Rhetoric over reality? Assessing the success of deterrence in cyberspace: Israeli and US cybersecurity approaches between 2008 and 2018

Melanie Jane Broder

Supervisors:

Professor Roger Bradbury (Emeritus)

Associate Professor Matthew Sussex

Associate Professor Sarah Heathcote

Associate Professor Jon R. Lindsay

Submitted in fulfilment of the requirements for the degree of
Doctor of Philosophy

Crawford School of Public Policy
Australian National University
2021

Abstract

In April 2007 Estonia suffered a series of cyber-attacks in which hundreds of thousands of computers were used to cripple dozens of government and corporate sites. The attacks appeared to originate from Russia, although no country claimed responsibility. Regardless of the origin or reasons for the attack the consequences were far-reaching. States with advanced cyber postures began rapidly adopting measures to increase their cybersecurity to avoid similar attacks on their national interests, including creating specific cyber security policies and strategies. By 2008 at least twelve states had adopted deterrence theory into their strategies for cyberspace despite a lack of evidence of its efficacy in the cyber domain. Yet by 2018 several states had begun moving away from deterrence.

With a focus on the approaches of two states leading developments in cyber strategy – the United States of America and Israel – this thesis considers the extent to which states employing deterrence as a strategy for cyberspace considered it successful between 2008 and 2018. It explores the context in which each case defined and adopted deterrence in comparison to the requirements for classic deterrence, and considers how this context influenced perceptions of success or failure of deterrence for cyberspace. It finds that while Israel's approach arguably meets the classic requirements of deterrence and considers its approach successful, the Israeli definition of success as cyclical and requiring 'refreshing' through the regular use of violent force is not necessarily an approach other states can, or indeed should, adopt. Neither is the US approach a potential model for other states, although the reasons differ: the US has not come close to meeting the requirements of classic deterrence and its pivot in 2018 away from deterrence was based on an assessment that the theory had failed rather than realisation it had never been fully implemented.

Cyberspace is a rapidly evolving domain and states are seeking theory to supplement their security approaches. This research shows the variation between states of conceptions of success influences the design, implementation and expectations of deterrence practices. And, most importantly, despite a decade of efforts to create deterrence in cyberspace neither case has demonstrated the ability to deter increasing numbers of cyber-attacks from progressively more sophisticated threat actors. Hence deterrence is at best a supplement to existing strategies focused on resilience. At worst, attempts to create deterrence may lead to escalation or unintended conflict.

Contents

List of Tables

List of Abbreviations

CDI	Cyber Deterrence Initiative
CERT	Computer Emergency Response Team
C3	command, control and communications (systems)
DoD	Department of Defense (US)
DSDE	Director of Security of the Defense Establishment
EMP	electromagnetic pulse
FBI	Federal Bureau of Investigation (US)
GDP	Gross Domestic Product
ICT	information communications technology
IDF	Israeli Defense Force
INCD	Israel National Cyber Directorate
ISIS	Islamic State
ISR	intelligence, surveillance and reconnaissance (systems)
NSA	National Security Agency
OECD	Organisation for Economic Cooperation and Development
PE	persistent engagement
PLA	People’s Liberation Army
PM	Prime Minister
UK	United Kingdom
US	United States

Statement of Original Authorship

The work contained in this thesis has not been previously submitted to meet requirements for an award at this or any other higher education institution. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made.

Signature:

Date: 17 September 2021

Acknowledgements

It took a village.

This thesis evolved with assistance from many people. The untiring academic support of Professor Roger Bradbury (Emeritus) and Associate Professor Matthew Sussex was greatly appreciated, even when pointing out my dreadfully policy-oriented writing habits. I also appreciated valuable early input on content, structure and planning from Associate Professor Sarah Heathcote and Associate Professor Jon R. Lindsay, and additional academic and emotional support from Dr Jennifer Hunt.

This research was funded by a scholarship from the Sir Roland Wilson Foundation as part of a partnership between the Australian Public Service and the Australian National University. It was an extraordinary privilege to research under the auspices of the Foundation, which provided invaluable support in navigating the complexities of academia and managing fieldwork as well as career planning and developing avenues to improve research impact. I am both professionally and personally indebted.

I am also extremely grateful to the cybersecurity professionals from the United States of America and the State of Israel who took the time to participate in this research. While examining policy documents and the relevant academic literature produced useful findings, it was the first-hand views from interview participants that provided detailed insights into the reasoning behind such policies as well as the relevant context for how deterrence was developed, implemented and judged.

Throughout this research I received extraordinary support from many areas of the Australian National University, including the amazing Crawford School of Public Policy's Higher Degree Research team of Dr Megan Poore and Tracy McRae. I would also like to thank the librarians and COVID-19 cleaners at the Chifley and Menzies Libraries for their efforts in providing research support and safe places to work.

This thesis was professionally edited by Hilary Bek; I am extremely grateful for her considerate services.

Writing a thesis as a single mother was always going to be a challenge; managing writing up findings while home-schooling my son amidst a global pandemic proved close to impossible. The completion of this research was only possible due to extraordinary support from my family, friends, colleagues and mentors. An overwhelming number of people (and one very special cat) cheered for me from the first research idea through to tears over footnotes. I will never have the right words to thank everyone who sent notes of encouragement; cooked meals; insisted I take breaks; delivered chocolate and told me they believed in me. Special thanks to: Jenna Gibbons; Gemma Gordon; Alison Greenhill; Isaac Hayne, Marcella Hawkes; Madeleine Nugent, Shannon O'Donnell; Nell Shipley; Candice Strack; Lauren Williams; Balanced Yoga: TT1 and the Ladies of the Lake.

This research is dedicated to my son, Henry Joseph Rettig.

I love you; never stop asking questions.

Introduction

The puzzle

Why do states include deterrence theory as part of their efforts to secure interests in cyberspace, despite the lack of evidence regarding its efficacy or appropriateness, and what implications does this have for security practices? Deterrence has underpinned the cybersecurity approaches of a number of influential states for over a decade[1], but this has been done with little clear confirmation it would work in cyberspace. How effective do these states consider deterrence, and should they be used as models for others to emulate? In this thesis I argue states have adopted deterrence approaches that reflect their unique historical experiences and approach cybersecurity through the lens of established strategic practice rather than responding to the product of a new strategic environment. This lens of established practice results in very different policies despite agreement on the core principles of theory. This potentially creates significant instability and risk in the strategic environment. Certainly, the potential for cyber-attacks to endanger national security has become a familiar and prominent concern in recent years. [2] This instability is problematic because cyberspace presents a broad array of challenges and opportunities for states, and securing this space – the practice of developing cybersecurity, defined by Martin Libicki as the state of systems being secure – is a key priority for many actors.[3] But cybersecurity is a poorly understood concept which is often conflated with other areas of cyber concern such as privacy, information sharing, intelligence gathering, and surveillance. [4] At the same time, issues of national security are notoriously complex.[5] Thus, much as they did during the Industrial Revolution, states must develop and implement policies – now in the cyber age – for a new environment in a relatively short timeframe, without experience of the risks or benefits of their policy decisions, or full understanding of the space in which those decisions are made. As well as a lack of practical experience, there also does not yet exist a substantial body of academic research on how to best create cybersecurity and manage related strategy;

[1] This research considers two cases in detail; however as the methodology will show, at least nine states have had deterrence as a central plank of their public national cybersecurity policies since 2008. These states include but are not limited to the United States of America, Commonwealth of Australia, Commonwealth of New Zealand, United Kingdom, State of Israel, Republic of Korea, Japan, Germany and Finland.

[2] For a consideration of the vulnerabilities and conflict in cyberspace, see Eric Sterner, 2011, 'Retaliatory Deterrence in Cyberspace', *Strategic Studies Quarterly*, Spring 2011, pp.62-65. Leuprecht et al. provide a detailed overview of the potential threats posed by offensive cyber weapons in Christian Leuprecht, Joseph Szeman and David B. Skillicorn, 2019, 'The Damoclean sword of offensive cyber: Policy uncertainty and collective insecurity', *Contemporary Security Policy*, 40:3, 382-407. See also Uri Tor, 2017, 'Cumulative Deterrence as a New Paradigm for Cyber Deterrence, *Journal of Strategic Studies*, 40:1-2, 92 for a state's specific view of the potential threat posed by cyber-attacks.

[3] Martin C. Libicki, 'Expectations of Cyber Deterrence', *Strategic Studies Quarterly : SSQ* 12, no. 4 (2018): 44–57. There are many competing definitions of cybersecurity; see also Lucas Kello, *The Virtual Weapon and International Order*, Yale University Press, New Haven, 2017, p. 46-47.

[4] Eric A Fischer, 12 August 2012, Cybersecurity Issues and Challenges: In Brief, Congressional Research Service, from https://fas.org/sgp/crs/misc/R43831.pdf

[5] Asher Arian, 1995, *Security Threatened: Surveying Israeli Opinion on Peace and War,* New York: Cambridge University Press, p.91

indeed, the existing literature is divided over the scale of the risks and the best ways to establish and manage cybersecurity.[6]

At the same time, the threats states face in cyberspace are seemingly vast and deeply interconnected, manifesting in ways that are entirely new to the Westphalian order, such as the increasing use of non-state actors as proxies.[7] Creating effective national security policy is thus a critical avenue for states to protect their interests in cyberspace because if states seek to adopt policies which prove ineffective or unintentionally provocative, they may have to pay a high price for failure.[8] This thesis takes up the challenge of assessing how states are protecting their interests in cyberspace through policy, and whether the adoption of existing strategic approaches such as deterrence are increasing, or risking, cybersecurity.

