or useless information or otherwise diverting cyber break-ins from their intended targets".[67]

25.4.3 Countermeasures

A third basis for response options consists of threatening or taking countermeasures. This involves actions taken in response to another State's violation of international law.[68] They may be defined as "pacific unilateral reactions which are intrinsically unlawful, which are adopted by one or more States against another State, when the former considers that the latter has committed an internationally wrongful act which could justify such a reaction".[69] Countermeasures are used to induce compliance (and enforcement) of international legal obligations.

Unlike retorsion, countermeasures interfere with the target State's international legal rights, and are therefore subject to preconditions.[70] They require (1) a prior internationally wrongful act that (2) can be attributed to a State; (3) with the sole purpose to induce the wrongdoer's compliance; (4) they are limited to non-forceful and proportionate actions only; and (5) a prior demand to the wrongdoer is required.[71] Finally, (6) countermeasures are not allowed once the unlawful act has ceased.[72]

In terms of responding to prior cyber incidents that violate international law, countermeasures could be used to actively hack back when the location of the infrastructure is known, e.g. the GRU headquarters, to stop the violation,[73] or to initiate action against States that should have acted to stop their infrastructure from being to for the violation, but are not willing to do so.[74]

25.4.4 Plea of Necessity

In addition, States facing 'grave and imminent peril' to its 'essential interests' might, when the strict conditions are met, rely on a plea of necessity in response.

---

[67]Gill 2013, p. 236.

[68]Schmitt 2014a.

[69]Geiss and Lahmann 2013, p. 629.

[70]Schmitt 2013b, p. 678; Tallinn Manual 2013, Rule 9; also *Parliamentary Papers* II, House of Representatives, 2010–2011, 32 500 V, no. 166, p. 2.

[71]See *supra* n 56, p 470.

[72]Geiss and Lahmann 2013, p. 638.

[73]*Parliamentary Papers II* (House of Representatives) 2018–2019, 33-649, no. 47 (annex), p. 7: "a cyber operation could be launched to shut down networks or systems that another state is using for a cyberattack". The 'GRU' is the military intelligence service of the Russian Federation.

[74]See the debate covered in the commentaries to Rule 20-25 in the Tallinn Manual 2.0 2017 and Schmitt 2017.

Unlike countermeasures, action based on this plea does not require a prior internationally wrongful act to which it is responding, and the author responsible for this act to could—next to States—also be a non-state or an unknown entity.[75] Once again, the preconditions are very strict. The threshold is high, as it requires (1) a situation of 'grave and imminent peril' to (2) 'essential interests' of the Victim State.[76] Moreover, action may (3) not involve the use of force,[77] should be (4) proportional, and it (5) requires attribution to the author of the (threatening) act who should be (6) addressed first ordering him/her to desist.

The crucial notion of essential interests of States is "vague in international law".[78] What is essential, is contextual and will depend from State to State. Grave and imminent peril to a State's essential interest, refers to actual harm and to threats: "the damage does not already have to have taken place, but it must be imminent and objectively verifiable".[79] Moreover, damage caused or threatened could be physical or non-physical, e.g. "situations in which virtually the entire internet is rendered inaccessible or where there are severe shocks to the financial markets" could be viewed as cases in which necessity may be invoked.[80] Alongside the strict conditions, the plea also gives leeway, as "establishing the existence of a situation of necessity does not require a State to determine the precise origin of the damage or whether another State can be held responsible for it."[81] Nevertheless, the necessity may only be invoked when "no other real possibility of taking action to address the damage caused or threatened exists, and provided there is no interference with the essential interests" of other States "or of the international community as a whole".[82]

In terms of cyberspace, closing down an intrusive cyber operation (e.g. ransomware) against central medical infrastructure or key financial technology (e.g. iDeal) caused by cyber criminals operating from an unknown jurisdiction so that international law enforcement cooperation is futile, could be a scenario to be used.

25.4.5 Self-Defence

Next to retorsion, countermeasures and a plea of necessity, States may in extreme situations of an armed attack, resort to yet another self-help mechanism:

---

[75]Schmitt 2014b; Geiss and Lahmann 2013. Tallinn Manual 2.0 2017, Rule 26.

[76]Schmitt 2013, p. 663,2014b: "In the cyber context, the plea of necessity is most likely relevant when cyber operations threaten the operation of critical cyber infrastructure."

[77]See *supra* n. 56, p 470.

[78]Tallinn Manual 2.0 2017, p. 135.

[79]*Parliamentary Papers II* (House of Representatives) 2018–2019, 33 649, no. 47 (annex), p. 8.

[80]*Parliamentary Papers II* (House of Representatives) 2018–2019, 33 649, no. 47 (annex), p. 8.

[81]*Parliamentary Papers II* (House of Representatives) 2018–2019, 33 649, no. 47 (annex), p. 8.

[82]*Parliamentary Papers II* (House of Representatives) 2018–2019, 33 649, no. 47 (annex), p. 8.

self-defence.[83] Before the terrorist attacks of 2001, international law accepted that States that are the victim of violent activities that reach the threshold of an armed attack[84] may respond with lawful measures of self-defence against the author(s) of that armed attack, "provided it does so in conformity with the other material (necessity and proportionality)[85] and procedural requirements of exercising self-defence (reporting to the Security Council)."[86]

Whether violent activities or operations qualify as an armed attack 'depends on its scale and effects'. Based on Article 51 UN Charter and customary law, an armed attack has been defined as "a use of force which originates from outside the target State's territory, rising above the level of a small scale isolated armed incident or criminal activity, which is directed against a State's territory, its military vessels or aircraft in international sea or airspace or lawfully present on another State's territory, or in certain situations directed against its nationals located abroad."[87]

Analysing its elements, an armed attack, first of all, involves the use of force, normally understood to be military force. It might be 'produced' through conventional, nuclear or other means and methods of warfare.[88] Second, it requires a significant use of force, usually measured in terms of "scale and effects",[89] as it is generally viewed as a more serious form of the use of force.[90] Third is the transnational or cross-border aspect of an armed attack. Normally, armed attacks are conducted by the armed forces of a State, launching or conducting a military operation against targets in or belonging to another State.

In accordance with the principle of necessity, self-defence is a forceful measure of last resort, that is, when no consent could be reached, and collective enforcement measures under Chapter VII of the UN Chapter are in-effective, not feasible or not

[83]See *supra* n 56, p. 472, Rule 23.05. For more details on self-defence: Gill 2015, esp. pp. 214–216; and Gill and Ducheine 2012, p. 443, 2015. See also Tallinn Manual 2013, Rules 13–17.

[84]See Article 51 UN Charter. See also its customary law basis in Gill 2015, pp. 214 ff (Rule 8.02).

[85]See Tallinn Manual 2013, Rule 14 on necessity and proportionality.

[86]See *supra* n 56, p. 472.

[87]Gill and Ducheine 2012, p. 443. Also: Gill 2015, p. 213, Rule 8.01.

[88]See: ICJ, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, [1996] ICJ Rep 226, 8 July 1996.

[89]CJ, *Case Concerning Military and Paramilitary Activities In and Against Nicaragua* (Nicaragua vs. United States), Merits, 27 June 1986, paragraph 195. Also: Gill 2015, p. 216, Rule 8.03: "a reasonably significant use of force".

[90]See Article 2(4) UN Charter.

opportune. Moreover, the self-defence response should be proportional.[91] In the context of this field of the *jus ad bellum*, proportionality has a distinct meaning.[92] Contrary to common misunderstanding, proportionality in self-defence does *not* require a response in kind. In other words, self-defence is a proper legal basis for cross-domain deterrence, as e.g. a classic armed attack could trigger a self-defence response with cyber capabilities, and vice versa, a digital armed attack could be followed by a conventional military response.

25.4.6 Self-Defence Post-2001

The classic interpretation of an armed attack however, has evolved as a result of the 9/11 terrorist attacks against the United States, and the 2015 terrorist attacks in France, including the subsequent responses that were based on self-defence. Next to States, non-states actors potentially qualify as the author of an armed attack too.[93] Moreover, an armed attack could be 'produced' or generated by non-military means and alternative methods, such as hijacked airliners. In addition, an armed attack could also comprise a series of smaller attacks, launched by a single author against the same target State, when these attacks are reasonably related in geographic and temporal terms.[94] These new insights, combined with current practises in cyber-space,[95] have forced States to review their security strategies and stances in international relations, including international law.

Witnessing the interdependence of societies, economies, households and humans created through and with cyberspace, it is notable that States as well as non-state actors have proven to possess capabilities which can threaten or affect vital

[91]Gill 2015, p. 221, Rule 8.04.

[92]Gill and Ducheine 2012, p. 450 "Proportionality in the context of self-defense refers to the requirement that measures of self-defense must not exceed those required under the circumstances to repel the attack and prevent further attacks from the same source in the proximate future and that they must be roughly commensurate to the scale and aims of the overall attack. Hence, the scale and nature of the attack will determine what is required to repel or, if necessary, over-come it and prevent a continuation". On the various meanings of proportionality, see Van den Boogaard 2019.

[93]See *supra* n 46.

[94]Boddens Hosang and Ducheine 2020, pp 14–15: "This would require that the series of attacks can, firstly, be attributed at all, and, secondly, be attributed to a common author. Hence, it involves (i) the capability of detecting an attack, (ii) the capability of technical or 'forensic' attribution of the attacks, and (iii) the capability of legal attribution of the attacks to a common author (operating from abroad). Thirdly, the series of attacks should be directed against targets in or belonging to a single State. Fourthly, the series of attacks are—somehow—related in terms of time and location. And fifthly, the series of attacks, or the attack as whole, constitutes force of sufficient gravity in terms of scale and effects as to qualify as an armed attack". Also: Gill and Ducheine 2012. See i.a. UN Doc. S/2001/947 (Letter dated 7 October 2001 from the Chargé d' affaires a.i. of the Permanent Mission of the United Kingdom of Great Britain and Northern Ireland to the United Nations Addressed to the President of the Security Council), p. 1.

[95]See *supra* n 10.

interests.[96] As noted by Boddens Hosang and Ducheine, "launching cyber operations that potentially equal the effects of an armed attack, as was the case on 9/11, either by State or non-state actors, is not just a theoretical chance or risk."[97] In recognition of this, the Netherlands[98] and France, take the view that cyber-attacks could qualify as armed attack,[99] including the option of purely non-physical consequences of the attack. France notes that a "cyberattack could be categorised as an armed attack if it caused substantial loss of life or considerable physical or economic damage. That would be the case of an operation in cyberspace that caused a failure of critical infrastructure with significant consequences or consequences liable to paralyse whole swathes of the country's activity, trigger technological or ecological disasters and claim numerous victims."[100] The Netherlands' government, based on its advisory councils, recognizes that "disruption of the state and/or society, or a sustained attempt thereto, and not merely an impediment to or delay in the normal performance of tasks"[101] could indeed qualify as an armed attack. Notably, a cyber operation targeting "the entire financial system or prevents the government from carrying out essential tasks" could well be equated with an armed attack.[102]

25.5 Other Parameters: Institutional Arrangement and Attribution

In addition to the legal basis as part of the legal framework that contributes to the conceptual component of power (instruments), two other legal elements are relevant in order to generate effective capabilities with the designated capacities: the institutional set-up and the ability to attribute. Once again, in case these elements are not in place, producing (or threatening with) action with power instruments would be non-credible and ineffective, as opponents would be (or could be) aware of the missing link to transform capacities into effective capabilities.

Related to the legal basis and to the tasking of responsible State organs, and impacting on the decision-making procedure thereto, is the paradigm governing the potential or real response. So, rules concerning the roles, mandates and responsibilities of services and State organs i.a. the Ministry of Foreign Affairs, Ministry of

[96]See *supra* n 94, p. 13, referring to WRR 2019; Algemene Rekenkamer 2019; Dutch Safety Board 2020.

[97]See *supra* n 94, p. 13.

[98]*Parliamentary Papers II* (House of Representatives) 2018–2019, 33 649, no. 47, p. 8 (see *supra* n 59). For the Advisory Report it follows: AIV/CAVV 2011.

[99]In general terms, this is also the explicit view of NATO, the United Kingdom, Estonia and Australia.

[100]France 2019, p. 8.

[101]See AIV/CAVV 2011, p. 21.

[102]See AIV/CAVV 2011, p. 21.

Trade and Development Aid, Economic Affairs, Police, Public Prosecutors, armed forces etc., ought to be in place. It also entails decision-making procedures describing the (legal and political) authority to order the use of the designated assets.[103] Moreover, it involves the legal regimes applicable when these assets are to be used, i.a. rules of engagement, should be clear.[104] Likewise, accountability and oversight mechanisms will have to be in place.[105]

Next, a four-tiered attribution framework, is required.[106] First, threats or harmful cyber incidents need to be detected. Without adequate detection, States are unaware of threats or actual damaging situations in cyberspace, and therefore unable to respond or deter at all. Detection capacities also require conceptual (i.a. legal) backing, before capabilities emanate. Hence, it should be clear who is tasked with what kind of detection or surveillance responsibilities, as well as how detection is handled and communicated to what authorities. For that reason, surveillance and/or investigative powers should be available to the relevant services. Second, technical attribution is needed: a technical forensic inquiry is required to assess e.g. what malware was used, how it operates, from which IP-address or cyber identity it came from, what path it followed and who authored it and has sent it. Obviously, this will require investigative powers. Third, through legal attribution the actors who bear responsibility for the incident may be designated. This relates to the burden of proof and affiliating the perpetrator e.g. an APT to a State or subject to State control. The so-called Articles on States Responsibility are the key legal concept in this realm. The final part is political attribution in which a State may choose to use political communication to address the responsible State (and author)[107] and if necessary, seek (legal) retribution.[108] But this 'naming and shaming' will not always follow suit;[109] it will often be conducted discreetly and not in public especially if the relation with the perpetrator is sensitive or if it is a friend rather than a foe. It should be noted however, that political attribution is not required to stem from digital forensics and/or legal attribution. Often the political attribution is a solitary and unilateral act.[110]

The concepts (and rules) for these three forms of attribution should be available, clear and ready to be used, exercised if possible. In case essential parts of this framework are lacking, outdated, not well known or badly rehearsed, the conceptual

[103]See *supra* n 47.

[104]See *supra* n 48.

[105]See *supra* n 49.

[106]Rid and Buchanan 2015; Bijleveld 2018.

[107]See e.g. The Netherlands considers Russia's GRU responsible for cyber-attacks against Georgia, at https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/diplomatic-statements/2020/02/20/the-netherlands-considers-russia%E2%80%99s-gru-responsible-for-cyber-attacks-against-georgia.

[108]See e.g. the indictments against the Internet Research Agency by the US Department of Justice: US DOJ 2018a.

[109]Finnemore and Hollis 2019.

[110]US White House 2016; UK Foreign and Commonwealth Office 2020.

component is suboptimal, and credibility, hence also effectiveness, of the deterrent instrument could be at stake. For example, with its Defence Cyber Command, cyber capacities in the Netherlands are available. Moreover, the ambition to use these capacities in a deterrent posture had been expressed publicly. However, when the meaning of what an armed attack entails, is unclear, or when political[111] or operational[112] decision-making procedures to actually use these capacities in self-defence would be missing, no credible, hence no effective capability is around. As that would be the same when the political will to actually use the capacities of the Defence's Cyber Command, is lacking.

25.6 Instruments—Legal Bases Matrix

While the analysis of the legal framework above was presented in the context of cyber capabilities and threats, this framework is generic and essential to all democratic rule-of-law States. The matrix in Table 25.1 is composed of the various power instruments as previously described. It conveys how states can resort to specific legal bases when considering employing instruments of power. The numbered boxes offer realistic combinations of instruments/modalities and legal basis. The numbering refers to a vignette below. While space restriction precludes covering each of the available options,[113] a few fictitious examples for the

Table 25.1 Legal bases matrix

Legal basis instrument	Consent	Retorsion	Countermeasures	Plea of necessity	Self-defence
Diplomacy	1	2			
Information and knowledge (incl. Intelligence)	3	4	5	6	7
Military	8	9*	10*	11*	12
Economy and financial	13	14	15	16	
Culture	17	18			
Legal	19	20	21	22	

The * stand for: non-violent/non-forceful action only
(*Source* Ducheine and Pijpers)

[111] See *supra* n 47.

[112] See e.g. Smeets and Work 2020.

[113] Fictitiously ranging from 1 to 22 in the matrix (Table 25.1).

Table 25.2 Vignette for option 2—Halt diplomatic consultations (Retorsion)

Instrument	Diplomacy
Action	Halt consultations
Paradigm	Diplomacy
Authority	Cabinet/MFA
Legal Basis	Retorsion
Action by	MFA
Oversight	Parliament

(*Source* Ducheine and Pijpers)

Table 25.3 Vignette for option 5—Counter-Intelligence operation (countermeasures)

Instrument	Informational (intelligence)
Action	Take control of C2-server
Paradigm	Countermeasures
Authority	Minister home affairs
Legal basis	Countermeasures
Action by	Intelligence service (AIVD)
Oversight	Parliament (CIVD) and CTIVD

(*Source* Ducheine and Pijpers)

Netherlands' institutional and constitutional setting, including the EU framework, will serve to demonstrate the logic and value of the matrix.[114]

In scenario one, based on the Cabinet's decision, the Minister of Foreign Affairs has ordered a negotiation team on bilateral trade cooperation with State B to pause consultations (see option 2 and Table 25.2).[115] The decision came after the annual report by one of the Intelligence Services revealed that B was caught in an attempt to exfiltrate stolen intellectual property. The Minister just announced this in Parliament, who have formulated questions to learn more details. Using the matrix, this example can be expressed as the following (see Table 25.2).

Another vignette involves a counter-intelligence operation (see option 5, and Table 25.3). Based on authorisation by the Minster of Home Affairs, the General Intelligence and Security Service (AIVD), has taken control over a command and control server located in State B that was used by one of B's proxies, to steer a large botnet threatening to overload C2000 communications. The Minister has informed the Parliamentary Intelligence Committee (CIVD), and the Review Committee on the Intelligence and Security Services (CTIVD) is aware of the operation and will evaluate the legitimacy of the operation in the coming year.

[114]As States will have different institutional and constitutional settings, these vignettes based on the Dutch background serve as an example only.

[115]See e.g. Van der Meer 2018.

25.7 Conclusion

Contemporary conflicts are no longer exclusively fought in the military domain, if they ever were. Other arenas and instruments of power have come to the fore. Next to military power, economic, diplomatic, cultural, legal and especially informational means are important in today's world in which physical confrontation is often absent or less relevant, *inter alia* due to the emergence of cyberspace as an omnipresent domain of engagement.

In order to effectively apply State power, through whatever instrument, the capacities need to be in place as well as the will to apply them. An often-overlooked factor however is the conceptual component: a clear idea on how to apply the instruments, the relevance of which only increases with the widening set of instruments of power States may consider, or be forced to employ, such as cyber operations.

For democratic States the conceptual component fundamentally includes the legal framework and proper and well established institutional arrangements. The legal framework, often undervalued, generates the conceptual legitimate basis for executing operations, including deterrence operations. It includes the legal basis in terms of proper authority and decision-making procedures, legal regimes, accountability and oversight mechanisms. Moreover, the framework must not merely exist, it must be trained in a cross-domain setting, because in case essential parts of the legal framework are lacking, outdated, not well known or badly rehearsed, the conceptual component is suboptimal, and credibility, hence also effectiveness, of the deterrent instrument could be at stake.

Although this framework was set up within cyberspace and with cyber threats as a starting point, the argument is that in its generic shape, this legal framework is relevant outside cyberspace in expressing the State's will and for countering outside threats. The framework itself, composed of international legal bases and other national legal elements, is presented here in a matrix, combining all instruments of powers, and applicable legal bases enabling the actual or potential use of those instruments in their various modalities.

The matrix also demonstrates that other strategic functions could benefit from the idea that power entails capacities, concepts to use it, and the actual will to do so. The examples demonstrated that threats from one domain could be countered by responses in another domain. The legal framework thus may empower the ambition to effectuate so-called cross domain deterrence.

References

AIV/CAVV (2011) Advisory Council on International Affairs/Advisory Committee on Issues of Public International Law. Cyber Warfare. Advisory Report no. 77/22. Online at: www.aiv-advice.nl or www.advisorycouncilinternationalaffairs.nl/documents/publications/2011/12/16/cyber-warfare. Accessed 1 May 2020

Algemene Rekenkamer (2019) Strengthening the digital defences: the cyber security and critical water structures. ARK, The Hague. https://english.rekenkamer.nl/publications/reports/2019/03/28/strengthening-the-digital-defences-the-cyber-security-of-critical-water-structure

Bellinger III J (2020) Suing China over the coronavirus won't help. Here's what can work. The Washington Post. https://www.washingtonpost.com/opinions/2020/04/23/suing-china-over-coronavirus-wont-help-heres-what-can-work/. Accessed 23 April 2020

Betz D J, Stevens T (2011) Cyberspace and the state: toward a strategy for cyber-power. Adelphi Series, 424. International Institute for Strategic Studies (IISS). Online via. http://dx.doi.org/10.1080/19445571.2011.636954

Biddle S (2006) Military Power: Explaining Victory and Defeat in Modern Battle, 5th edn. Princeton University Press, Princeton

Bijleveld A (2018) We have to steer the cyber domain, before it steers us (keynote speech). Militair Rechtelijk Tijdschrift. https://puc.overheid.nl/mrt/doc/PUC_248478_11/1/. Accessed 23 April 2020

Boddens Hosang J F R (2015) Force Protection, Unit Self-Defence, and Personal Self-Defence: Their Relationship to Rules of Engagement. In: Gill T D, Fleck D (eds) The Handbook of the International Law of Military Operations, 2nd edn. Oxford University Press, Oxford, Chapter 24, pp 476–501

Boddens Hosang J F R, Ducheine PAL (2020) Implementing Article 42.7 of the Treaty on European Union: Legal Foundations for Mutual Defence in the Face of Modern Threats. (SSRN forthcoming), pp. 14–15

Booz Allen (2020) Bearing Witness: Uncovering the Logic Behind Russian Military Cyber Operations, at https://www.boozallen.com/c/insight/publication/the-logic-behind-russian-military-cyber-operations.html. Accessed 1 May 2020

Borghard E D, Lonergan S W (2017) The Logic of Coercion in Cyberspace. Security Studies 26.3, pp 452–481

Barnett M, Duvall R (2005) Power in International Politics. International Organisation 59.1:39–75

Delerue F (2019) Reinterpretation or contestation of international law in cyberspace? Israel Law Review, 52.3, pp 295–326

Ducheine P A L (2015a) Non-Kinetic Capabilities: Complementing the Kinetic Prevalence to Targeting. In: Ducheine P, Schmitt M N, Osinga F P B (eds) Targeting: Challenges of Modern Warfare. TMC Asser Press, The Hague, pp 201-220 Online SSRN draft at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2474091

Ducheine P A L (2015b) Military Cyber Operations. In: Gill T D, Fleck D (eds) The Handbook of the International Law of Military Operations, 2nd edn. Oxford University Press, Oxford, Chapter 23, pp 456–475

Ducheine P A L, Arnold K L, Pijpers B M J (2020) Decision-Making and Parliamentary Control for International Military Cyber Operations by the Netherlands Armed Forces. https://ssrn.com/abstract=3540732. Accessed 1 May 2020

Ducheine P A L, Osinga F (2017) Winning without killing – The Strategic and Operational Utility of Non-Kinetic Capabilities in Crises, NL ARMS Netherlands Annual Review of Military Studies 2017. TMC Asser Press, The Hague

Ducheine P A L, Pijpers B M J (2020) The Notion of Cyber Operations. In: Tsagourias N, Buchan R (eds) The Research Handbook on the International Law and Cyberspace, 2nd edn. forthcoming. Edward Elgar, Cheltenham. https://ssrn.com/abstract=3575755. Accessed 1 May 2020

Ducheine P A L, Pouw E H (2009) Operation Change of Direction: A Short Survey of the Legal Basis and the Applicable Legal Regimes. In: De Weger M J, Osinga F P B (eds) Complex Operations: Studies on Lebanon (2006) and Afghanistan (2006-present). NL Arms - Netherlands Annual Review of Military Studies 2009. Netherlands Defence Academy, Breda, pp 51–96