Deterrence, not widely examined since the Cold War, rose in popularity from the early 2000s as a potential avenue for states to help secure their interests in cyberspace. But there is not yet a body of evidence to suggest whether this adoption is likely to achieve the desired results and the implications of its use in policy and strategy more broadly are as yet unclear. Hence research into securing cyberspace and considering how this fits within broader strategic research is in its infancy.[9] Such research is complicated by the speed with which cyberspace has evolved: the rapidity of change in both technological and human terms has resulted in key authors not agreeing on the most basic cyber terminology.[10] Further, the shape of the threat is likely to influence international relations more broadly. Here for instance we can contrast Eric Gartzke's argument that cyber war will not fundamentally transform either war or world affairs with

[6] Scholars are deeply divided over the applicability and usefulness of deterrence theory to states' cybersecurity policies. For arguments that the threat is exaggerated and deterrence will not be fundamentally changed by cyberspace see Colin S. Gray, 2013, 'Making strategic sense of cyber power: Why the sky is not falling' *Strategic Studies Institute,* Carlisle, PA; and Jon R. Lindsay, 2013, 'Stuxnet and the Limits of Cyber Warfare', *Security Studies,* 22, 365-40. For considerations of the problems of applying deterrence theory to cyberspace see Alexander Klimburg, 2020, 'Mixed Signals: A Flawed Approach to Cyber Deterrence', *Survival*, 62:1, 107-130; see also Alex Wilner, 2020, 'US cyber deterrence: Practice guiding theory', *Journal of Strategic Studies*, 43:2, 245-280; Will Goodman, 2010, 'Cyber Deterrence: Tougher in Theory than in Practice?' *Strategic Studies Quarterly*, Fall 2010, 102-135. For arguments that deterrence may have a role in improving cybersecurity see Richard A. Clarke and Robert K. Knake, 2010, *Cyber War: The Next Threat to National Security and What To Do About It,* HarperCollins; Martin C. Libicki, 2009, *Cyberdeterrence and Cyberwar,* RAND Project Air Force; Patrick Cirenza, 2015, *An Evaluation of the Analogy Between Nuclear and Cyber Deterrence*, Stanford University; Liam Nevill and Zoe Hawkins, 2016, 'Deterrence in cyberspace: different domain, different rules', *Australian Strategic Policy Institute: Special Report.*

[7] Chris C. Demchak and Peter Dombrowski, 2011, 'Rise of a Cybered Westphalian Age', *Strategic Studies Quarterly,* 5:1, 32

[8] In 2003 senior US cyber adviser Richard A. Clark testified to a US Congressional Committee that that threat posed by cyber-attacks was serious and the consequences of not addressing such threats could be dire. See Richard A. Clark, 8 April 2003, Testimony to the Committee of Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, p.1.

[9] Noluxolo Gcaza et al., 2017, 'A General Morphological Analysis: Delineating a Cyber-Security Culture', *Information and Computer Security,* 25:3, 259-60; see also Tim Stevens, 2012, 'A Cyberwar of Ideas? Deterrence and Norms in Cyberspace', *Contemporary Security Policy*, 33:1, 148-170

[10] Consider the inherently contradictory definitions of cyberwar, cyber terrorism and cyberespionage all listed as subsets of cyber-attack by Riordan in Shaun Riordan, 2019, 'Cyberdiplomacy: Managing Security and Governance Online', 2; or the inclusion by Herb Lin of information warfare into the spectrum of cyber warfare operations in Herb Lin, 2019, 'On Cyber-Enabled Information/Influence Warfare and Manipulation', forthcoming, Oxford Handbook of Cybersecurity.

Jason Healey's view of cyber-attacks as a primary means for nations to project their power.[11] This research thus aims to contribute to scholarship on cybersecurity by exploring why some states have turned to deterrence theory as a potential avenue to protect their interests in cyberspace, including considering how states define and construct deterrence for cyberspace, and exploring the perceived efficacy of this decision. It also offers a consideration of the potential risks and benefits for states considering applying deterrence theory to policies relating to cyberspace and cybersecurity.

Such research is necessary because most states with published cybersecurity strategies mention deterrence in some form. The premise for this seems simple enough – deterrence has previously been judged a success in many cases, such as by preventing great powers from descending into nuclear conflict, and perhaps it could help secure cyberspace as well. Deterrence however is notoriously difficult to measure[12], and the question of whether deterrence is successful in cyberspace is common – but lacking a definitive answer.[13] Identifying successful deterrence relies on a deep understanding of an adversary's intent, plans and decision-making processes, something that has proved almost impossible to establish throughout history.[14] However, it is possible to gather useful inferences for theory through an examination of state behaviours. This research therefore seeks to make a unique contribution by moving beyond the theoretical debates in the literature and considering states' policies and practices.

To accomplish this, the thesis adopts a generalised approach to explore the intersection of deterrence theory with states' national security policies.[15] Strategists agree that classic deterrence is an attempt, usually by a state, to persuade an adversary not to undertake an attack by altering their cost-benefit calculation.[16] Chapter 1 considers the three broadly agreed requirements for successfully creating such a change in behaviour: states must have the capability to enact a threat; credibility that the threat will be enacted; and the threat must be effectively communicated.[17] The chapter explores the substantial and

[11] Eric Gartzke, 2013, The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth, *International Security,* 38:2, 65; see also J Healey, the Age of Cyber Warfare

[12] Richard Ned Lebow, Janice Stein, and Canadian Institute for International Peace and Security, 1990, 'When Does Deterrence Succeed and How Do We Know?', vol. no. 8., Ottawa: The Canadian Institute for International Peace and Security

[13] Mariarosaria Taddeo, 2018, 'The Limits of Deterrence Theory in Cyberspace', *Philosophy & Technology* 31:3, 340

[14] See Patrick M. Morgan's argument the lack of knowledge the US had regarding Soviet intentions during the Cold War in Morgan, 'Deterrence Now', p.31

[15] Gaddis articulated the gap between the study of history and the construction of theory in *On Grand Strategy*, and argued that both were needed if the ends are to be aligned with the means. See John Lewis Gaddis, *On Grand Strategy*, (New York: Penguin Press, 2018), 23

[16] Thomas C. Schelling, 2008, *Arms and Influence*, Yale University Press; Alexander L. George and Richard Smoke, 1974, *Deterrence in American Foreign Policy: Theory and Practice*, New York: Columbia University Press; see also Lawrence Freedman, 2004, *Deterrence*, Malden, MA: Polity Press; Patrick M. Morgan, 2003, *Deterrence Now*, 89; Bernard Brodie, 1946, 'The Absolute Weapon: Atomic Power and World Order', Harcourt

[17] This principle is articulated by Freedman, see also Morgan 'Deterrence Now' and Jim Chen, 2018, 'Does Conventional Deterrence Work in the Cyber Domain?', in *European Conference on Cyber Warfare and Security,* Reading: Academic Conferences International Limited, 106-111; for a useful framing of credibility, see David J. Lonsdale, 2018, 'Warfighting for Cyber Deterrence: A Strategic and Moral Imperative', *Philosophy & Technology,* 31:3, 410-412, https://doi.org/10.1007/s13347-017-0252-8

See Martin Libicki's testimony to the House Committee on Armed Services Hearing on Cyber Warfare. Libicki included attribution as a separate fourth requirement. 'House Committee on Armed Services Hearing on Cyber well-tested body of knowledge on these requirements for deterrence to work in practice.[18] Of course, the examination of deterrence theory and its potential applicability to cyberspace is not new, nor is it restricted to the field of international relations.[19] Indeed, the question of whether deterrence can, or indeed should, be applied to cyberspace has been investigated by scholars since the earliest days of the internet.[20] And while considering the efficacy of deterrence is not unique – among scholars and laypeople during the Cold War, for example, the discussion and study of deterrence more broadly in Israel acquired the 'popularity of a national sport'[21] – I argue there is a need for research which seeks to explore deterrence efficacy in a systemic, cumulative manner.[22] In particular there is a substantial dearth of studies that consider both the theory as well as the practical implications of adopting that theory through policy practices.

Despite the basic intent and requirements of deterrence being agreed however, this research identifies three areas where the literature is contested on applicability for cyberspace. These are considered in detail in Chapter 1. The first concerns defining the problem states are facing through cyberspace for which deterrence might be an answer. This is a challenging endeavour given that researchers and strategists have not yet reached consensus over the requirement for deterrence in cyberspace. There is disagreement over the nature and seriousness of the threat[23]; the question of whether to treat cyberspace as a domain of warfare;[24] and the complex question of identifying attackers, also known as attribution.[25] Secondly, states vary over how to think about deterrence in cyberspace. This includes how deterrence as a concept should

Warfare', *Political Transcript Wire*, 3 March 2017, http://www.proquest.com/docview/1874238660/abstract/D72E2687EE404A2DPQ/1

[18] For an overview of the aim of deterrence as being to inform a challenger's cost-benefit calculus, see Lawrence Freedman, 2004, 'Deterrence', Cambridge Polity Press, p.26. This issue is explored in further detail in Chapter 1.

[19] Alex S. Wilner, 2020, 'US Cyber Deterrence: Practice Guiding Theory', *Journal of Strategic Studies,* 43:2, 249, https://doi.org/10.1080/01402390.2018.1563779

[20] Chris Painter, 2018, 'Deterrence in Cyberspace', Australian Strategic Policy Institute, Policy Brief Report No. 4/2018, 16; see also Jun Osawa, 2017, 'The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?', *Asia-Pacific Review,* 24:2, 113-31, https://doi.org/10.1080/13439006.2017.1406703; see also Tim Stevens, 2012, 'A Cyberwar of Ideas? Deterrence and Norms in Cyberspace', *Contemporary Security Policy*, 33:1

[21] Jonathan Shimshoni, 1988, *Israel and Conventional Deterrence: Border Warfare from 1953 to 1970* Cornell University Press, Ithaca and London, p.1

[22] Alexander L. George and Andrew Bennett, 2005, *Case Studies and Theory Development in the Social Sciences*, Cambridge, Mass: MIT Press, p.67

[23] Libicki, 2011, 'Expectations of Cyber Deterrence'; see also Eric Sterner, 2011, 'Retaliatory Deterrence in Cyberspace', *Strategic Studies Quarterly,* 5:1: 62-80.