Ducheine P A L, Pouw E H (2012a) Legitimizing the Use of Force. In: Van der Meulen J, Vogelaar A, Beeres R, Soeters J (eds) Mission Uruzgan: Collaborating in multiple coalitions for Afghanistan. AUP, Amsterdam, Chapter 3, pp 33–46

Ducheine P A L, Pouw E H (2012b) Controlling the Use of Force: Legal Regimes. In: Van der Meulen J, Vogelaar A, Beeres R, Soeters J (eds) Mission Uruzgan: Collaborating in multiple coalitions for Afghanistan. AUP, Amsterdam, Chapter 5, pp 67–80

Ducheine P A L, Van der Meulen J, Moelker R (2010) Legitimacy and Surveillance: Shifting Patterns of External Control. In: Soeters J, van Fenema P C, Beeres R (eds) Managing Military Organizations: Theory and Practice. Routledge, London, pp 29–41

Ducheine P A L, Van Haaster J (2014) Fighting Power, Targeting and Cyber Operations. In: Brangetti P, Maybaum M, Stinissen J (eds) Proceedings of the 6th International Conference on Cyber Conflict. CCDCOE, Tallinn, pp 303–328

Ducheine P A L, Van Haaster J, Van Harskamp R (2017) Manoeuvring and Generating Effects in the Information Environment. In: Ducheine P, Osinga F (eds) Winning without killing – The Strategic and Operational Utility of Non-Kinetic Capabilities in Crises, NL ARMS Netherlands Annual Review of Military Studies 2017. TMC Asser Press, The Hague, pp 155-180 online SSRN version: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2979287

Dutch Safety Board (2020) Patient safety during IT outages in hospitals. Onderzoeksraad voor de Veiligheid, The Hague. https://www.onderzoeksraad.nl/en/media/attachment/2020/2/13/patient_safety_during_it_outages_in_hospitals.pdf. Accessed 1 May 2020

Finnemore M, Hollis D B (2019) Beyond Naming and Shaming: Accusations and International Law in Cybersecurity. https://ssrn.com/abstract=3347958. Accessed 1 May 2020

Fischerkeller M P, Harknett R J (2017) Deterrence is Not a Credible Strategy for Cyberspace, In: Foreign Policy Research Institute (ed) Orbis 61.3, pp 381–393

France (2019) International law applied to operations in cyberspace. https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf. Accessed 1 May 2020

Geiss R, Lahmann H (2013) Freedom and Security in Cyberspace: Shifting the Focus Away from Military Responses Towards Non-Forcible Countermeasures and Collective Threat-Prevention. In: Ziolkowski K (ed) Peacetime Regime for State Activities in Cyberspace International Law, International Relations and Diplomacy. NATO CCDCOE, Tallinn, pp. 621-658 SSRN: https://ssrn.com/abstract=2462950

Gibson W (2018) Neuromancer, Ace. Penguin Press, New York, p 22

Gill T D (1992) The Forcible Protection, Affirmation and Exercise of Rights by States under Customary International Law. Netherlands Yearbook of International Law 23:105–173

Gill T D (2013) Non-Intervention in the Cyber Context. In: Ziolkowski K (ed) Peacetime Regime for State Activities in Cyberspace International Law. International Relations and Diplomacy. NATO CCDCOE, Tallinn, pp 217–238

Gill T D (2015) Legal Basis of the Right of Self-Defence Under the UN Charter and Under Customary International Law. In: Gill T D, Fleck D (eds) The Handbook of the International Law of Military Operations, 2nd edn. Oxford University Press, Oxford, Chapter 8, pp 213–224

Gill T D, Ducheine P A L (2012) Anticipatory Self-Defence in Cyber Warfare. In: Schmitt M (ed) Cyber War and International Law. 89 International Law Studies 2012, pp 438-471. https://digital-commons.usnwc.edu/ils/vol89/iss1/6/

Gill T D, Ducheine P A L (2015) Rescue of Nationals. In: Gill T D, Fleck D (eds) The Handbook of the International Law of Military Operations, 2nd edn. Oxford University Press, Oxford, Chapter 12, pp 240–243

Gill T D, Fleck D (eds) (2015) The Handbook of the International Law of Military Operations, 2nd edn. Oxford University Press, Oxford

Giumelli F (2017) Winning Without Killing: The Case for Targeted Sanctions. In: Ducheine P, Osinga F (eds) Winning without Killing – The Strategic and Operational Utility of Non-Kinetic Capabilities in Crises, NL ARMS Netherlands Annual Review of Military Studies 2017. TMC Asser Press, The Hague, pp 91–106

Jakobsen P V (1998) Western Use of Coercive Diplomacy After the Cold War. MacMillan, London

Jakobsen P V (2007) Coercive Diplomacy. In: Collins A (ed) Contemporary Security Policy. Oxford University Press, pp 225–247

Jakobsen P V (2011) Pushing the limits of military coercion theory. International Studies Perspectives 12:153–170
Kitzen M (2012a) Close encounters of the tribal kind: the implementation of co-option as a tool for de-escalation of conflict: the case of the Netherlands in Afghanistan's Uruzgan Province. Journal of Strategic Studies 35(5):713–734
Kitzen M (2012b) Western military culture and counter-insurgency, an ambigious reality. Scientia Militaria: South African Journal of Military Studies 40.1:123–134
Koh H H (2012) International Law in Cyberspace. Faculty Scholarship Series, 4854, pp 1–9
Kuehl D T (2009) From Cyberspace to Cyberpower. In: Kramer F D, Starr S H, Wentz L K (eds) Cyberpower and National Security. University of Nebraska Press, pp 24–42. https://doi.org/10.2307/j.ctt1djmhj1.7
Łoś R (2019) U.S. and China: Hard and Soft Power Potential. International Studies. Interdisciplinary Political and Cultural Journal 22(1):39–50. https://doi.org/10.18778/1641-4233.22.03
Mann M (2013) The Sources of My Sources. Contemporary Sociology: A Journal of Reviews 42.4:499–502
Max Planck Encyclopedia of Public International Law [MPEPIL]. https://opil.ouplaw.com/home/mpil. Accessed 1 May 2020
NATO (2016) Warsaw Summit Communiqué, (July), pp 1–30
NATO (2017) Allied Joint Doctrine - AJP 01
Nye Jr J S (2013) Hard, Soft, and Smart Power. In: Cooper A F, Heine J, Thakur R (eds) The Oxford Handbook of Modern Diplomacy, pp 1–17
Nye Jr J S (2016) Deterrence and Dissuasion in Cyberspace. International Security, 41.3:44–71
New York Times (2018) Italy Orders Seizure of Migrant Rescue Ship, 20 November 2018. https://www.nytimes.com/2018/11/20/world/europe/italy-aquarius-seizure-order.html. Accessed 1 May 2020
New York Times (2019) U.S. Seizes North Korean Ship for Violating Sanctions, 9 May 2019 https://www.nytimes.com/2019/05/09/us/politics/wise-honest-north-korea-ship-seized.html. Accessed 1 May 2020
NL Defence Staff (2019) Netherlands' Defence Doctrine. Ministry of Defence, The Hague. https://english.defensie.nl/downloads/publications/2019/06/27/netherlands-defence-doctrine. Accessed 1 May 2020
Pirker B (2013) Territorial Sovereignty and Integrity and the Challenges of Cyberspace. In: Ziolkowski K (ed) Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy. NATO CCDCOE, Tallinn, pp 194–199
Qiao L, Wang X (1999) Unrestricted Warfare. PLA Literature and Arts Publishing House, Beijing. https://archive.org/details/Unrestricted_Warfare_Qiao_Liang_and_Wang_Xiangsui/mode/2up
Rid T, Buchanan B (2015) Attributing Cyber Attacks. Journal of Strategic Studies 38(1–2):4–37
Rodriguez C A, Walton T C, Hyong C (2020) Putting the "fil" into "dime": growing joint understanding of the instruments of power. Joint Force Quarterly 97.2:121–128
Sanger D E (2016) Obama Strikes Back at Russia for Election Hacking. In: New York Times (29 December 2016) https://www.nytimes.com/2016/12/29/us/politics/russia-electon-hacking-sanctions.html. Accessed 1 May 2020
Sari A (2020) Hybrid threats and the law: Concepts, trends and implications. Hybrid Centre of Excellence Trend Report 3 (April) https://www.hybridcoe.fi/wp-content/uploads/2020/05/Hybrid-CoE-Trend-Report-3.pdf. Accessed 1 May 2020
Schmitt M N (2013a) Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press, Cambridge
Schmitt M N (2013b) Cyber Activities and the Law of Countermeasures. In: Ziolkowski K (ed) Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy. NATO CCDCOE, Tallinn, pp 659–690
Schmitt M N (2014a) 'Below the Threshold' Cyber Operations: The Countermeasures Response Option and International Law. Virginia Journal of International Law 54 https://ssrn.com/abstract=2353898. Accessed 1 May 2020

Schmitt M N (2014b) Normative Voids and Asymmetry in Cyberspace. Just Security (29 December 2014). http://justsecurity.org/18685/normative-voids-asymmetry-cyberspace. Accessed 1 May 2020
Schmitt M N (2017) Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd edn. Cambridge University Press, Cambridge
Schroeder R (2015) Introduction: the IEMP model and its critics. In: Hall J A, Schroeder R (eds) An Anatomy of Power: The Social Theory of Michael Mann. Cambridge University Press, Cambridge, pp 1–16
Smeets M, Soesanto S (2020) Cyber Deterrence Is Dead. Long Live Cyber Deterrence! Council on Foreign Affairs, pp 1–6
Smeets M, Work J D (2020) Operational Decision-Making for Cyber Operations: In Search of a Model. The Cyber Defense Review (March). https://cyberdefensereview.army.mil/About-CDR/. Accessed 1 May 2020
Taddeo M (2018) The Limits of Deterrence Theory in Cyberspace. Philosophy & Technology 31.3:339–355. https://doi.org/10.1007/s13347-017-0290-2
Tallinn Manual (2013), see Schmitt M N (2013a)
Tallinn Manual 2.0 (2017), see Schmitt M N (2017)
UK Ministry of Defence (2010) Joint Doctrine Publication 04: Understanding a JDP 04, 1st edn. DCDC, Swindon. http://knowreqts.yolasite.com/resources/1.3%20%20JDP04%20Understanding.pdf. Accessed 1 May 2020
UK Foreign and Commonwealth Office (2020) Press release—UK condemns cyber actors seeking to benefit from global coronavirus pandemic
UK Ministry of Defence (2011) Joint Doctrine Publication 0-01: British Defence Doctrine
UK Ministry of Defence (2017) Land Operations - ADP AC 71940. Centre Land War Doctrine
US Cyber Command (2018) Achieve and Maintain Cyberspace Superiority
US DOJ (2018a) Department of Justice: Internet Research Agency Indictment https://www.justice.gov/file/1035477/download. Accessed 1 May 2020
US DOJ (2018b) Department of Justice: GRU Indictment. https://www.justice.gov/file/1080281/download. Accessed 1 May 2020
US Joint Chiefs of Staff (2013) Joint Publication 1: Doctrine for the Armed Forces of the United States
US White House (2016) Fact Sheet: Actions in Response to Russian Malicious Cyber Activity and Harassment (29 December 2016) https://perma.cc/C83Z-SQSL. Accessed 1 May 2020
Van den Boogaard J C (2019) Proportionality in international humanitarian law .PhD, University of Amsterdam. https://hdl.handle.net/11245.1/57363698-c6b8-458d-9033-0fd9cfc9bb91. Accessed 1 May 2020
Van der Meer S (2018) State-level responses to massive cyber-attacks: a policy toolbox. Clingendael Policy Brief (December). https://www.clingendael.org/sites/default/files/2018-12/PB_cyber_responses.pdf. Accessed 1 May 2020
Van Haaster J (2019) On cyber: the utility of military cyber operations during armed conflict. PhD, University of Amsterdam, NLDA, Breda. https://pure.uva.nl/ws/files/37093787/Thesis.pdf. Accessed 1 May 2020
Voetelink J (2015) Status of forces: criminal jurisdiction over military personnel abroad. TMC Asser Press, The Hague
Voetelink J E D (2017) Reframing Lawfare. In: Ducheine P, Osinga F (eds) Winning without Killing – The Strategic and Operational Utility of Non-Kinetic Capabilities in Crises, NLARMS Netherlands Annual Review of Military Studies 2017. TMC Asser Press, The Hague
Whyte C (2016) Ending cyber coercion: Computer network attack, exploitation and the case of North Korea. Comparative strategy, 35.2:93–102. https://doi.org/10.1080/01495933.2016.1176453
Wiltenburg I L (2019) Security force assistance: practised but not substantiated. Militaire Spectator 188(2):88-99. https://www.militairespectator.nl/sites/default/files/uitgaven/inhoudsopgave/MilitaireSpectator2-2019Wiltenburg.pdf

WRR (2019) Netherlands Scientific Council for Government Policy. Preparing for Digital Disruption (Summary), WRR-report no. 101. WRR, The Hague. https://english.wrr.nl/topics/digital-disruption/documents/reports/2019/09/24/preparing-for-digital-disruption. Accessed 1 May 2020

Young N (2009) The Cultural Crusades. New Internationalist 423:8–10 https://newint.org/features/2009/06/01/culture. Accessed 1 May 2020

Ziolkowski K (2013) General Principles of International Law as Applicable in Cyberspace. In: Ziolkowski K (ed) Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy. NATO CCDCOE, Tallinn

Paul Ducheine (Ph.D.) is an active serving general officer of the Netherlands Army and Professor of Cyber Operations at the Netherlands Defence Academy (NLDA), as well as Endowed Professor of Military Law of Cyber Operations and Cyber Security at the University of Amsterdam.

Peter Pijpers is Associate Professor for Cyber Operations at the Netherlands Defence Academy and Ph.D. Candidate at the University of Amsterdam.

Part VI
Conclusion

Chapter 26
Conclusion: Insights from Theory and Practice

Tim Sweijs and Frans Osinga

Contents

T. Sweijs (✉) · F. Osinga
Faculty of Military Sciences, Netherlands Defence Academy, Breda, The Netherlands
e-mail: timsweys@gmail.com

F. Osinga
e-mail: fpb.osinga@mindef.nl

F. Osinga and T. Sweijs (eds.), *NL ARMS Netherlands Annual Review of Military Studies 2020*, NL ARMS, https://doi.org/10.1007/978-94-6265-419-8_26

Strategists are fond of saying that the nature of war is immutable, but its character is not.[1] Even Von Clausewitz, whose very objective was to develop a general theory of war, held that every age has "its own kind of war, its own limiting conditions, and its own peculiar preconceptions."[2] The same can be said for strategy. History offers ample examples of strategic concepts that guide how means are to be connected to political ends in order to defeat adversaries in particular historical contexts. Warfighting concepts have included dislocation and exhaustion to target the adversary's will, and attrition and annihilation to deal with its capabilities.[3] In times of relative peace such concepts have included containment, assurance and most famously deterrence. The use and utility as well as the practical application—the character—of such concepts are context bound as they are determined by a range of social, economic, (geo-)political and technological factors.[4] Some strategic concepts wither away and are consigned to the dustbin of history; other concepts persist and are updated to address the challenges of today's world. Deterrence belongs to that latter category. It continues to feature as a prominent concept in contemporary strategic thinking and practice.

26.1 Deterrence Rediscovered

Although deterrence was neglected in military doctrines and real world campaign designs for about two decades following the Cold War, in practice it was never absent (and that disconnect might well have been one of the major factors hampering achieving operational success). In the first part of the book Lawrence Freedman elegantly lays out this recent history of deterrence in theory, policy and practice to remind us of its enduring presence and utility as well as its complexity. The Cold War flattered deterrence, he dryly observes, suggesting deterrence is easy. It is not. While in some cases general deterrence might have transformed into an established norm guiding international behaviour, in many cases deterrence was

[1] Gray 2016.
[2] Von Clausewitz 1989, p. 593.
[3] Echevarria 2017, p. 9.
[4] Murray et al. 1994.

problematic and failed because it revolved around deterring specific unwanted behaviour in a crisis where a state or non-state aggressor thought his interests were better served with challenging the status quo. As Freedman concludes, "deterrence works best with unambiguous red lines, established over time, linked with vital interests, formulated in clear and credible messages, backed by actual capabilities, about what will happen if they are crossed. It will work less well as more uncertainties are introduced—about where the lines actually are, how much any transgressions will matter, whether there will be much of a response if they are crossed, and what difference that will actually make." Freedman therefore warns us in Chap. 1 that deterrence's efficacy should not be taken for granted, especially not in unique situations when deterrent threats are formulated under time pressure and their credibility is in doubt.

26.1.1 Deterrence—A Fresh Perspective

Michael Mazarr, in Chap. 2, a wonderfully concise primer on deterrence, captures the various familiar conceptual distinctions—general versus immediate, direct versus extended, narrow versus broad, denial versus punishment—but importantly adds that, in contrast to the classical works on deterrence that harped on (nuclear) capabilities, the most important conclusion of his chapter is that "deterrence and dissuasion must be conceived primarily as an effort to shape the thinking of a potential aggressor". Mazarr argues that in designing a deterrent posture a deterring state should first and foremost understand the "interests, motives, and imperatives of the potential aggressor, including its theory of deterrence (taking into account what it values and why)." This is necessary because the behaviour of potential transgressors is not necessarily the exclusive product of belligerent expansionism. Effective deterrence therefore involves more than mere threats and requires "the nuanced shaping of perceptions so that an adversary sees the alternatives to aggression as more attractive than war".

26.1.2 Conventional Deterrence

Karl Mueller agrees with that admonition in his discussion on conventional deterrence in Chap. 4. Deterrence is not dependent on war appearing costly or risky in the eyes of the target: it requires that the prospect of war appears worse than the other options, which is certainly not always the case. The potential transgressor's cost benefit assessment of war is fundamentally shaped by its beliefs about the consequences of it actions, or, in other words, by its subjective expectations. History is rife with cases of misperception and mistaken prediction and decision-makers pursuing courses of action that in hindsight they had been better off not pursuing.

Deterrence by conventional military force has its limitations; it is contestable. The challenger can take defensive measures so that the deterrer will not be able to inflict the damage that it threatens with. It requires substantial force to ensure that costs can be inflicted to translate into coercive pressure. Conventional deterrence is nonetheless selected because often deterrence by nuclear or unconventional instruments is too costly, or deploying such instruments is seen as 'incredible, unpalatable, or simply inconceivable'. Mueller analytically distinguishes between four conventional deterrence strategies: battlefield defeat, punitive resistance, strategic retaliation, strategic defeat (threatening the opponent with defeat after a prolonged war). In addition to substantial military force, effective conventional deterrence requires robust political will and endurance on the side of the deterrer, to convince the potential transgressor that the threat will materialise in the end. Finally, deterrence may also require making "not going to war look more attractive though reassurance measures or promises of rewards".

26.1.3 NATO and the Shock of the Old

For the West, the rise of China and the resurgence of Russia has heralded a new era of strategic competition, in which nuclear deterrence has returned to the political, military and academic agenda. The markedly different geopolitical context poses a new set of distinct conceptual, strategic and political dilemmas to Western states and their security organisations, as Sten Rynning argues in Chap. 3. For the North Atlantic Treaty Organization (NATO), deterrence of Russian aggression has made tackling challenges related to power projection, force modernization, and burden-sharing more paramount. According to Rynning, "in addition to its limited muscle, it lacks institutional memory when it comes to joint high-intensity warfare, and faces a political geography that favours Russian interior lines and confounds NATO plans of reinforcement, and discomfort with a new interface between conventional and nuclear deterrence." It is not good at understanding either Russia's political intentions or its military capabilities. The rise in nationalism in NATO member states undermines the cohesion of an alliance founded on liberal values. Meanwhile, NATO is still trying to articulate a vision and a concomitant long term strategy for engaging its decidedly non-liberal neighbour. The combination of NATO's conventional military shortcomings, Europe's geographical makeup, and Russia's anti-access area-denial capabilities means that NATO is almost forced to rely on a deterrence by punishment posture by default. The military plan underpinning that posture is prepared but, as we know from traditional deterrence theory, robust capabilities need to be accompanied by clear political will in order for deterrent threats to be credible.

26.1.4 High Expectations: NATO Deterrence and the Baltic States

NATO's challenges, and its search for a coherent deterrence strategy, are explored in the context of the Baltic states where they become tangible by Jörg Noll et al. in Chap. 7. Using a strategic cultural perspective, they explore how the three Baltic states perceive the underlying strategic logic of NATO's Enhanced Forward Presence (EFP) in the Baltics as a deterrent instrument. In Estonia, government documents reflect the official NATO narrative of deterrence by punishment, even if other sources stress the illusion, expectation or aspiration of deterrence by denial. In Lithuania, both documents, officials and experts emphasise deterrence by denial as opposed to deterrence by punishment. Latvia considers the strategy behind EFP as one of deterrence by punishment. The strategic cultures, the history and threat perceptions of the Baltic states explain these differences to a large extent, so the authors argue. In particular, the presence of Russophone minorities in Estonia and Latvia may account for some of the reluctance of these countries to fully embrace NATO's strategy, even though both countries prepare to counter Russia's threat with their allies. If for the US and Western European states NATO's deterrence strategy and its challenges at times remain rather abstract, for the Baltic states, clarity concerning the nature and credibility of the deterrence strategy is an acutely felt requirement and differences in interpretation may undermine rather than reinforce that strategy.

26.1.5 Extended Deterrence

Several other challenges to deterrence stability are discussed in this volume, each a manifestation in its own right of the significant differences between the contemporary geopolitical context in comparison to the Cold War. Paul van Hooft puts the spotlight back again on the political drivers shaping the present and future of the US' extended deterrence posture in Chap. 6. He assesses not only technical and doctrinal developments but also points towards the critical role of economic and political interests, warning that the US nuclear umbrella for its European allies will not necessarily endure into perpetuity given the vastly different strategic circumstances of the 21st century. Van Hooft therefore considers U.S. extended deterrence guarantee to be "precarious"; extended nuclear deterrence has always been "inherently dubious" but increasing uncertainty about the ability of the US to win a conventional conflict at limited costs, and asymmetric interests is likely to further exacerbate that dubiousness. It also suggests that nuclear weapons will be playing a more important role in the US extended deterrence posture.

26.1.6 Nuclear Deterrence, Stability and Arms Control

Alexey Arbatov also looks at extended deterrence in Chap. 5. He complements van Hooft's analysis with an examination of recent trends in Russian nuclear strategy and policy. Arbatov notes that over the past thirty years, the nuclear capabilities of Russia and the US have been significantly reduced both in terms of warheads and in terms of kilotons but the risk of nuclear war is higher than it was at the end of the Cold War. Recent adaptations of the nuclear postures of these two nuclear giants collide with a period of substantial military-technological change. Arbatov describes how the introduction of new effectors and enablers such as hypersonic missiles, space-weapons, cyber instruments, and the integration of AI in nuclear command and control systems poses a formidable challenge to strategic stability. Early warning systems can be either be attacked or fooled by new space and cyber capabilities. The use of sea based missiles can shield the identity of the attacker. Hypersonic missiles make earth based radars irrelevant and significantly shorten the time to respond after detection by satellite systems which are not one hundred percent flawless. This takes place in the context of a polarised US-Russia relationship in which there is little interest from either side to collaborate through confidence building measures and arms reduction treaties. His ominous analysis concludes with a set of concrete policy recommendations for the foundations of a new generation of arms control initiatives to promote strategic stability. Perhaps the most important take away from his chapter is the vivid reminder, coupled with the important warning, that nuclear stability presumes a shared understanding of the meaning of strategic stability and a willingness to invest not only in deterrence capabilities, but also in a stability enhancing mutually agreed upon political framework.

26.1.7 Cross-Domain Deterrence

The emerging era of strategic competition has spawned a stream of literature propagating labels such as hybrid warfare, grey zone competition, new total war, and liminal war. If anything, they are reflective of a growing awareness that actors such as China and Russia, but also Iran and others utilise a wide array of military and non-military activities for coercive purposes. These include economic pressure, disinformation campaigns, inciting political corruption, espionage, providing weapons to opposition groups, polarising domestic debates in target countries, and cyberattacks. Partly in response to this development, and partly in response to the emergence of cross domain war fighting strategies in strict military domains, Western analysists have coined the notion of cross domain deterrence.