[24] Liam Neville and Zoe Hawkins, 27 July 2016, 'Deterrence in Cyberspace: Different Domain, Different Rules', *Australian Strategic Policy Institute: The Strategist*; Jim Chen, 2018, 'Does Conventional Deterrence Work in the Cyber Domain?', in *European Conference on Cyber Warfare and Security,* Reading: Academic Conferences International Limited, 106

[25] David D. Clark and Susan Landau, 2010, 'Untangling Attribution', in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy,* National Research Council, p.400; Jon R. Lindsay, 2015, 'Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack', *Journal of Cybersecurity,* 1:1, 53-67

be defined[26]; how success should be conceptualised[27]; and whether deterrence should be considered as a stand-alone 'cyber deterrence' practice, or whether it should be considered as part of a state's broader deterrence strategy.[28] Lastly, while the most basic theoretical requirements of capability, credibility and communication are agreed in the literature, the question of how best to deliver these in any domain is still contested.[29] Both the literature and state practices differ over issues such as the role of the military in cyberspace, the need and potential risks associated with attempting to gain or maintain superiority, and the role and definitions of offensive actions in creating deterrence. Specifically in this thesis I explore the different approaches two states – Israel and the United States – have taken to apply deterrence theory to cyberspace, with the aim of generating findings into why their approaches differed, and the potential impact they had on perceptions of efficacy. The research considers that if states' previous experiences of deterrence theory and practices influenced the adoption and construction of deterrence in cyberspace then it may be possible to predict the shape deterrence took in policy approaches. By exploring not only states' cybersecurity policies, but also the context for their development and implementation, the thesis also seeks to identify potentially generalisable lessons.

Given the rapid adoption by several states of deterrence approaches since 2008, there is sufficient practice-based evidence to assess whether states that had adopted deterrence consider it had improved their cybersecurity. In Chapter 2, I offer a methodology to explore two states' public policy approaches to deterrence theory as part of public cybersecurity strategies between 2008 and 2018.[30] By considering their approaches over this period, I examine a decade of data beginning from the earliest days of cybersecurity strategies. While evaluating the efficacy of deterrence is notoriously fraught[31], I argue that finding a way to analyse the efficacy of such deterrence strategies in cyberspace is both possible and necessary given the

[26] Consider Richard A Clarke and Robert K. Knake, 2010, *Cyber War: The Next Threat to National Security and What To Do About It,* New York: HarperCollins, p.62 where deterrence is cast as an operational response, which contrasts with Jeffery R. Cooper 'A Framework for Cyber Deterrence' in Derek S. Reveron, 2012, *Cyberspace and National Security,* Washington DC: Georgetown University Press, pp.108-109 which argues for a rethink of deterrence to account for new capabilities for influencing behaviours.

[27] Martin Libicki, 2016, *Cyberspace in Peace and War,* Maryland: Naval Institute Press, p.20; see also Fred Kaplan, 2016, *Dark Territory: The Secret History of Cyber War,* New York: Simon and Schuster, p.283

[28] Amir Lupovici, 2016, argues for deterrence as a higher-level concept in *The Power of Deterrence: Emotions, Identity and American and Israeli Wars of Resolve*, Cambridge: Cambridge University Press ; whereas Martin Libicki uses the term 'cyberdeterrence' to explain activities undertaken to deter in cyberspace. See Libicki, 2016, *Cyberspace in Peace and War,* Maryland: Naval Institute Press, pp.222-223

[29] Michael P. Fischerkeller and Richard J. Harknett, 2017, 'Deterrence Is Not a Credible Strategy for Cyberspace', *Orbis,* 61:3, 381-93; Jesse C. Johnson, Brett Ashley Leeds, and Ahra Wu, 2015, 'Capability, Credibility, and Extended General Deterrence', *International Interactions,* 41:2, 309-36; Gcaza et al., 'A General Morphological Analysis: Delineating a Cyber-Security Culture'

[30] Although states may also have classified strategies or views which are not publicly available, this research did not seek to include any classified material. Doing so would not only have breached secrecy requirements; such classified approaches do not substantially build understanding of deterrence, as such policies are only effective if they are communicated. Although some communication between states may take place behind closed doors, publicly available policies provide important insights into how states not only communicate policy, but also how they wish that policy to be perceived.

[31] George and Smoke, *Deterrence in American Foreign Policy: Theory and Practice.*

increasing number of states relying on deterrence strategies to secure their interests.[32] While some strategists contend that as there is currently no cyber weapon of sufficient capability to force a doctrine of no first use in the way nuclear weapons did, the threat of overwhelming devastation from a cyber threat simply does not yet exist.[33] Without that threat, the ability to deter is absent. But deterrence was not invented with nuclear weapons, and even during the Cold War deterrence was never a strategy in isolation, even for the US. Rather it was only a part of a broader set of measures and plans.[34] At the height of the Cold War, when nuclear deterrence was perceived as successful in creating a relatively stable balance of power, the presence of nuclear weapons alone was not enough to build and maintain a deterrence posture. Further, nuclear weapons are overt, cause catastrophic damage, and are traceable. In contrast, cyber weapons are covert, are often dual use, have concealable origins, and (so far) only cause limited and usually temporary damage.[35] If researchers who compare cyber to nuclear deterrence are correct in that these differences mean deterrence has no role in cyber strategy, then those states choosing to adopt and implement deterrence into cybersecurity polices are potentially opening themselves to serious risk. But this framing of deterrence around a particular weapon is neither helpful nor accurate enough for policymakers. Deterrence should not be characterised by the means by which states attempt to influence their adversaries.[36] The beginning of the shift towards a multi-polar world after 1990 also introduced further complexity.[37] Thus, just as our understanding of nuclear deterrence has evolved, so too must our understanding of the potential role deterrence may play in cyberspace.

Constructing a principles- and practice-based methodology

This research seeks to move beyond abstract theoretical arguments over whether the way deterrence was adopted for the Cold War provides an appropriate methodology for cyberspace. While such arguments are interesting, they do not help us understand why states are pursuing deterrence despite obvious differences in operational environments. Instead, I start from the premise that as a number of states have already adopted deterrence in cyberspace, it is more useful to assess state practices against a framework of the most basic agreed requirements for deterrence theory: capability, credibility, and communication.[38] Hence in the thesis I explore states' approaches to deterrence in cyberspace by considering how their

[32] Uri Tor 2017, 'Cumulative Deterrence as a New Paradigm for Cyber Deterrence, *Journal of Strategic Studies*, 40: 1-2, 92

[33] Eric Gartzke, 2013, 'The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth', *International Security,* 38:2, 41-73

[34] Raymond P. Ojserkis, 2003, *Beginnings of the Cold War Arms Race: The Truman Administration and the U.S. Arms Build-Up*, Westport, Conn: Praeger, 108

[35] Stephen J. Cimbala, 'Nuclear Deterrence and Cyber Warfare: Coexistence or Competition?', *Defense & Security Analysis* 33, no. 3 (2017): 193–208

[36] Keith B. Payne, 2001, *The Fallacies of Cold War Deterrence and a New Direction*, The University Press of Kentucky, pp.30-31; see also James J. Tritten and Paul N. Stockton, 1992. *Reconstituting America's Defense: The New U.S. National Security Strategy,* New York: Praeger, pp.4-5; John J. Mearsheimer, 1983, *Conventional Deterrence*, Ithaca: Cornell University Press

[37] James John Tritten and Paul Stockton, 1992, *Reconstituting America's Defense: The New U.S. National Security Strategy*, New York: Praeger, p.153

[38] Patrick M. Morgan, 1977, *Deterrence: A Conceptual Analysis*, Beverly Hills, Calif: Sage; Morgan, *Deterrence Now*; Freedman, *Deterrence*; George and Smoke, *Deterrence in American Foreign Policy: Theory and Practice*

public policies aligned against this classic deterrence framework. I ask whether each state had a capability; credibly threatened its use; and communicated its intent to do so. By exploring two cases that had adopted deterrence theory against this framework I develop findings in relation to the different approaches taken and examine how they also helped reflect debates in the literature. The case studies and subsequent cross-case analysis demonstrate that while scholars and states may be in agreement over the core requirements for deterrence, the fundamentally different experiences of states with deterrence theory influences how they define deterrence in cyberspace, and whether or not it is perceived as being successful. By conducting a structured, focused comparison through a theoretical framework comprised of these basic deterrence requirements, this approach remains centred on assessing states' practices against the core theory and answering the question: do the declared deterrence approaches and activities of states actually met a definition of the most basic deterrence requirements? Although a seemingly basic description of deterrence theory, by reviewing and analysing how states adapt the three measures of capability, credibility and communication into strategies, we can understand their relative importance to each states' conception of deterrence success and assess whether the approaches states had met this test of deterrence practice.

The analysis is structured in that it asks the same set of general questions of both cases to standardise data collection regarding those deterrence requirements, and focused in that it deals only with the deterrence strategies and approaches of the cases.[39] The research begins by considering how each case defined the problem posed by cyberspace to which deterrence had been judged the solution. By considering how the states under review have defined the threats to their interests in cyberspace and the seriousness of that perceived threat, as well as whether it considered cyberspace should be considered a domain of warfare – and if so, what were appropriate responses – I develop the context for each case's deterrence approach. I then consider how each case defined deterrence, including how they framed success and how such approaches accounted for broader conventional or nuclear deterrence. This step is necessary to ensure that perceptions of success or failure were based on each case's own definitions of success, before considering broader perceptions of success or failure. Next, the thesis explores how the two states in question delivered deterrence in practice by examining their policy measures and behaviours labelled as being part of each case's deterrence approach. Each case is considered against its own definitions in individual chapters, before being considered against broad indicators of each measure in a penultimate critical analysis chapter.