Tim Sweijs and Samuel Zilincik assess a recent body of literature on cross domain deterrence in Chap. 8 and argue that it offers plenty of practical insights on how to effectuate measures to deal with challenges related to attribution, threat

credibility and proportionality, signalling and escalation management both in and across domains, but has also engendered innovation on the conceptual front. Their review reveals significant continuities but also significant changes in the insights offered by the cross domain deterrence literature in comparison with the classical literature. They relate that deterrence has been cross domain in character since its inception and observe that the continuities with traditional deterrence literature are indeed considerable. Traditional concepts of deterrence by punishment and denial still feature in the strategic lexicon, while favouring conditions of successful deterrence including the communication of credible threats of cost imposition rooted in robust capabilities and strong political will is also extensively discussed. Yet, the cross-domain deterrence literature also provides a range of new theoretical insights both by reinterpreting and by expanding traditional concepts of deterrence. It employs a more sophisticated understanding of the cost-benefit calculus of deterrence actors that considers identity and social belief systems. It includes both traditional and new military domains as well as non-military domains such as the economic and the information domains. It calls attention to the role of social costs in deterrence by punishment arguing for the important role of norms in deterrence by delegitimisation because transgressors will be disinclined from engaging in certain behaviour out of moral conviction or fear that it will result in widespread condemnation. It finally expands the scope from negative to positive incentives through deterrence by entanglement in which transgressors hurt themselves if they harm the deterring actor.

On this basis, they assert that the discussion in the cross-domain deterrence scholarship is more than old wine being served in new bottles. Finally, they conclude that this conceptual expansion of deterrence that involves a wide array of military and non-military instruments which can be used "both as a stick and a carrot, both to compel and to deter, both to persuade and to dissuade", may well be necessary to deal with today's strategic challenges, but they suggest that the use of dissuasion as the umbrella term for the wider deterrence by denial and punishment, norms, entanglement, resilience and assurance may be more appropriate.

26.2 Non-Western Concepts of Deterrence

26.2.1 Russia and China

In comparison to traditionally much more straitjacketed and dichotomous understandings of deterrence that prevailed in the West, official Chinese and Russian concepts of deterrence are rooted in much more holistic understandings. These holistic understandings encapsulate elements of both deterrence and compellence, can take place before, during and after war, and cross military and civil domains, as highlighted by Dean Cheng in Chap. 10 and Dmitry Adamsky in Chap. 9.

Starting with an insightful exploration of the etymological Russian roots of deterrence related concepts, Adamsky explains that Deterrence *à la Ruse* stands for "the use of threats, sometimes accompanied by limited use of force, to preserve the status quo ("to deter" in Western parlance), to change it ("to compel" in Western parlance), to shape the strategic environment within which the interaction occurs, to prevent escalation and to de-escalate during actual fighting". This is different from the Western conceptualisation in which deterrence suggests a reactive approach while compellence a more proactive approach. Strategy is being wrought as part of a permanent engagement, with no distinction between peacetime and wartime. Adamsky uses the term *struggle* to denote the Russian notion of strategic interaction in its totality. The common dichotomy of war versus peace has meaning only in the sense that it signifies the level of intensity of the competition, which is regarded as continuous and takes place before, during and after armed conflict. This logic informs the Russian understanding of deterrence throughout the entire spectrum of strategic interaction including preventing a threat from emerging in the first place whether or not in peacetime, using force in crisis or war, or shaping the strategic environment afterwards.

The Chinese conceptualisation is closer to the Russian than to Western concepts of deterrence, allowing for substantial differences. Referring to official Chinese literature and scholarly analysis, Dean Cheng suggests that the Chinese do not necessarily think in terms of deterrence, as that term is employed in Western strategic literature, but in terms of coercion. Whether an adversary agrees to do something they would prefer not to do, or avoids doing something they would prefer to do, both fit within the Chinese term *weishe*. This term incorporates both compellence and dissuasive aspects. Moreover, instead of regarding deterrence as a goal, in the Chinese conceptualisation deterrence is seen as an instrument. For Chinese decision-makers, Cheng explains, successful deterrence is ultimately a form of political activity and psychological warfare, whereby an adversary is constrained in its actions, allowing China to achieve its objectives. The concept is used to describe signalling and activities both towards and during military conflict, and spans all phases of war. As such, Cheng concludes, the Chinese interpretation of deterrence is closer to the Western conceptualisation of 'coercion' in its pre-war and intra-war forms.

In the Russian and Chines conceptualisations of deterrence, power accrues from the employment of both military and non-military instruments. In that sense, theirs is a multi-domain concept of deterrence that includes nuclear, space, and information means. Moreover, both share the idea that coercive efforts are closely tied to their war-fighting concepts. As Cheng notes, Chinese deterrence capability is "based on the ability to wage real war", and the structure of deterrent strength is indistinguishable from combat strength, including mounting nuclear strikes. Adamsky in Chap. 9 also explains that in Russian strategic thinking the notion of military victory has not disappeared from nuclear strategy. The linkage itself, by raising issues of crisis stability, enhances deterrent effects. Applying the Western terminological framework to explain Russian and Chinese concepts may thus lead to misperceptions, and mirror imaging invites strategic mistakes.

26.2.2 Iran

The Iranian concept of deterrence present another fascinating case that illustrates the limits of classical Western conceptualisations of deterrence and the importance of strategic context and strategic culture. Hassan Ahmadian and Payam Mohseni rightfully highlight a dearth of theoretical work on deterrence in non-western settings in Chap. 13. They explain that the difficulty of understanding Iranian behaviour stems from the fact that the country's strategy is built on a combination of conventional and asymmetric deterrence that incorporates the support of other state and non-state actors. The logic stems from the strategic history of Iran and Syria. Their threat perceptions, the authors explain, have been shaped by a shared sense of regional isolation and a shared antiimperialist ideology. The two countries forged a partnership with the practical objective of deterring regional threats from their main adversaries primarily the United States, Israel, and Iraq under the regime of Saddam Hussein.

Iran maintains a two-pronged deterrence strategy. Its conventional deterrence capabilities are largely rooted in its domestic ballistic missile programme and its capacity to use missiles to hit regional targets (such as strikes in Iraqi Kurdistan and on ISIS positions in Syria). Iran also has asymmetrical deterrence capabilities largely through its support of regional non-state actors, such as Hezbollah in Lebanon, and also through the operational activities of the external branch of the Islamic Revolutionary Guards Corps (IRGC), the Quds Force. The Iranian strategy within the Levant, Ahmadian and Mohseni argue, should be understood as "forward deterrence", defined as the "deployment or possession of deterrent capacity beyond one's own national borders that abut on the adversary's frontier". This strategy does not rely on direct forward deployment of armed forces. Instead deterrence capacity is predominantly provided by partners and allies. For Iran, the strategic function of Syria is to provide it with strategic depth in the Levant and access to Hezbollah. Syria also maintains a combined conventional and asymmetric deterrence strategy against Israel. Combined, the authors conclude, these elements constitute Iran's comprehensive deterrence doctrine in which it uses a diverse and multi-layered assortment of means to defend itself from any form of potential aggression.

26.2.3 Japan

The Japanese deterrence strategy is similarly deeply influenced by its history, as Nori Katagiri explains in Chap. 11. Japan's national security resources and institutions are not suited to deter foreign attackers because limitations on Japan's ability to offensive military operations—a necessary factor for deterrence relying on threats to impose costs. Existing restrictions on the use and threat of force stem from post-war constitutional and normative constraints. As a result, Japan's default

strategy is one of deterrence-by-denial which is hampered in its implementation by the inherent limit on its practical ability to deter foreign attacks.

26.2.4 India and Pakistan

In Chap. 12 Sander Ruben Aarten demonstrates how deterrence dynamics between two nuclear powers—India and Pakistan—may play out very differently than what classical deterrence theory suggests, once again underlining the notion that deterrence in practice is context specific. Classical deterrence theory argues that the risk of conventional war will diminish when both actors possess nuclear weapons and have a declared nuclear deterrence strategy, out of fear of inadvertently exceeding the nuclear threshold of the other actor. Since both countries openly declared themselves nuclear weapon powers in 1998, India faced the daunting challenge of formulating an effective counterterrorism strategy—deterring Pakistani incursions on the Kashmir region—while remaining under Pakistan's nuclear threshold. India's response was the 'cold start doctrine'. This doctrine involves limited retaliatory advances inside Pakistan by rapidly mobilising infantry and armour before Pakistan's defensive positions can be occupied. In reaction, Pakistan developed its doctrine of full spectrum deterrence. As Aarten contends, the idea behind full spectrum deterrence is to provide Pakistan with retaliatory options that are commensurate with the intensity of the aggression it faces by linking conventional means with nuclear options on all levels—from tactical to strategic. Strong cross domain dynamics are key features of the subcontinental deterrence landscape as a result. The risk is considerable as Pakistan keeps open the option of a nuclear first-use and India adheres to a doctrine of massive retaliation. Thus, an all-out nuclear exchange may result from a Pakistan-supported militant attack on Indian soil, if both states abide by their doctrines. Yet this has not occurred, as Aarten observes, due to a shared reluctance by both sides to escalate to the nuclear realm. These findings all indicate that nuclear deterrence is less unstable than is assumed by many analysts and scholars, but also that nuclear deterrence can invite circumventing strategies which may result in occasional probes and responses in the conventional domain. The stabilising effect of nuclear weapons may thus not percolate into the conventional domain.

26.3 Deterring Non-state Actors in Non-traditional Contexts

Today's deterrence literature also exhibits a keen appreciation for the specific requirements for the effective application of deterrence in internationalised intra-state conflict that is so prevalent today against state and non-state actors.

These contexts call for tailored deterrence, as Morgan discussed in 2012. Already during the peacekeeping operations of 1990s deterrence dynamics were at play at the local tactical level, which was again confirmed by counterinsurgency (COIN) operations in Iraq and Afghanistan. Counter-terrorism studies following the Al Qaeda attacks of 9/11 2001 focused on the question whether non-state actors could be deterred. A massive stream of studies dissected terrorist groups, suggesting that tailored deterrence might require specific approaches towards states sponsoring terrorist groups and towards leaders of terrorist groups while other influence methods might be more useful in preventing individuals from assisting or joining a terrorist group. The COIN literature emphasised the importance of mapping the socio-political structure of societies so as to identify those who might actively support the insurgents, who were politically supportive of them, and who might work with COIN units in suppressing them. These literatures—on peacekeeping, counter-terrorism, and counter-insurgency—often remained unconnected and unrelated to deterrence research.

Four studies in this volume address and remedy this disconnect. Eitan Shamir offers a thorough synthesis of research on the deterrence-violent non-state actor nexus in Chap. 14. In an innovative analysis in Chap. 15, Martijn Kitzen and Christina van Kuijck apply it to the COIN context where both insurgents and counter-insurgents vie for control over and support of the population. In Chap. 17, Peter Viggo Jakobsen applies deterrence theory to the context of peace operations where deterrence needs to focus on both state level actors and local non-state actors. Finally, in an imaginative contribution in Chap. 16, Maarten Rothman explores Russia's application of deterrence concepts in the context of preventing separatist or democratic movements to succeed in countries bordering Russia.

26.3.1 Deterring the Threat of Terrorism

In Chap. 14 Eitan Shamir builds on and synthesises a growing body of work on the nexus of deterrence and violent non-state actors. He details how Israel has developed a portfolio of tailored deterrence concepts against violent non-state actors that includes aspects of restrictive and cumulative deterrence aimed at curbing the opponent's ability but also at educating it in a process based approach that envisages a continuous deterrent relationship between the deterrer and the deterred. The consensus opinion held that terrorist groups, in particular those that are religiously motivated, are very hard to deter due to the fact that they present few tangible targets one can threaten, are often not monolithic organizations but consist of a covert network of relatively autonomous cells; there is not necessarily leadership with whom a state can communicate; while their fundamentalist ideologies preclude normal diplomatic negotiations; and the group will see the confrontation as a zero-sum game. The Israeli approach exemplifies a de facto reconceptualization of the meaning of deterrence, which once again corroborates the idea that strategic experience and culture has an important effect on concepts of deterrence.

Instead of conceiving of deterrence in absolute terms, which fails if one terrorist attack succeeds, Israel adheres to a restrictive deterrence approach. First, defensive infrastructure functions as part of deterrence, limiting the chance a terrorist attack will reach its target and achieve the destructive effect it seeks. Second, triadic deterrence involves threatening interests of those states that sponsor the terrorist group. Third, the mere fact that Israel uses force against groups such as Hamas or Hezbollah should not necessarily be considered a failure of deterrence, but as a reminder of Israel's ability to hurt such groups at will. It thereby serves to communicate that certain offensive actions have crossed the limit of violence Israel is willing to accept, thereby re-establishing the norm of what is considered acceptable. Moreover, a deterrent effect is not expected to accrue from symbolic attacks but from repeated strikes, whenever the norm has been violated. This so-called 'mowing the grass' approach also serves to degrade the capabilities and the will of the violent non-state actor. Restrictive and cumulative deterrence against violent non-state actors is therefore inspired more by criminological understandings of the notion than Cold War concepts of absolute deterrence.

26.3.2 Insurgents and Localised Deterrence

In Chap. 15 Kitzen and van Kuijck look at tactical and operational level challenges of deterring insurgents and ensuring support from the local population. They propose an influence continuum in combination with an audience typology and outline different methods to target different audiences that specifically includes non-kinetic instruments, all at the local level where troops must deal with local power brokers—legitimate or otherwise—and the local population. They argue that the popular western heart-and-minds approach overemphasises persuasive methods to influence the population which often fail against the more intimidating authoritarian approach employed by insurgents. Acknowledging that a social environment is made up of people which are friendly, neutral or hostile to the counter-insurgent force, localized deterrence, based on a solid socio-cultural understanding of the environment, flows from a fluid application of influence operations designed to deter undesired behaviour—support the insurgent—and convince the population and local power brokers that the counterinsurgent contingent represents a legitimate and effective presence which will succeed in establishing a lasting secure environment. That array of influence instruments includes soft tools (information), economic incentives, and rewarding cooperation (or the withdrawal thereof), but must also include, more than is generally admitted in Western doctrines, coercive tools, such as empowering rivals of local power brokers and, the use of force against so called irreconcilables.

26.3.3 Deterrence and Peace Operations

In Chap. 17 Peter Viggo Jakobsen considers deterrence in another important context that features both state and non-state actors: peace operations. The attacks on Western peacekeeping units in the Balkan in the 1990s prompted scholarly interest in how threats and use of limited force could help deter such attacks and/or compel transgressors to stop them. Peace forces operate in a fluid context in which strict demarcations between deterrence and compellence break down. Jakobsen's *ideal policy* framework lays out the minimum requirements for success to deter and compel transgressors in such an environment. First, a credible threat which is strengthened if the coercer can demonstrate a capability to defeat the adversary swiftly at little cost. Second, a deadline for compliance in order to convince an opponent to refrain or stop attacks or engage in other forms of hostile behaviour in order to create a sense of urgency. Third, assurance that there will be no additional demands following compliance. Fourth and finally, and in line with Mueller's advice, inclusion of positive inducements to reduce the costs of compliance. An important notion, in line with the analysis of Shamir, Kitzen and van Kuijck, is Jakobsen's emphasis that deterrence in peacekeeping operations involves multiple means targeting multiple actors. As he relates, a key lesson from the Balkan conflict was that the international coalition had to deter and to compel "a variety actors on and beyond the battlefield simultaneously". This required coercion tailored to the different actors at multiple levels. In his contribution Jakobsen expands on that lesson and distinguishes four groups of actors that facilitate or frustrate deterrence in peace operations: (1) *combatants* that use force on the battlefield; (2) *combatant allies* that material support to combatants; (3) *combatant supporters* that block action in regional or global institutions; and finally, (4) *bystanders,* from the battlefield to the global level, that fail to act. To succeed, Jakobsen concludes, deterring actors cannot rely solely on threats and use of force but must supplement their use of coercion with persuasion and inducement and devise and implement influence strategies that draw on all three components.

26.3.4 Deterring Revolts

Finally, in Chap. 16, Maarten Rothman examines the use of deterrence by president Putin of the Russian Federation against potential democratic revolts. While conceptually perhaps akin to the deterrence challenges explored by Shamir, Kitzen and van Kuijck, Rothman adds to their analyses by looking at the potential for a powerful state to use military threats to discourage popular movements against its puppets and allies. Combining insights from the literatures on democratic revolutions and social movements on the one hand, and deterrence and coercion on the other, Rothman hypothesises that from Putin's perspective two strategies present themselves to discourage or deter democratic revolts: suppression by the authorities

of the affected country and the threat of intervention against the pro-democracy protesters or prospective protesters, either in support of allied regimes during the uprising or as punishment after their overthrow. The target of deterrence experiences both a domestic and an outside threat simultaneously.

This outside threat is a safe guard for Putin for there is a limit to what extent he can rely on domestic repression for this is under the control of the local authorities, Putin's allies, who might take guidance or direction from him but for the most part rely on local resources and personnel. The effectiveness of domestic repression depends on local restraints and sympathies, including those of security services personnel. Their loyalty, Rothman suggests, might waver when they are asked to use violence against the protesters. Russian punishment therefore makes use of local strongmen but also employs Russian operators and usually a sizeable contingent of soldiers. Russia's ability to inflict punishment therefore does not suffer from the same constraints: those enforcing the repression are not compatriots, they are not sensitive to local sympathies, and any defections will not challenge Moscow's authority.

The drawback, as Rothman argues, for this type of deterrence is that democratic revolts are not conducted by a unitary actor but by an emergent collective which only emerges as a collective during the event. Backchannel negotiations and communicating threats is not an option and targeting the population at large might backfire. The deterrent effect however may be retained nevertheless because Russia can hurt democratic protesters in the sense that it can threaten to undermine the revolt's chances to make good on its promise of a better life after the revolt. Moreover, it can sustain the pain by propping up separatist governments, sustaining an environment rife with low-level violence with continued risk of escalation. Such punishment also ensures continued media attention which can be exploited to convey the message that the revolt will fail like previous revolts. As Rothman concludes, it serves Russia's interest, then, to periodically feed the media stories to fuel this narrative by manufacturing an incident. This chapter thus nicely complements Adamsky analysis of Russia's unique conceptualization of deterrence.

26.4 New Instruments and Domains

26.4.1 Cyber-Deterrence

In Chap. 20 Stefan Soesanto and Max Smeets, in a very rich synthesis of the debate on cyber deterrence, consider how different scholars evaluate the possibility of deterrence in cyber-space. According to Smeets and Soesanto, as a military concept, cyber-deterrence has at least three different meanings. It can refer to "the use of (military) cyber means to deter a (military) attack [..]; the use of (military) means to deter a (military) cyber-attack [..]; [and] the use of (military) cyber means to deter a (military) cyber-attack". Scholars currently disagree to what degree it is generally

possible to deter an adversarial cyber-attack. One group argues that cyber deterrence functions akin to conventional deterrence. Others believe cyber deterrence features unique issues because cyberspace is markedly different from the traditional domains (air, land, sea). A better understanding of the specifics of cyberspace and the dynamics of deterrence therein is required to explain when deterrence works or fails. According to the third group cyber deterrence is impossible; cyberspace features an abundance of actors all with access to offensive cyber weapons. Moreover, the threshold for offensive actions is low, the number of attacks high and the chance of retaliation slim. Finally, some hold that the strategic value of damage inflicted by cyber-attacks is generally limited and easy to contain and repair. Threats of a cyberattack therefore lack the punch required for effective deterrence.

Proponents of cyber deterrence, Soesanto and Smeets observe, tend to discuss one of the following four deterrence logics, which also appear in the cross domain deterrence literature discussed by Sweijs and Zilincik in Chap. 8: deterrence by denial (which is synonymous to cybersecurity); deterrence by punishment (costs will outweigh the benefits); deterrence by entanglement (interdependence may disincentivise states to launch cyber attacks); and deterrence by de-legitimisation (to "raise the reputational costs of bad behaviour, and shrink the battlespace to only encompass military combatants").

There is no consensus among scholars and strategists in this debate. While cyberspace may have been recognised as a new warfighting domain and constitutes an essential venue for single and cross domain operations, beyond the military utility of cyberattacks and cyber defence at tactical and operational levels, their strategic utility in support of deterrence is as of yet uncertain. One way out was adopted in the US strategy: in an environment of constant contact, a strategy grounded in persistent engagement is considered to be more appropriate than one of operational restraint and reaction for shaping the parameters of acceptable behaviour. This involves a high level of cyber activity to identify and track perpetrators and includes if necessary aggressive cyber operations. This stretches the notion of deterrence beyond the common understanding of the concept. Unsurprisingly, Soesanto and Smeets observe, European policymakers are not inclined to discuss, let alone consider, a strategy of persistent engagement, which is considered to be too aggressive. Moreover, they lack the operational capabilities to operate "seamlessly, globally, and continuously", which is required by persistent engagement. Theory development meanwhile remains a challenge since politically motivated cyberattacks with strategic impact are few in number, most of the documents are highly classified, there is little access to cyber operators, and existing military cyber organisations are in the embryonic stage. Going forward, Soesanto and Smeets outline four future avenues of research for cyber deterrence: further integration of cyber deterrence in more comprehensive deterrence postures in the context of multi-domain competition; greater focus on technical aspects at the operational and tactical levels; greater emphasis on compellence; and the exploration of novel strategic concepts "to contain and blunt adversarial aggression in cyberspace" outside of traditional deterrence thinking.

26.4.2 Artificial Intelligence

Embryonic is also an apt word to describe the development of Artificial Intelligence (AI) capabilities as well as the debate on their potential relevance for security policy, military strategy and deterrence theory and practice, as Alex Wilner and Casey Babb explain in Chap. 21. The limited knowledge base is reason for concern given the high expectations concerning a wide range of fruitful military AI applications including autonomous weapon systems (AWS). But also beyond AWS, they contend, AI will influence defence and security in several important ways. AI will alter the way states plan and conduct military engagements, collect and use intelligence, and protect their domestic national security. Traditional notions of state power are also increasingly intertwined with national expertise and investment in AI. An arms race is thought to be developing between the United States and China as a result.

Wilner and Babb explain the various ways AI is likely to affect coercion: AI may alter cost-benefit calculations by removing the fog of war, by superficially imposing rationality on political decisions, and by diminishing the human cost of military engagement. It may recalibrate the balance between offensive and defensive measures, tipping the scales in favour of pre-emption, and undermine existing assumptions embedded in both conventional and nuclear deterrence. AI might altogether remove human reasoning and emotions from the practice of coercion. It may provide users the ability to collect, synthesis, and act upon real-time intelligence from several disparate sources, augmenting the certainty and severity of punishment strategies, both in theatre and online, thereby compressing the distance between intelligence, political decisions, and coercive action. AI enhanced drones may be employed to swarm and overwhelm the defences of opponents, or, alternatively, offer a fail-safe automatic response option during escalation.

As a result, AI may quicken the overall pace of action across all domains of coercion, in conflict, crisis, and war. These factors may lead to ‘hyperwar’, they conclude, in which data will be filtered and analysed in near or real-time providing decision-makers with a greater awareness and more options far more quickly, but also result in higher risks for inadvertent escalation and—lured by the illusion of certainty and superiority—in risk-seeking behaviour. Currently this topic still belongs to the realm of speculation. The actual study of AI and deterrence and coercion has only just begun. Military AI enabled technologies are immature yet their consequences for deterrence can be expected to be significant. As military AI applications will materialise and be more fully integrated by defence organisations, AI deterrence theory will be informed by empirical analysis.

26.4.3 Sanctions

Sanctions are another instrument of direct relevance to deterrence strategy yet they have often been discussed in a different body of literature, despite the fact that threatening with and/or imposing a sanctions regime often has deliberate coercive purposes (signalling, constraining, compelling) and such sanctions regimes precede and surround subsequent steps to boost the deterrent signal with military threats. Sanctions, as Francesco Giumelli explains in Chap. 18, are supposed to inflict pain on the receiver, and the logic goes that such economic pain would translate into political gain, such as deterring the repetition of certain behaviours and the escalation of conflict. In addition, sanctioning a target shapes the expectations of other actors (or potential targets in the future) of the implications of certain activities.

During the Balkan crisis of the 1990s and Western campaigns against Libya and Iraq, comprehensive sanctions targeted entire economic sectors with disastrous humanitarian consequences. Moreover, sanctions were counterproductive as the real targets managed to either avoid the impact of sanctions or were, occasionally, even strengthened by them. Serbia for instance benefited from the arms embargo as they had control over a sizeable military arsenal. In Iraq, the population suffered the brunt of the embargo while Saddam Hussein continued to live in affluence. Subsequent research has indicated that different types of regimes—democratic or authoritarian—have different vulnerabilities and display different responses with authoritarian regimes at least in theory being more vulnerable to sanctions that hurt specific personal interests of the leadership. These insights coupled with detrimental effects of previous sanctions prompted scholars and practitioners to envisage targeted sanctions. Targeted sanctions include restrictions on freedoms for individuals and non-state entities as well as asset freezes and financial restrictions.