As the structured focused comparison approach is specifically designed to discourage decision-makers from relying on a single historical analogy[40], the above approach offers the ability to not only answer the question of how effective states considered their specific approaches to be, but also to illuminate the

[39] Alexander L. George and Andrew Bennett, *Case Studies and Theory Development in the Social Sciences*, (Cambridge, Mass: MIT Press, 2005), 66

[40] Alexander L. George and Andrew Bennett, 2005, *Case Studies and Theory Development in the Social Sciences*, Cambridge, Mass: MIT Press, p.66

implications of these assessments for cybersecurity strategies, and our understanding of deterrence more broadly. Further, it helps ensure the cases are being assessed against deterrence theory, rather than in comparison with the narrower subset of nuclear deterrence. Any evaluation of the role of deterrence in cybersecurity policies is subjective in that it depends entirely on the perspectives and definitions of each state. However, the case study methodology allows for contextualisation of each case to ensure states are evaluated against their own definitions of deterrence and success. To assess whether states had each requirement, and how effective they were judged to be, the thesis presents evidence through a diverse dataset comprising the secondary literature, policy documents and expert interviews. These are then examined against a framework that demonstrates not only how states are assessed through broad literature and stated public policy, but that considers how effective each state's experts judged their efforts. By examining not only explicit government policy but also the expert opinion of policymakers, academics, commentators and industry representatives who had input into (or experience of) the implementation and development of cyber deterrence policies between 2008 and 2018, this research presents a cohesive picture of the policies intended effect expert views on the policy's' intended effect, and the capacity to assess whether this effect was achieved. Epistemologically, this research follows a positivist model that assumes we can make objective claims about the behaviour of states. Empirical theory (the idea we can explain processes and identify causal behaviours in the real world of relations between states)[41] is of particular use in evaluating strategic theory – which is itself theory developed to explain the practical behaviours of states.

Analysis and findings

To answer the puzzle of why states chose to pursue deterrence as an approach to secure their interests in cyberspace, I analyse two cases with public commitments to deterrence as part of their cybersecurity: the United States of America (US), and Israel. This was a targeted case selection from a number of other states with a public deterrence policy approach for cyberspace. I argue these cases are particularly instructive for an examination of deterrence because both are global leaders in the technology and behaviours of cyberspace, setting norms and trends for the rest of the world through their policies and actions. Both face active and ongoing cyber threats from a range of both state and non-state actors. And both have been active and vocal about their own – and their adversaries' – behaviours in cyberspace. However, this is not a 'most-similar' case study design. Rather, these cases represent a 'most-different' approach in that their geo-political circumstances, threats faced from states and state-based actors, and views on the appropriate use of force have been markedly different. Yet despite these differences the evidence presented in the following chapters indicates that states' experiences of deterrence shape their application and expectations of deterrence as a strategy for cyberspace, with the result that neither case study presents as an example of a deterrence approach that can, or indeed should, be considered an example by other states.

[41] Richard Smoke and Alexander George, 1973, 'Theory for Policy in International Affairs', *Policy Sciences,* 4:4, 387

In the first case study I argue that since Israel is a global leader in cyber technology with a booming entrepreneurial sector, extensive cybersecurity governance and a considered approach to deterrence as part of its broad security framework, I expected to find its deterrence approach to be considered an overwhelming success. Yet while this is largely the case, and its approach met the basic requirements for deterrence of having a capability, credibly threatening its use, and communicating its deterrent intent, Israel's view that deterrence has been successful is problematic. Its definition of deterrence success as cumulative and its reliance on overwhelming force to implement its policies seem to be creating an environment of rapidly escalating cyber-attacks by adversaries, rather than deterrence 'success'.

In the second case – on the US – I initially expected to find extensive deterrence policies and a strong perception of success amongst experts. The US is a leader in the field of security, its choices and actions in cyberspace have consequences for the rest of the world. Given it is widely acknowledged that its deterrence posture during the Cold War was considered successful, I expected to find extensive and well-considered deterrence policies for cyberspace, and a similar perception that such policies were successful. Yet the analysis presented here instead finds that the US has judged its deterrence efforts in cyberspace a failure, resulting in a move to a more active approach of 'pre-emptive force and persistent engagement'. This is because US reliance on superior power and exceptionalism created an incomplete deterrence approach for cyberspace, which from the outset emphasised capability without building a credible threat of response to attacks or communicating deterrent intentions effectively through policy. Therefore the US decision to move away from deterrence theory may be based on a misapplication, rather than a failure, of theory. But regardless of this, the result of the incomplete US application of deterrence theory seems to be creating risk through rapidly escalating cyber behaviour.

By considering the cases against both the analytical framework and each other in a comparative analysis in Chapter 5, I demonstrate that while both the US and Israel had deterrence as declared strategies for cyberspace, their approaches varied in completeness and implementation. The US approach was not consistent with the analytical framework, lacking credibility and to a lesser extent, communication. The Israeli approach to cyber deterrence conforms neatly to the expectations of classical deterrence theory, however its definition of deterrence success was markedly different from Western definitions. Moreover, neither state's approach has deterred its adversaries from acquiring or using capabilities to conduct cyber-attacks against it. Thus despite both states having made substantial policy efforts which were ostensibly aimed at creating deterrence, the behaviour of both states had not produced the desired deterrent response.

The thesis concludes in Chapter 6 by summarising the main findings. First, I find that far from providing a template for other states considering deterrence theory for cyberspace, the US and Israeli experiences of deterrence should instead be regarded as a cautionary tale. The consistent lessons from a decade of deterrence practice in Israel and the US is that deterrence is risky, requires constant effort, and is difficult to implement in cyberspace. Hence, I argue, deterrence should be considered as only a partial answer – at best – for states seeking to secure their interests in cyberspace. As in all other domains, deterrence carries substantial risks. For a deterrence relationship to be successful, each side must understand the other, and both the Israeli and US cases demonstrate multiple occasions of misunderstandings and unintended consequences of activities branded as deterrence.

Thus, I argue that while both states have made significant efforts towards establishing a deterrence-based approach, US policy has been especially incomplete and inconsistent. As a result, it cannot be viewed as meeting the requirements of classic deterrence. In turn this means we are unable to assess whether deterrence could have been successful between 2008 and 2018 had it been complete; but the research indicates that this incomplete approach has proved detrimental to deterrence. And while Israel could be regarded as having met the requirements of deterrence, its method of operationalisation requires regular demonstrations of overwhelming force – an activity which is not, in fact, demonstrative of deterrence at all. As a pathway for future research, the conclusion notes that considering deterrence as a practice rather than a theory may help states operationalise their approaches, as would approaching deterrence as a whole of nation approach rather than attempting to confine it cyberspace. This is because 'cyber deterrence' – as demonstrated by the cases in the thesis – is potentially a misleading and unhelpful term that is too narrowly focused on dyadic models. And yet so too deterrence-as-practice may be similarly fraught. For instance, the increasing practice of naming pre-emptive strikes as deterrence measures erodes credibility and is creating new norms encouraging the use of cyber weapons in cyberspace. This may lead to a variety of unintended consequences, such as escalation and cyber arms racing.

The thesis concludes with the argument that regardless of government rhetoric regarding deterrence, the presence of comprehensive deterrence policies has ultimately not deterred adversaries from acquiring capabilities and conducting cyber-attacks. This finding suggests that states seeking to deter adversaries in cyberspace must accept ongoing engagement as a feature of the domain, and define their success in relative rather than absolute terms. Further, states wishing to adopt deterrence theory into cybersecurity policies should consider the final finding that such policies are more likely to be successful where their approach is balanced across the requirements of classical deterrence; and operationalisation of these policies is carefully managed in order to prevent unintended escalation.

The thesis demonstrates this argument over five chapters. Following the introduction, Chapter 1 considers the current state of literature on the usefulness of deterrence theory for cyberspace, and emphasises that the current literature is based on extrapolations of theory or isolated cases, rather than analysing the policies or practices of states. Chapter 1 makes the case for research that examines state deterrence practices. Chapter 2 then explores why the case study methodology is the most effective for studying deterrence and proposes a return to basic principles as a basis for a structured, focused comparison. It argues for the case for using three separate data sources, including the extensive use of primary source material from expert interviews and states' declared policies in order to provide a broad base for analysis. Chapter 3 and Chapter 4 present the Israeli and United States case studies, laying out preliminary findings before the structured cross-case analysis explored in Chapter 5, comparing the experiences and perceptions of each case against basic deterrence requirements. Lastly, Chapter 6 provides a summation of the reasoning behind the overall finding of this research: that despite significant policy effort, two of the most cybersecurity conscious states in the world have proved unable to deter cyber-attacks on their interests. While deterrence might theoretically work in cyberspace, neither case examined demonstrated efficacy in its application in that domain. States choosing to adopt deterrence for cyberspace should therefore do so with a balanced approach, an abundance of caution, and an expectation that deterrence will fail.