While potentially more effective than comprehensive sanctions and less prone to produce counterproductive side effects, Francesco argues that targeted sanctions also present new features complicating deterrence efforts. First, targeted sanctions frequently target individuals, and individuals behave according to different logics in comparison to complex organizations such as states. Moreover, individuals have human rights, which constrains the feasibility of targeted sanctions because sanctioning individuals requires evidence to be presented, indicted individuals need to be brought to court, and procedures to rectify mistakes made by listing authorities need to be in place. Second, while classical deterrence is based on the promise of serious damage to be inflicted, targeted sanctions are designed not to inflict lethal pain on their targets. Third, according to Giumelli, targeted sanctions can increase the likelihood of the behaviours that they intend to discourage as they present a problem of moral hazard; one party to the conflict might be incentivized to provoke a conflict if it expects that targeted sanctions would be imposed on the other side. Finally, sanctions today are used for a very long list of objectives in a variety of crises, from international terrorism, to non-proliferation, conflict management, post-conflict reconstruction, but also asset recovery as well as combating organized crime and human trafficking. “The over-utilization of sanctions”, he concludes,

"and their apparent light impact could undermine, rather than strengthen, an international criminal deterrence doctrine".

26.4.4 Resilience

In Chap. 19 Cees van Doorn and Theo Brinkel explore another instrument for boosting deterrence: resilience. Resilience has gained increasing attention following awareness of the potency of hybrid threats to disrupt the integrity of economic, social and political structures in Western democracies. Hybrid warfare opens the possibility to use all instruments short of actual war. Disinformation campaigns, that exploit social media, have been salient instruments. Spreading fake news as well as fuelling alternative narratives are part and parcel of attempts to dislodge Western democratic societies and undermine the morale of the population.

Resilience—the ability of individuals, communities, or organizations to prepare for disruptions, to recover from shocks and stresses, and to adapt and grow from disruptive experiences—has come to be considered a key pillar of deterrence against hybrid activities for multiple reasons. First, because it is impossible to defend against all threats societal resilience negates the benefits to be derived from any attacks. Second, acknowledging that effective deterrence typically depends on strong defence capabilities matched with equally credible political resolve, in the context of information warfare, credibility is also a decisive denial capability weapon. As Brinkel and van Doorn assert, veracity, consistency and respect for the truth are the exact opposite of disinformation campaigns and contribute to what has been described as deterrence by delegitimization. Resilience usually concerns technical solutions and infrastructure but resilience can also be found in attitudes, declarations, and images. It manifests itself in common values and objectives. Resilience is therefore a quintessential part of the social capital and trust in society and results from good governance, human rights and freedoms, as well as the rule of law.

Van Doorn and Brinkel use the aftermath of the downing of flight MH17 to explore how resilience has functioned as a deterrent to subversive Russian disinformation activities. They examine counter-measures (creating credible narratives, nuanced messaging, careful fact finding) implemented by the Netherlands government and analyse how these affected societal trust in reaction to disinformation activities. The Dutch government's narrative has consistently focused on three courses of action: bringing the victims home, establishing the facts about the circumstances in which the plane went down, and holding to account those responsible in the court of law while respecting the independent position of others, such as the Public Prosecution Service and the free press, in their search for the truth. Other sources of information, such as free independent news networks and digital forensic networks have been paramount in discrediting disinformation and allowing the public to reach its own conclusions. During the prosecution process, civic journalists played an important role in disclosing the exact route of the BUK missile

system entering and leaving Eastern Ukraine. As a result, Russian alternative narratives explaining the cause of the downing and deflecting the blame for it have not been able to gain any real foothold in Dutch society.

26.5 Decisions, Decisions

26.5.1 Game Theory, a Re-appraisal

The cool and perhaps even cold-hearted idea that game theoretical calculus should be the basis of deterrence strategy and inform decision making processes during a nuclear crisis has inspired much critique and resulted in a wave of research exploring how decision making works in reality. In Chap. 22 Roy Lindelauf nevertheless fruitfully reminds us of the utility of game theory, and argues for continued attention to it, also in light of the emergence of AI. Commonly used game and decision theoretic models fail to explain the empirics of deterrence and, as Lindelauf asserts, this has unjustly led many theorists to criticize the (rationality and other) assumptions underpinning of such models. Game theorists readily admit these models do not represent an accurate model of complex and varied decision making situations but merely describe what a decision maker *ought* to do in a given situation. As Lindelauf reminds us, "all models are wrong, but some are useful". Game theory can help to lay an axiomatic foundation under the theory of deterrence. Moreover, algorithms are entering each and every aspect of our lives including the command and control of weapon systems. Lindelauf expects that these systems will deploy game- and decision theory based algorithms to coordinate and control. Such AI and autonomous systems have the potential to dramatically affect nuclear deterrence and escalation and the fact that the nuclear deterrent decision-cycle will also be based on algorithmic analysis makes it paramount that we need to further develop game theory in the context of both the theory and the practice of nuclear deterrence.

26.5.2 How the Mind Plays Games with Rationality

Our understanding of targets' perceptions of deterrence and their reception of deterrent signals is deepened by the contributions by Tom Bijlsma (Chap. 23) and Samuel Zilincik and Isabelle Duyvesteyn (Chap. 24). Their contributions explore *terra* largely *incognita* by opening up the black box of the human psyche and concentrating on the role of emotions in deterrence, both on the part of the deterrer and on the part of the deterred. As Tom Bijlsma notes, research in the third wave, capitalising on new insights from the psychological, economics, and decision-making literature, indicated that decision making in reality deviated

substantially from the assumptions of the rational actor model. Apart from organisational and political interests, processes, routines, and group think, deterrence may fail because of misperception on either or both sides of the crisis. Bijlsma takes us on a tour along the causes of such misperceptions; the heuristics (rules of thumb) and biases (systemic errors such as inclinations or prejudices) that the human mind most often unconsciously employs as short-cuts to rationality, which colour the incoming stream of information and the processes to digest it and come to a decision.

Because of anchoring humans rely heavily on the first piece of information offered when making a decision. The confirmation heuristic reflects the human tendency to seek information that supports one's existing point of view and neglect or ignore signs that can lead to contrary evidence. The availability heuristic refers to the mental shortcut in judgments about the probability of events based on the ease with which examples come to mind. Improbable events are excluded from decision making processes. The representativeness heuristic compares a situation with mental models in our minds. Stereotyping and profiling are forms of this heuristic. The affect heuristic represents the fact that humans tend to be more positively inclined to what they like. The related fluency heuristic explains the fact that the human mind tends to give preference to an option if it is processed faster or more fluently than an alternative option. In other words, the more elegantly an idea is presented, the more likely it is to be considered seriously, irrespective of whether or not it is logical.

An important issue for deterrence research and strategy concerns the question how leaders deal with risk. Prospect theory explains that humans evaluate the potential value of losses and gains differently. In contrast to rational choice theory, prospect theory finds that decision makers are apt to overweight losses with respect to comparable gains, and tend to be risk averse when confronted with choices between gains while risk acceptant when confronted with losses. That explains perhaps why it is easier to deter an actor from starting an invasion than to compel him to retreat from territory it gained. In short, applied to deterrence dynamics, the result is that leaders are inclined to take more risks to maintain their positions, reputations etc., than they are to enhance their positions. The higher the stakes, the higher the risk of being caught in a psychological trap as Bijlsma concludes.

26.5.3 The Emotional Turn in Deterrence Theory

In Chap. 24 Samuel Zilincik and Isabelle Duyvesteyn continue further down this path by surveying recent insights concerning the role of emotions in decision making processes and assessing their relevance for deterrence theory. Their findings suggest that emotions give new meaning to deterrence by changing the nature of deterrence theory and by highlighting problems of practice. Emotions are not only the consequences of the defender's actions; they emerge through the challenger's interpretation of the situation and, once triggered, specific emotions affect cognitive

processes and action (or inaction) in far more sophisticated ways than has been assumed. Emotions are responsible for different kinds of biases that affect decision-making and judgments. They affect perceptions and, therefore, change how individuals perceive the world. Similarly, emotions and stress interact in dynamic ways. Anger, for example, is a negative emotion, similar to fear. However, while fear tends to make people more risk-averse and pessimistic, anger tends to make people feel risk-prone and optimistic. Furthermore, the behavioural influence of emotions varies from one context to another. Fear, for example, can motivate freezing, fleeing, or fighting. Happiness can motivate both the relaxation of efforts and their pursuit, depending on whether the emotion is experienced or merely anticipated in the future. Relating these insights to deterrence, they assert that emotions in different configurations shape decision making processes. Emotions are, in fact, essential for any decision, rational or not, as emotions make decision-makers care about the consequences of their actions, which in turn enables them to choose from competing objectives in any given context. However, the varied and sometimes contradictory influence of specific emotions makes deterrence without a better grasp of their impact an uncertain endeavour. Zilincik and Duyvesteyn therefore argue that emotions need to be taken seriously in future deterrence research because it will allow for a more nuanced understanding of the micro-level causal mechanisms that explain how deterrent threats are perceived and interpreted by targets of deterrence of different strategic cultures and different psychological makeups. They thus conclude that deterrence is "the continuation of emotional life with the admixture of violent means".

26.5.4 The Legal and Governance Side of Effective Deterrence

Finally, in Chap. 25, Paul Ducheine and Peter Pijpers address two related and relatively neglected issues in deterrence research: first, the legal framework applying to the use of deterrence instruments and, second, the intragovernmental arrangements which facilitate coordinated deterrence strategy. Effective deterrence by Western democracies, especially in the context of deterring hybrid threats, requires that robust capabilities and political resolve, which are clearly communicated, are complemented with a legal framework that is a prerequisite for deterrent power because it provides a variety of responses with a firm legal basis. The effective orchestration of actions during a crisis, as Ducheine and Pijpers argue, requires prior identification of the roles and responsibilities of different governmental departments (e.g., the ministry of foreign affairs, defence, finance) and a shared understanding of the potential effects associated with various potential instruments. Moreover, as they illustrate in a description of the legal prerequisites, such intergovernmental arrangements require clear demarcation of legal authority of each of the departments, and clarity of the appropriate international and national

legal frameworks. Deterrence against hybrid threats will be ineffective absent the clear allocation of responsibilities and legal frameworks because governments will simply be unable to carry out credible counteractions in time. Considering that the Cuban Missile Crisis is the landmark case study that highlighted the ways in which organisational interests and politics can influence deterrence strategy in practice, the relative lack of research into the governance of security these days seems strangely at odds with the demands of cross domain deterrence.

26.6 A Renaissance of Deterrence Theory and Practice

This volume took Patrick Morgan's 2012 analysis concerning the '*State of Deterrence in International Politics Today*' as a point of departure starting from the premise that recent geopolitical and technological developments may have moved deterrence research beyond Jeffrey Knopf's fourth wave. As has become evident from the state of the art overviews of recent insights contained in the twenty-six chapters in this volume, contemporary deterrence theorising and practice is experiencing a true *renaissance*. New theoretical and practical concepts on how to effectively deter different actors within and across domains are being put forward. In the context of considerable military-strategic change these insights are put to test, exhibiting a fruitful but also relatively swift accelerated interaction between theory and practice, akin to other historical periods that featured similar paces of military-strategic change such as for instance the late 1950s.

Contemporary deterrence researchers seem also to finally heed the oft-repeated calls in the deterrence literature, including those by Michael Mazarr in his stock-taking of contemporary deterrence research in this volume, to take context and actor perceptions seriously. As such, there is a growing body of literature that really does differentiate between specific context related challenges while paying ample attention to tailor made solutions.

It is also increasingly acknowledged that contemporary threats may well require strategic concepts that exceed the analytical scope of strict deterrence. In our digitally wired world instruments to inflict harm have proliferated to a greater number of (state and non-state) actors. Today's threat universe features novel opportunities to project power as well as new vulnerabilities to tools of power projection. The multiplicity of actors and the sometimes opaque nature of threats further complicates deterrence. This, in combination with new insights from psychological and decision-making research into how the human psyche operates, leads many authors to observe that deterrence should be complemented by other approaches that include compellence and suasion.

At times, there is conceptual creep with the meaning of deterrence stretched far beyond its limits. At other times, it is plainly pointed out that deterrence should constitute one strategy in a broader portfolio of strategies and that the neat theoretical categorisation of strategies is absent in practice where strategies can flow into each other. The demarcation of categories—when does deterrence stop of fail, when

does a symbolic demonstration of force to boost one's credibility start to resemble a brute force approach—is fluid. As Byman and Waxman noted in light of the experience of coercive diplomacy in the 1990s, and confirmed here by Mazarr, Jakobsen and Shamir, compelling a halt can be described as deterring to advance further.[5] Moreover, symbolic uses of force should not necessarily be considered a sign of deterrence failure, but as a method to bolster deterrence.

In addition to the elaboration of new concepts of deterrence, existing concepts are scrutinised more closely and refined accordingly. It is increasingly acknowledged that there are other non-Western approaches to deterrence, that in some respects may be fundamentally different. The contributions to our volume demonstrate that there is a real appreciation for the fact that strategic actors conceptualise deterrence differently, and, as Dmitry Adamsky amongst others relates, perhaps do not recognise deterrence as a distinct strategic concept with its own logic at all.

Taking stock of the body of insights that have emerged over the past, we submit that the considerable pace of military-strategic innovation of the past two decades has been accompanied by the blossoming of deterrence theory and practice building on the approaches to the study of deterrence that emerged during previous waves. It has shed its predominantly state based nuclear and conventional deterrence focus characterised by deductive reasoning encapsulated in game theoretic models (1st wave). It continues to feature plenty of case work and some, albeit far fewer, large-N approaches (2nd wave). It fruitfully incorporates insights from other academic disciplines (3rd wave) including psychology, communication and signalling theory, which are applied in the context of asymmetric deterrence against non-state actors (4th wave), but also against state actors, in and across new and old domains, and before, after but also during war. The current deterrence literature is less concerned with large-N hypothesis testing shedding some of its political science aspirations. Instead it relies on more general theorising based on the examination of the dynamics of particular cases in line with a disciplinary approach more prevalent in strategic studies. We therefore submit that a fifth wave of deterrence theory is in fact emerging even if it is in its early stages (see Table 26.1).

The nascent fifth wave is characterised by relatively short feedback loops between theory and practice in a reciprocal relationship that runs in both directions: theoretical ideas about how to deter are transferred and tried out in the real world at the same time as deterrent practices from a specific context and domain are studied, generalised, and theorised to also be useful in other contexts. In addition, there is ample attention to the practical prerequisites for favouring conditions of effective deterrence that go beyond more generic precepts and address more context specific elements. This is thus one particular area in which there are actual attempts to bridge that famous gap between theory and practice.

In addition to these strengths there are certainly also gaps, weaknesses and potential pitfalls with the fifth wave. First, similar to previous waves, today's

[5]Byman et al. 1999.

Table 26.1 Five Waves of Deterrence Theory (*Source* The authors)

Wave	Central question	Features
The 1st wave (1940s)	What is the effect of the atomic bomb on international stability?	Exploratory analysis; nuclear domain; great power centric; bipolar system; outside of war
The 2nd wave (1950s–1960s)	How to defend national security, attain limited political objectives but also control the horrors associated with nuclear war?	Deductive analysis; game theoretic; operational modelling; nuclear and conventional; great power centric; bipolar system; outside of war; status quo and stability oriented; mirror imaging and assumption of unitary actor rationality
The 3rd wave (1970s–1980s)	How to strike a proper balance between conventional and nuclear forces?	Empirical; psychological and decision-making perspectives; historical case studies; large-N approaches; nuclear and conventional domain; great power centric; bipolar system; outside of war
The 4th wave (1990s–2000s)	How to deter non-state actors and rogue leaders?	Empirical; multidisciplinary; psychology, terrorism studies; historical case studies; conflict domain; non-state actor centric; unipolar system; outside of war; application in peace keeping context; incorporated in wider debate on coercive diplomacy and the dynamic relationship between deterrence and compellence; deterrence failures; debate on the utility of precision weapons for conventional deterrence; military theorising on most effective coercive mechanisms in peace operations to deter and if necessary to compel
The 5th wave (2010–onwards)	What does the deterrence of composite challenges look like?	Partly exploratory, partly empirical; strategic studies; multidisciplinary; perceptions and context; insights from criminology, cognitive sciences and sanctions literature; all domain and cross domain, civ and mil; all actor centric; multi-polarity; inside and outside of war; non-status quo orientation; impact of novel technologies

deterrence literature continues to grapple with how to conceptualise and examine decision making by deterrence target actors. The literature typically fails to properly delineate the deterring and deterred agents—in the person of the individual political leader, in a larger group of decision makers surrounding him, or in a hypothetical unitary state construct. As a result, there are few attempts to subsequently

empirically study agents' decision making processes and the perceptions that inform them. In many cases the agent is largely left unspecified with authors paying lip service to the issue but implicitly relying on a hypothetical unitary state construct. In a similar vein, there are few in depth process tracing studies that scrutinise the decision making of both the deterrer and the deterred and establish whether deterrent signals were both sent and understood.[6] This is a key issue in determining the actual efficacy of deterrence because it is both unclear whether there is a deterrent relationship in the first place,[7] and, should there be one, there is no recorded empirical evidence to corroborate the causal mechanisms through which deterrence works. The empirical base underlying the purported efficacy of deterrence in particular domains is therefore thin.

Second, and related to this point, from a research perspective, the situation is certainly not helped along by the emerging fifth wave's tendency to conceptually expand understandings of deterrence to encompass a wider variety of functions, including compellence and suasion, because the use and utility of concepts that lack strict delineations of their scope are even harder to ascertain empirically. Meeting the full spectrum of today's strategic challenges certainly requires more than threats that rely on the denial of direct benefits or the prospect of unacceptable imposition of costs. Fundamental features of today's strategic environment which include a greater number of actors and effectors, larger attack surfaces and vulnerabilities, ambiguity and opaqueness, and complex relationships, necessitate comprehensive responses that utilise a broad portfolio of strategic ways and means. The empirical examination of the efficacy of these responses, however, benefits from conceptual clarity about what is being analysed in the first place.

Third, deterrence in newer domains including cyber, space but also where it concerns information or economic pressure campaigns, requires a solid grasp of the finer technical details of the possibilities as well as the limitations in order to be able to make sensible judgments about the feasibility of deterrent concepts that are being proposed. If the disconnect between the knowledge possessed by strategists and specific domain technological subject matter experts grows, deterrence theorising risks becoming not only hollow but also meaningless. Deterrence scholars therefore need to combine strategic expertise with in depth understanding of the intricacies of particular domains in order to continue to make meaningful contributions to the study of deterrence in the future.

Overall, from a philosophy of science perspective, the deterrence research programme in its current incarnation seems to be a blossoming field that continues to expand and grow. At the same time, it is—in Lakatosian terms—neither progressive nor degenerative,[8] but does risk to remain on the surface if it continues to ideate and explore but does not start specifying the deterrent mechanisms and examining how these work empirically. Even if it is a healthy sign that, in times of

[6]Like for instance Lebow and Stein did for the US-Soviet deterrent relationship, see Lebow 1995.

[7]See also Lebow and Stein 1990.

[8]Lakatos 1999.

considerable military-strategic change, deterrence research is evolving along with it both in terms of its focus and content, it will need to move beyond the ideation and exploration phase. That in turn will require a concerted and cross disciplinary effort by strategists, historians and political scientists, amongst others, to borrow from each other's research methods, and a willingness to harvest insights from other more distant but relevant disciplines such as cognitive sciences, communication studies, human decision making, science and technology etc.

In this volume, we have tried to facilitate cross-disciplinary pollination bringing together insights from a range of fields including strategic studies, intelligence studies, military operations, political science, psychology, biology, mathematics, science of technology, history and law. We submit that the field of deterrence research will benefit from more collaborations of this kind. This necessitates that larger structural hurdles are overcome. At present, there are no real incentives for scholars to engage in extended cross disciplinary research even if there are relevant and shining examples of how especially strategic studies and political science have advanced as result of it.[9] For researchers working in the latter two categories it is typically not in their professional interest to devote too much of their sparse professional time interviewing decision makers and doing archival research. Historians, in turn, are more likely to look at specific conflicts or relationships rather than trace more ephemeral strategic concepts such as deterrence. But reality is not destiny. This can be changed. Career incentive structures can be adjusted, and new funding schemes can be established to engage in real cross disciplinary collaboration. This in turn will also be very useful for practitioners and the defence and security community who will benefit from being able to draw on empirically proven concepts.

This then spells out the future research agenda for deterrence. Attempts to explore and adapt concepts to the changing character of challenges will continue be necessary in times of rapid military-strategic change, which is not expected to slow down any time soon. Alongside conceptual exploration and adaptation, it is necessary to start putting these adaptations on firmer empirical grounding in order to replace high level maxims such as *use unambiguous threats* and *signal consistently* with actual assessments of what works in particular contexts and domains based on multilevel scrutiny and in-depth case study. Such in depth case studies lend themselves to subsequent comparative case study work. This can perhaps be followed later on with larger-N work that seeks to unpack both the outcomes at the macro level, the dynamics at the microlevel, and the meso mechanisms that transfer these from the microlevel level to the macrolevel and back, in the recognition that the practice of deterrence as a strategy is partly an art, albeit one that can and should be studied scientifically. Whether this will happen will—as always—depend on intellectual curiosity, scholarly persistence and critical debate, but will be helped

[9]Think for instance how Marc Trachtenberg's analysis of audience costs in historical case studies marked a caesura in the political science and strategic studies research dedicated to abstract theorising about the role of audience costs. See Trachtenberg 2012.

along if the right academic and professional incentives structures are put in place. We look forward to the further maturation of the fifth wave of deterrence literature.

References

Byman DL, Waxman MC, Larson E (1999) Air Power as a Coercive Instrument. RAND Corporation, Santa Monica

Echevarria A (2017) Military Strategy: A Very Short Introduction. Oxford University Press, Oxford

George A (1967) The "'Operational Code"': A Neglected Approach to the Study of Political Leaders and Decision-Making. RAND Corporation, Santa Monica

Gray CS (2016) The Strategy Bridge: Theory for Practice. Oxford University Press, Oxford

Lakatos I (1999) The Methodology of Scientific Research Programmes (Worral J, Currie G (eds)). Cambridge University Press, Cambridge

Lebow RN (1995) Deterrence and the Cold War. Political Science Quarterly 110:157–81

Lebow RN, Stein JG (1990) Deterrence: The Elusive Dependent Variable. World Politics 42:336–69

Mazarr M et al (2018) What Deters and Why: Exploring Requirements for Effective Deterrence of Interstate Aggression. RAND Corporation, Santa Monica

Murray W, Knox M, Bernstein A (1994) The Making of Strategy: Rulers, States, and War. Cambridge University Press, Cambridge

Trachtenberg M (2012) Audience Costs: An Historical Analysis. Security Studies 21:3–42

Von Clausewitz C (1989) On War (Howard M, Paret P (eds)). Princeton University Press, Princeton

Dr. Tim Sweijs is the Director of Research at The Hague Centre for Strategic Studies and a Research Fellow at the Netherlands Defence Academy. He is the initiator, creator and author of numerous studies, methodologies, and tools for horizon scanning, early warning, conflict analysis, national security risk assessment, and strategy and capability development. He serves as an Adviser Technology, Conflict and National Interest to the UK Government's Stabilisation Unit. Tim holds degrees in War Studies (Ph.D., MA), International Relations (M.Sc.) and Philosophy (BA) from King's College, London and the University of Amsterdam.

Air Commodore Prof. Dr. Frans Osinga is Professor of Military Operational Art and Sciences, Chair of the War Studies Department at the Netherlands Defence Academy (Faculty of Military Sciences). He is also the Special in War Studies at Leiden University. A graduate of the Royal Military Academy, the Advanced Staff Course of the Netherlands Defence College and a former F-16 pilot, he obtained his PhD at Leiden University in 2005 following a tour as the MoD Senior Research Fellow at the Clingendael Institute. He is the author of more than seventy publications.