Chapter 1 Deterrence in cybersecurity: The theory/policy divide

1.1 Introduction

As outlined in the introduction, this research asks to what extent states employing deterrence as a cyberspace strategy consider it successful. Without exploring this question, we are potentially missing information: states are making the decisions to apply (or indeed, abandon) deterrence theory in cyberspace despite a lack of agreement on whether such application is likely to have a positive effect on cybersecurity, risking unintentional escalation and potential warfare. This chapter makes the case for research that examines states' efforts to implement and evaluate deterrence strategies to fill this gap. I begin by considering the importance of strategic theory for states' security practices, and argue the risks and opportunities of cyberspace are placing considerable pressure on states to re-evaluate such theories. In doing so I consider why securing cyberspace is a critical priority for states, and how deterrence came to be viewed as a potential answer to providing that security, by reviewing the status of deterrence theory and considering the major challenges with implementing such theory into strategy. The chapter then considers the implications of the development of nuclear weapons and argues this has led to a dangerous narrowing of deterrence theory. With 'nuclear deterrence' being often used as a synonym for deterrence, particularly in academic literature originating from the US, the chapter argues there is a need to return to first principles when examining deterrence for cyberspace. It contends that – despite the challenges posed by nuclear weapons – the core requirements of agreed deterrence theory remain largely unchanged and may yet offer a path for states to secure their interests in cyberspace.

And while there is an emerging but divided body of literature on the potential usefulness of deterrence for cyberspace, this division is due to authors being either too focused on the theory or too narrowly focused on comparisons to nuclear deterrence. I therefore consider the limitations of deterrence theory broadly, before considering the particular complications caused by the unique nature of cyberspace. The chapter then examines the conceptual issues with the term 'cyber deterrence' and argues the different ways states use terminology in the space directly influence conceptions of success. It argues that despite the disputed nature of the academic literature, states are choosing to adopt deterrence theory into their cybersecurity policies. The chapter closes with the argument that, with more than a decade of state practice to examine, research that considers how states have applied deterrence theory in cyberspace is not only possible, but necessary.

1.2 The significance of the research

In identifying the key research question this thesis examines, I initially considered whether a new variant of deterrence theory was required to take into account the complexities of cyberspace and cybersecurity. However, the literature on what comprises deterrence theory is and how it can work is comprehensive and consistent.[42] Here we can suggest that the missing element is perhaps not the theory itself, but rather a practical test of that theory.[43] The question of whether including deterrence in the cybersecurity strategies of states may reduce or prevent cyber-attacks has not yet been answered, and this chapter considers the acknowledged complexities of such an evaluation. At the same time, as the decision to adopt a strategy of deterrence with respect to a particular threat carries significant long-term consequences,[44] this chapter argues that such research is necessary as states increasingly turn to existing theory in attempts to bolster their security. The dilemma of cyberspace is that it offers a potential shared experience for humanity and entrepreneurship, which states are seeking to encourage, while also offering new avenues for states to pursue their interests. The concept of securing this space, or attaining 'cybersecurity', has proved difficult to define;[45] this research adopts a working definition of cybersecurity as the ability of a state to secure its interests in cyberspace. This definition allows for wide variation in states' ideas about security and interests.[46]

But providing security in cyberspace is a complex and rapidly shifting task for governments as societies become increasingly interconnected, and thus the potential for risk increases.[47] One indication of this risk is the increasing complexity of states' cybersecurity strategies. The earliest policies developed by states sought to protect basic information communications technology (ICT) infrastructure, but these were quickly expanded to include efforts in relation to incident management and response, aspects of national defence, and the use of offensive measures in cyberspace.[48] For example, one of the earliest US policies was the 2009 'Comprehensive National Cybersecurity Initiative' which aimed to defend against cyber threats and strengthen the future cybersecurity environment.[49] In 2016, the US released a Presidential Policy Directive on 'Cyber Incident Coordination'.[50] And by 2018 the US had four separate but interrelated strategies specifically designed to increase cybersecurity: the National Cyber Strategy,[51] the

[42] Schelling, *Arms and Influence*; George and Smoke, *Deterrence in American Foreign Policy: Theory and Practice*; Freedman, *Deterrence*; Morgan, *Deterrence Now.*

[43] This research also considered the possibility that there may not a causal connection between theory and practice. However the influence of modern deterrence theory on policy practice – even if imperfectly applied – indicates that exploratory tests of this theory have merit. For an argument for the necessity of examining deterrence theory in spite of its deductive origins and poorly understood causal links, see George and Smoke, *Deterrence in American Foreign Policy: Theory and Practice* pp. 2-5.

[44] Amir Lupovici, 2019, 'Toward a Securitization Theory of Deterrence', *International Studies Quarterly,* 63:1, 177–86, https://doi.org/10.1093/isq/sqy045

[45] Derek S. Reveron, 2012, *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, p.5

[46] Alexander Klimburg, 2012, 'National Cyber Security Framework Manual', NATO CCD COE Publication

[47] Jun Osawa, 2017, 'The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?', *Asia-Pacific Review* 24:2, 113; see also Richard A. Clarke and Robert K. Knake, 2010, *Cyber War: The next Threat to National Security and What to Do about It*, 1st ed., New York: HarperCollins

[48] 'UNIDIR Cyber Policy Portal: Collation of State's Cyber Security Policies', n.d., https://unidir.org/cpp/en/.

[49] Barack Obama, May 2009, 'The Comprehensive National Cybersecurity Initiative', The White House, US

[50] 'Presidential Policy Directive -- United States Cyber Incident Coordination', The White House, 26 July 2016

[51] 'National Cyber Strategy of the United States of America', September 2018, The White House, US

Cybersecurity Strategy,[52] the Department of Defense Cyber Strategy[53], and the National Defense Strategy.[54] Such policy efforts are in direct response to threats which are not particularly well defined or understood in a period of significant global change. Myriad competing threats – that can be internal, external and transnational – include global economic uncertainty due to the COVID-19 pandemic[55]; a contested international system; the rise of right-wing political parties in Western democracies[56]; and longer-term challenges such as climate change.[57] All of these challenges have cyber elements. To further complicate matters, the challenges posed by cyberspace to national security are often poorly understood by decision-makers.[58] Indeed, the pace of advancement in cyber technologies has led to tactics, strategy, and policy for cyberspace being developed and implemented before corresponding theories from academia are understood or tested. This situation challenges the ability of bureaucracies and political systems to manage change effectively.[59]

At the same time, as Lucas Kello argued in 2017, cybersecurity research that adopts and tests even the most basic strategic principles remains in its infancy.[60] This lack of research presents a serious challenge: because although considerable debate exists about the impact of cyber developments on national and international security, there remains a focus on adapting existing theory rather than examining basic principles of theory to assess if it is still appropriate.[61] Strategists, such as Amir Lupovici, argue that there is a critical need for scholarship that explores whether theories such as deterrence may be successfully applied in cyberspace.[62] It is arguably the case that research which considers the implications and risks of applying theory to cyberspace is necessary not only to examine perceived efficacy of current policies, but also to better inform states' decision-making regarding future cybersecurity policies.

[52] 'U.S. Department Of Homeland Security Cybersecurity Strategy', 15 May 2018, US Department of Homeland Security

[53] 'Department of Defense: Cyber Strategy 2018', September 2018, US Department of Defense

[54] 'Summary of the 2018 National Defense Strategy of The United States of America: Sharpening the American Military's Competitive Edge', 2018, Department of Defense

[55] Cristie Columbus, Karen B. Brust, and Alejandro C. Arroliga, 2020, '2019 Novel Coronavirus: An Emerging Global Threat', Baylor University Medical Center, Proceedings, 33:2, 209-12

[56] Sven Hillen and Nils D. Steiner, 2020, 'The Consequences of Supply Gaps in Two-dimensional Policy Spaces for Voter Turnout and Political Support: The Case of Economically Left-wing and Culturally Right-wing Citizens in Western Europe', *European Journal of Political Research*, 59:2, 331-53; see also Shelley Boulianne, Karolina Koc-Michalska, and Bruce Bimber, 2020, 'Right-Wing Populism, Social Media and Echo Chambers in Western Democracies', *New Media & Society*, 22:4, 683-99

[57] The 2017 US National Security Strategy outlines threats as 'political, economic, and military competitions', see Donald J. Trump, 2017, 'National Security Strategy Of the United States of America', The White House, US, pp.2-3

[58] The 2017 US National Security Strategy outlines threats as 'political, economic, and military competitions', see Donald J. Trump, 2017, 'National Security Strategy Of the United States of America', The White House, US, pp.2-3

[59] Alex S. Wilner, 2020, 'US Cyber Deterrence: Practice Guiding Theory', *Journal of Strategic Studies,* 43:2, 247; Martin Libicki, 2016, *Cyberspace in Peace and War*, 1st ed., Naval Institute Press

[60] Lucas Kello, 2017, *The Virtual Weapon and International Order,* New Haven: Yale University Press, p.3

[61] Kello, p.3

[62] Lupovici, 'Toward a Securitization Theory of Deterrence', 179

1.3 Why study strategic theory?

It is reasonable to question how a researcher can find answers about the efficacy of deterrence in policies for cyberspace when evaluating deterrence is notoriously difficult.[63] But one can also argue that complexity is excellent grounds for a return to theory. Theory gives us frameworks for understanding the world, and is most useful when grounded in reality.[64] As Alan Bryman argues, examining theory may provide an understanding through establishing patterns, and a framework within which social phenomena can be understood.[65] This being the case, exploring how existing theory is being applied to cyber policy may help build a better understanding of why a specific option is perceived as being successful or unsuccessful. A common criticism of theories however, and particularly strategic theory, is that while they may be intellectually interesting they are often too simplistic to be useful for decision makers.[66] But such misunderstandings often occur where theories guiding state practice are developed in isolation from practical realities and without reference to the broader strategic context. Put simply, research which is grounded in practice is more likely to be useful to policymakers. As Thomas Mahnken has argued, strategic theory grounded in practical evaluations is critical for well-informed decision making.[67] And as George and Smoke contend, policymakers can benefit greatly from theory: properly formulated, it can assist in diagnosing emergent situations and in determining how best to apply strategy.[68] Thus research that examines the extent to which applying strategic theory to cyberspace strategies is considered successful may assist us in understanding how such theories and strategies operate in practice, and help policymakers determine how theory should be applied in future.

Strategy is, at its most basic, the art of distributing and applying military means to fulfil the ends of policy.[69] Strategic theory is based on the premise that while the methods of warfare may change, the principles underlying it do not.[70] These principles continue to be tested, with conflict an ongoing feature of the international system, both within and between state and non-state actors; the wars in Iraq and Afghanistan, conflicts over land and resources in the Sudan and Congo, and threat of a rising China and assertive Russia indicate strongly that state-based conflict will continue to be a feature of the modern era.[71] Further, conflict between non-state actors, criminal organisations and proxy actors is rising, and

[63] Thomas C. Schelling, 2008, *Arms and Influence*, Yale University Press; Alexander L. George and Richard Smoke, 1974, *Deterrence in American Foreign Policy: Theory and Practice*, New York: Columbia University Press

[64] Schelling, *Arms and Influence*; George and Smoke, *Deterrence in American Foreign Policy: Theory and Practice*.

[65] Alan Bryman, 2012, *Social Research Methods*, 4th ed., New York: Oxford University Press

[66] Alexander L. George and Richard Smoke (1974) frame the problem of oversimplification as the premise for the examination of deterrence presented in *Deterrence in American Foreign Policy: Theory and Practice,* Columbia University Press, see pp.2-3

[67] Thomas G. Mahnken, 'Strategic Theory', in *Strategy in the Contemporary World*, 67

[68] Smoke and George, 1974, *Deterrence in American Foreign Policy*, p.589

[69] Gaddis, On Grand Strategy, p. 21

[70] Robert Ayson, 2006, 'Concepts for Strategy and Security', in Robert Ayson and Desmond Ball (eds.) *Strategy and Security in the Asia-Pacific,* Sydney: Southwood Press, p.12; see also Basil Liddell-Hart, 1967, 'Strategy: The Indirect Approach', London: Faber, p.335

[71] Richard A. Clarke and Robert K. Knake, 2010, *Cyber War: The Next Threat to National Security and What To Do About It,* New York: HarperCollins, p.19

cyberspace provides significant opportunities for threat actors with relatively small resources.[72] If John Garnett is correct about the ongoing conceptual and historical relevance of strategy,[73] then understanding strategic theory, and the lessons and frameworks it can provide for decision-makers for states concerned by both state and non-state threat actors remains relevant today. Further, as Lawrence Freedman notes, engaging with strategic theory is essentially both a pragmatic and practical activity.[74] As the basic principles of strategy have managed to stay relevant throughout the modern history of warfare[75], it is both reasonable and necessary to examine whether these principles also remain relevant in cyberspace.

1.4 Rethinking strategy in the cyber age

Given the importance of strategic theory and the major political, social and cultural shifts engendered by the ever-increasing reliance on cyberspace[76], there is a need for research that seeks to understand how strategy may shape and be shaped by the cyber age. While it seems logical that the fundamental principles of strategy are unlikely to change in cyberspace, testing such assumptions is an important step to building understanding of how strategic theory may be impacted by new technologies. As cyberspace evolves into an important domain of interstate conflict, understanding how theory operates in this domain remains an important endeavour.[77] For example, the very nature of cyberspace as an environment where state and non-state actors are active and influential, and yet the 'weapons' cannot yet produce overwhelming damage[78] means expecting deterrence to operate through binary dyadic relationships is not possible.[79] This research is not unique in arguing for the need to re-think strategy in the cyber age. For instance, Colin Gray has argued that strategic theory can provide useful frameworks for operating in cyberspace, and points to the ongoing relevance of strategy and the complex challenges states are facing in establishing and maintaining security in cyberspace as evidence.[80] Joseph Nye[81] and Lucas Kello[82] agree, pointing to the rapid shifts in technology and resultant shifts in state behaviour to argue that strategy needs to be re-thought in the cyber age. And Eric Gartzke contends that given the character of war has

[72] William J. Lynn, 2010 , 'Defending a New Domain: The Pentagon's Cyberstrategy', *Foreign Affairs*, 89:5, 98-99

[73] John Garnett, 2007, 'The Causes of War and the Conditions of Peace', in John Baylis, James Wirtz, Colin S. Gray and Eliot Cohen (eds.) *Strategy in the Contemporary World,* 2nd ed., Oxford University Press, p.35

[74] Lawrence Freedman, 2008, 'Strategic studies and the problem of power', in *Strategic Studies: a reader*, Thomas G. Mahnken and Joseph A. Maiolo (eds.), Routledge, p.22

[75] Hugh Smith, 2005, *On Clausewitz : A Study of Military and Political Ideas*, New York: Palgrave Macmillan, 68-69

[76] Erik Gartzke, 'The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth', *International Security*, 38:2, 41

[77] Will Goodman, 2010, 'Cyber Deterrence: Tougher in Theory than in Practice?', *Strategic Studies Quarterly*, Fall 2010, 102

[78] James F. Pasley, 2008, 'Chicken Pax Atomica: The Cold War Stability of Nuclear Deterrence', *Journal of International and Area Studies* 15, no. 2: 21–22.

[79] For an overview of the dispersed nature of the cyber threat and the range of threat actors and threat abilitites see Jasper Frei, 'Israel's National Cybersecurity and Cyberdefense Posture: Policy and Organizations', application/pdf (ETH Zurich, 2020), 7, https://doi.org/10.3929/ETHZ-B-000438397.

[80] Colin S Gray, 2013, 'Making strategic sense of cyber power: Why the sky is not falling' *Strategic Studies Institute,* Carlisle, PA, p.4

[81] Joseph S. Nye, *The Future of Power* 2011, Public Affairs: New York, 322

[82] Kello, 45

evolved over time, it is reasonable for observers to consider the impact of new technologies on the nature of war.[83] Further, this is an area of research where cross-field research has never been more critical: as Anthony Kenny reminds us, that for all the technological advances of the cyber age, war is, and will remain, a human activity.[84] And therefore, while the main objectives and conduct of that activity may remain contested, it is thus nonetheless also fundamentally knowable.

Naturally, examining the influence of cyberspace on the entire field of strategic theory is beyond the scope of a single thesis. While there are several areas of strategic theory academics are examining in light of the cyber age, the most contentious and problematic of these is deterrence.[85] Deterrence is as old as strategy, based on defensive principles, and perceived as having often been successful.[86] At face value, deterrence seems a logical part of states' cybersecurity strategies, and an option that should help states secure their interests in cyberspace. Governments adopt deterrence theory into explicit government cybersecurity policies with the ostensible aim of preventing conflict. And yet such adoption is never perfect. As Freedman has observed, the conceptual frameworks adopted by policymakers are likely to be as eclectic, inchoate and self-contradictory as they are systemic and rigorous, but that does not mean they can be readily dismissed.[87] In particular the adoption by states of deterrence into cybersecurity policy over the past decade represents a rich opportunity to explore how states embedded and implemented theory into cybersecurity policies, with the ultimate aim of considering how successful such attempts have been in preventing cyber-attacks. As understanding how and why states have adopted deterrence strategies in cyberspace requires an understanding of what deterrence is and how it operates, the next section of this chapter considers deterrence theory, including acknowledged issues with the theory, before exploring how it came to have a central role in states' cybersecurity policies.

1.5 The basic concept of 'Classic' deterrence

Deterrence, as the idea that it is possible to manipulate another's behaviour through threats,[88] is neither new nor unique to the field of strategy. However in order to evaluate deterrence as part of states' strategy, we must first briefly examine its origins.[89] Early strategists like Thucydides[90], Sun Tzu[91] and Karl von

[83] Eric Gartzke, 2013, 'The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth', *International Security,* 38:2, 43

[84] Anthony Kenny, 1985, *The Logic of Deterrence,* Firethorn Press, p.5

[85] Will Goodman, 2010, 'Cyber Deterrence: Tougher in Theory than in Practice?', *Strategic Studies Quarterly*, Fall 2010, 103

[86] Both Patrick Morgan and Alexander L. George and Richard Smoke note that while deterrence has often been perceived as successful, these successes need to be carefully considered. See Patrick M. Morgan, Deterrence Now, vol. 89., (Cambridge [England];New York; Cambridge University Press, 2003), p. 285; Alexander L. George and Richard Smoke, Deterrence in American Foreign Policy: Theory and Practice, Book, Whole (New York: Columbia University Press, 1974), p. 589

[87] Freedman, 2004, *Deterrence*, p.5

[88] Ibid, p. 6

[89] Roy E. Jones, 1968, *Nuclear Deterrence: A Short Political Analysis,* London: Routledge, p.1

[90] Robert B. Strassler (ed.), 1996, *The Landmark Thucydides: A Comprehensive Guide to the Peloponnesian War,* Rev., New York: Simon and Schuster

[91] General Tao Hanzhang, 1990, *Sun Tzu's The Art of War*, trans. Yuan Shibing, New York: Sterling, p. 15

Clausewitz[92] all explored the idea that groups sought to deter others from actions that would harm their interests as a core precept of strategy. Thucydides noted several instances during the Peloponnesian Wars where one side manoeuvred for allies or advantages to change an opponent's calculation of the associated costs and risks, and influence their action accordingly.[93] In more modern times Thomas Schelling described deterrence as the 'persuading of an enemy that he should, in his own interests, avoid certain courses of activity'.[94] Alexander George and Richard Smoke defined deterrence in 1976 as the idea that 'it is possible to persuade an opponent that the costs or risks of a given course of action outweigh the benefits and thus deter them from acting'.[95] Similarly, John Mearsheimer in 1983 characterised deterrence as persuading an opponent not to initiate a specific action because the perceived benefits do not justify the estimated costs.[96] Ultimately, the purpose of deterrence is therefore to prevent conflict, a potential Basil Liddell-Hart characterised as 'the perfection of strategy'.[97] The concept of persuading an enemy however immediately reveals the complexity of deterrence theory; it is frequently described as a psychological relationship because the focus is on the perception and decision process of the opponent.[98] Thus even though the concept of persuading an enemy not to attack is complicated (as this chapter will illustrate), the potential benefit for states is the avoidance of conflict and war while protecting their interests. Deterrence is also useful in that it is not limited to military considerations: when formulating a deterrence posture it can be supported by broad measures, although as this also means leaders must consider risks and costs of a non-military nature, from economics to society[99] and even culture.[100]

[92] See Carl von Clausewitz, 1976, *On War,* Michael Howard (ed.) Princeton, NJ: Princeton University Press; Robert B. Strassler (ed.) 1996, *The Landmark Thucydides: A Comprehensive Guide to the Peloponnesian War* Rev. New York: Simon and Schuster. See also Alexander L. George and Richard Smoke, 1974, *Deterrence in American Foreign Policy: Theory and Practice*, New York: Columbia University Press

[93] Richard Ned Lebow, 2007, 'Thucydides and Deterrence' *Security Studies* 16:2, 163-164; see also Alexander L. George and Richard Smoke, 1974, *Deterrence in American Foreign Policy: Theory and Practice*, Columbia University Press, p.5

[94] Thomas C Schelling, 1960, *The Strategy of Conflict*, Cambridge, MA: Harvard UP, p.9

[95] Alexander L. George and Richard Smoke, 1974, *Deterrence in American Foreign Policy: Theory and Practice*, Columbia University Press, p.11

[96] John Mearshimer, 1983, *Conventional Deterrence*, Cornell University Press, p.1 4

[97] Basil Liddell-Hart, 1996, *Strategy,* 2nd ed., London: Faber, p.338

[98] Patrick M. Morgan, *Deterrence: A Conceptual Analysis* 1977 Sage Press, 32

[99] John Mearshimer, 1983, *Conventional Deterrence*, Cornell University Press, p.14

[100] Strategic culture, the concept that states approach strategic issues differently due to their own lived experiences, is based on the understanding that states are predisposed by their historical experiences, political systems and cultures to deal with security issues in a particular way, an approach that on face value could have added to this research. But while some strategists make the case for the importance of strategic culture as a framework for strategy (see Rashed Uz Zaman, 2009, 'Strategic Culture: A "Cultural" Understanding of War', Comparative Strategy 28, no. 1, 68–88); I argue that the contested nature of strategic culture as a concept would have added unnecessary complexity. Colin Gray noted this complexity when he argued it would be wiser to think of strategic culture as an umbrella concept under which multiple cultural identities are at play. See Michael C. Desch, 2005, 'Culture versus Structure in Post-9/11 Security Studies', *Strategic Insights*, IV:10. Further, as Wyn Rees and Richard J Aldrich note it 'remains an ill-defined and under-used concept'. See Patrick Hinton, 2020, 'Strategic Culture: In Defiance of a Structural World Order', *The RUSI Journal*, 165:4, 80–87. Lastly, as Pauline Kerr argues strategic culture is not a sufficient concept by itself; as an intellectual tool it does not recognise the important claim that security is comprehensive and involves the use of force outside of the state as well as military factors inside and outside of the state. See Pauline Kerr, 1998, Researching Security in East Asia: From 'Strategic Culture' to Security Culture, Working Paper No. 326, Canberra: Strategic and Defence Studies Centre, Australian National University .

The essential idea of 'classic' deterrence is a strategy of persuasion: an attempt to influence the cost-benefit calculations for the purpose of avoiding war.[101] This concept has remained relatively consistent – as Freedman notes, deterrence is one of the better-tested concepts in strategic theory.[102] However, despite agreement on the aim of deterrence, operationalising it into strategy is an entirely different matter. States have had serious difficulties with creating strategy that delivered the intended deterrent aims, certainly pre-dating its application to cyberspace. Moreover, states have also varied widely in their ideas about what 'successful' deterrence is, and how it should be judged.

1.6 What is success? The complexity of applying deterrence theory

While the conceptual basis and aim of deterrence is clear, the question of how best to implement and evaluate deterrence in practice is more complex. Freedman points out that while deterrence can be a technique, a doctrine, and a state of mind, in all cases it includes the need for setting boundaries and establishing the risks associated with crossing those boundaries.[103] But the question of how best to establish and enforce those boundaries is the subject of ongoing conceptual debate. Deterrence becomes immediately complicated when we try to consider how best to threaten, and if the threat fails, how best to punish.[104] These debates are important for framing research on deterrence because As Patrick Morgan argued, the different views of deterrence have substantially different implications for national security policy.[105] How theorists define deterrence success and how best to achieve it directly impacts whether states judge their own, and others, efforts as successful or otherwise. This indicates a need to examine the key problems with operationalising deterrence theory, especially how strategists have traditionally conceptualised deterrence success.

Traditional deterrence theorists concentrated on the conditions needed for success[106], which requires an actor issuing a deterrence threat and the target of that threat understanding it as intended.[107] Patrick Morgan framed the conditions for successful deterrence as requiring three main elements: the ability to persuade your opponent that you had an effective military capability; that you could credibly impose unacceptable costs on him; and that you would use it if attacked.[108] This basic, but effective, summary of the core principles required to create deterrence is agreed by leading strategists.[109] Roy E. Jones argues a threat is only effective if it is perceived as such[110], highlighting the importance of both credibility and

[101] Stanley Allen Renshon, 2010, *National Security in the Obama Administration: Reassessing the Bush Doctrine*, New York: Routledge, p.114
[102] Lawrence Freedman, 2008, *Strategic Studies and the Problem of Power*, in *Strategic Studies: A Reader*, Routledge; see also Roy E. Jones, 1968, *Nuclear Deterrence: A Short Political Analysis,* London: Routledge, p.7
[103] Lawrence Freedman, 2004, *Deterrence,* MPG Books, 116
[104] Patrick M. Morgan, 1977, *Deterrence: A Conceptual Analysis* Sage Press, p. 17
[105] Ibid p. 74
[106] George and Smoke, Deterrence in American Foreign Policy, p. 589
[107] Amir Lupovici, 2019, Toward a Securitization Theory of Deterrence: Theory Note, *International Studies Quarterly*, 63, 177
[108] Patrick M. Morgan, 2003, *Deterrence Now*, Cambridge University Press, p.4
[109] Schelling and Freedman
[110] Roy E. Jones, 1968, *Nuclear Deterrence: A Short Political Analysis,* London: Routledge, p.1

channels of communication. And Aaron F. Brantly noted the need to establish clear and unambiguous signals to potential adversaries of what is and isn't acceptable behaviour as a critical and central tenet of deterrence.[111] These requirements – summarised as capability, credibility and communication – form the most basic test of deterrence. Yet while seeming quite simple on face value, operationalising each as a part of strategy, for traditional strategic interactions much less for cyberspace, has proven difficult.

Consider the problem of developing capabilities: the means by which a state can threaten the use of force. As Robert Powell has observed, the greater a state's defensive capability, the less an adversary can hurt it; the greater a state's punitive capability, the more punishment it can impose.[112] Thus as Mearsheimer argues, a potential attacker must know not only his own capabilities but those of his adversary.[113] If building capabilities is a critical requirement for a state seeking to deter adversaries[114], military preparations arguably make for peace by forcing would-be aggressors to consider the cost.[115] However, there is a countervailing school of thought from arms race theorists who contend that an increase in capabilities by any one nation then leads to an increase by rivals, potentially leading to a vicious cycle of wasteful expenditure at best, and war at worst.[116] In an arms race, both sides seek not parity of capabilities but military superiority; each side may interpret his rivals' capability as intent.[117] Thus we can see that establishing the first basic element of deterrence is a difficult enterprise for states, as the difference between a capability developed with intent to deter, versus a capability developed which presents a threat, depends entirely on the perceptions of adversaries.

Even if one could set aside the risk of an arms race, capabilities alone are insufficient for deterrence[118], regardless of how terrifying they are. Deterrence requires more than the ability to impose costs: as Robert Powell argues, an adversary must be sufficiently convinced that the state will actually use those punitive capabilities.[119] While the capabilities for offence and defence might be conceptually separate, actual military forces usually combine the two,[120] which is a problem that is particularly apparent in cyberspace. The idea of 'sufficiently convincing' is immediately subjective and relies on credibility and effective communication, making such a threat credible depends on a range of factors including the existing relationship, strategic and historical context, the potential damage caused by such punishment, and the risk of escalation. It also requires clear understanding of the circumstances in which force should be

[111] Aaron F Brantly, 2020, 'Entanglement in Cyberspace: Minding the Deterrence Gap', *Democracy and Security*, 16:3, 215

[112] Robert Powell, Nuclear Deterrence: The search for credibility p. 7

[113] John Mearshimer, 1983, *Conventional Deterrence*, Cornell University Press, p.63

[114] Jesse C. Johnson, Brett Ashley Leeds and Ahra Wu, 'Capability, Credibility and Extended General Deterrence' *International Interactions*, 41:2, 309-336

[115] Raoul Naroll, Vern Bullough and Frada Naroll, 1974, *Military Deterrence in History: A Pilot Cross-Historical Study*, State University of New York, p.3

[116] Ibid

[117] J. David Singer, 1962, *Deterrence, Arms Control and Disarmament*, Columbus: Ohio University Press

[118] Aaron F Brantly, *Entanglement in Cyberspace: Minding the Deterrence Gap,* p.211

[119] Robert Powell, Nuclear Deterrence: The search for credibility p. 7

[120] Ibid., p.9

expected. As Thomas Schelling argued, credibility is easy to establish in terms of defending one's own territory, but rather harder once threatening military activity beyond one's own boundary.[121] Israeli strategist Amos Malka has observed that in order to be credible, the issuing of threats must be supported by a willingness to pay the price whenever established red lines are crossed.[122] Thus while credibility is an agreed requirement of deterrence, just as for capability, creating it in any domain is difficult.[123] This is because credibility depends both on the ability and will of the defender to retaliate, or in the case of attempts to deny adversaries their intended outcome, to set aside the costs necessary to establish a reasonable denial structure.[124]

Similar difficulties apply to the requirement of communication. Deterrence situations are not natural ones, but rather represent social constructions that require constant adaptation to mitigate the risks of miscalculation; such adaptation relies heavily on timely and convincing communication.[125] Deterrence requires a state to have not only deep knowledge of their own capabilities, credibility and communication efforts but also sufficient understanding of an adversary to be able to predict and then deter a potential attack.[126] A further complication for operationalising deterrence is that to issue a threat there must be a role for force. But strategists disagree over whether such force needs to be merely threatened or actually used in order to create deterrence. Consider Schelling's argument that to be effectively coercive – that is, for a threat to be effective in influencing enemy intentions – violence has to be not only anticipated, but also avoidable by accommodation.[127] In other words, an adversary needed to have an available course of action that prevents the violence from being required. The concept of creating a deterrent threat so powerful that violence is too costly is known as deterrence by denial. Here, Jack Snyder has argued that a state deters by being able to physically deny the enemy their goal. Conversely, deterrence by punishment is where a state deters an adversary from invading by credibly threatening to impose enough punishment so that the costs of invading seem greater than the potential gains.[128] Similarly, Michael Mazaar has described denial strategies as seeking to deter an action by making it seem unlikely to succeed.[129] And as Martin Libicki notes a simpler conception of the aim of denial strategies is

[121] Thomas C. Schelling, 2008, *Arms and Influence,* Yale University, p.36

[122] The concept of crossing a 'red line' refers to an action which prompts a particular reaction from a state; see Amos Malka, 2008, Israel and Asymmetrical Deterrence, *Comparative Strategy*, 27:1, 6

[123] Robert Powell, Nuclear Deterrence: The search for credibility p. 9

[124] Glaser, Deterrence of Cyber-attacks and US national Security, see also Aaron F Brantly. Entanglement in Cyberspace Minding the Deterrence gap p. 211

[125] Jean-Loup Samaan, 1 May 2014, 'From War to Deterrence? Israel-Hezbollah Conflict Since 2006', Fort Belvoir, VA: Defense Technical Information Center, p.512

[126] Patrick M. Morgan *Deterrence Now*, Cambridge University Press, 2003, p.1

[127] Thomas C Schelling, 1991, *Arms and Influence,* Yale University Press (reprint) Ch. 1, 2

[128] Snyder, 1961, pp.14-16, see also Michael J. Mazarr, 2018, 'Understanding Deterrence'*, Perspectives*: RAND Corporation, p.2

[129] Michael J. Mazarr, 2018, 'Understanding Deterrence'*, Perspectives*: RAND Corporation, p.2 https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE295/RAND_PE295.pdf

to remove the incentive for attack, whereas deterrence by punishment threatens severe penalties if an attack occurs.[130]

As strategists recognise that not all threats can be denied, deterrence by punishment offers an explanation for how states could respond to unwanted behaviours in the hope of preventing future attacks. For Thomas Rid punishment (as the use of force in response to a committed offence) is a valuable part of deterrence strategy.[131] But the concept of punishment as a deterrent may also be problematic. After all, if force is used, it would appear in many circumstances that deterrence has failed. One answer to this conundrum is the concept of serial deterrence[132] which allows for force to be used in order to create periods of peace, and deter the use of even more devastating force. In this context the Israeli strategist Uri Tor has described deterrence as a cumulative process which requires regular 'refreshment' to be successful.[133] Thus we can see that the 'success' of activities and policies intended to deter depends entirely on broader strategic goals rather than any one use of force.

The intent behind the use of force is also a factor affecting deterrence. Morgan argues deterrence should be distinguished from the use of threats to prevent opposition or to interfere with aggressive objectives, and that such 'offensive deterrence' is a contradiction in terms.[134] However, the difference between a pre-emptive strike and an unwarranted act of war is notoriously difficult to define and depends upon the perceptions of the parties involved. Further, there is debate regarding whether deterrence should be considered as a stand-alone relationship with an adversary or, as Rid argues, a series of acts of force to create and maintain general norms of behaviour for many political actors over an extended period of time.[135] As states attempting deterrence must take into account the labyrinth of forces, constraints, projections and balances acting on the majority of the players from different directions,[136] then research which seeks to evaluate deterrence success must include not only deterrence relationships but the context in which those relationships occur in order to properly consider intent. Lastly, states define success at every level of deterrence to suit their own strategic goals, and these definitions vary both between states, and within states over time. While it is thus possible to consider whether states have met their own definitions of success, such declarations must be considered as part of each state's broader strategic context.

[130] Martin C. Libicki, 2009, *Cyberdeterrence and Cyberwar,* RAND Project Air Force, p.7; see also Michael J. Mazarr, 2018, 'Understanding Deterrence'*, Perspectives*: RAND Corporation, p.2

[131] Thomas Rid, 2012, 'Deterrence Beyond the State: The Israeli Experience'*, Contemporary Security Policy*, 33:1, 127

[132] Patrick Morgan describes serial deterrence in his book *Deterrence Now* (2003), see page 75

[133] Uri Tor, 2017, '"Cumulative Deterrence" as a New Paradigm for Cyber Deterrence', *Journal of Strategic Studies* 40:1-2, 92-117, https://doi.org/10.1080/01402390.2015.1115975.

[134] Patrick M. Morgan, 1977, *Deterrence: A Conceptual Analysis*, Sage Press, p. 30

[135] Thomas Rid, 2012, 'Deterrence Beyond the State: The Israeli Experience'*, Contemporary Security Policy*, 33:1, 124-147, p.125

[136] Amos Malka, 2008, 'Israel and Asymmetrical Deterrence', *Comparative Strategy*, 27:1, 2

1.7 Can deterrence be extended or collective?

As difficult as deterrence is to create, it becomes further complicated when states attempt to extend it beyond their borders, both in defence of their own interests, or those of allied nations. The notion of extended deterrence, despite being a complex and problematic concept in the nuclear era[137], has been adopted by some states. For example, the US moved to offer extended deterrence to allies in cyberspace in 2018. Yet extended deterrence itself is a problematic concept. Robert Powell, for instance, has described the idea of the US extending its deterrent capabilities to Western European states through threatening retaliation against the Soviet Union as 'inherently incredible'.[138] The concept of extended deterrence is linked to the equally problematic concept of collective actor deterrence, which is the idea that a group of states acting together have more power than a single state. Collective actor deterrence was thought to be more effective by challenging an adversary with the power of a collective, thus avoiding the security dilemma a single state might face.[139] But the viability of collective actor deterrence has always been questionable, and particularly difficult to make credible given the time it takes to form a collective.[140] Given the contested nature of the usefulness of these concepts, research seeking to evaluate the success of deterrence in cyberspace should examine statements about the efficacy of extended deterrence and collective actor deterrence with careful scepticism.

1.8 Intent: Critical but difficult to assess

In conceptualising success, states also need to consider whether the intent is to deter an adversary from an imminent attack (immediate deterrence) or whether opponents instead maintain a force posture to deter even though neither side is close to attacking (general deterrence).[141] This differentiation between general and immediate deterrence is closely related to nuclear theory (considered in more detail later in this chapter); however, as Rid has argued, the majority of theory developed relating to nuclear weapons pertains to immediate deterrence[142] rather than the far more common situation of general deterrence.[143] Both Rid and Morgan considered this was a poor practice because intellectual and policy efforts were largely directed at the far less likely threat.[144] Hence the difference between potential and actual threats is a crucial point for framing considerations of deterrence success: as deterrence is a difficult theory to operationalise into policy, states seeking to use deterrence should direct their efforts towards the most likely threat relationships. However, the difficulty of correctly identifying the most likely threats is not a new problem in deterrence theory. Here, Schelling has contended that deterrence is about an enemy's

[137] Robert Powell, Nuclear Deterrence: The search for credibility p. 13
[138] Ibid
[139] Morgan, 1977, *Deterrence Now*, p.174
[140] Ibid p. 177
[141] Morgan, 1977, *Deterrence: A Conceptual Analysis*, p.28
[142] Thomas Rid, 2012, 'Deterrence Beyond the State: The Israeli Experience'*, Contemporary Security Policy*, 33:1, 126
[143] Patrick M. Morgan, 1977, *Deterrence: A Conceptual Analysis,* p.29
[144] Ibid p. 37

intentions, not just his capabilities,[145] and Morgan pointed out that states having the capability to attack does not necessarily mean that they will.[146] Indeed Morgan argued one of the most important, but least recognised, pre-requisites of deterrence is that one cannot deter someone who is giving no thought to attack.[147] Thus if deterrence is to make any sense, it must concern the relationship between opponents;[148] and states seeking to establish parameters for success must consider whether they intend to deter specific adversaries, or plan for more general deterrence. However, the concepts of denial and punishment, and general and immediate deterrence, are also problematic in that they arose from the particular circumstances of the nuclear era. Deterrence theory underwent a substantial revision and revival due to nuclear weapons, and any evaluation of deterrence success must take into account the impact this era had on the understanding and operationalisation of theory.

1.9 The influence of nuclear weapons on deterrence theory

Indeed, before we can research the application of deterrence theory to cyberspace it is important to acknowledge the extraordinary influence of nuclear weapons on deterrence theory. Kenneth Waltz described this impact thus: 'Nuclear weapons make the cost of war seem frighteningly high and thus discourage states from starting any wars that might lead to the use of such weapons.'[149] Nuclear weapons represented the development of military capabilities to such an extent that conflict could be 'ruinously destructive',[150] nuclear deterrence potentially offered a way for states to influence and interact with each other without inviting total war.[151] The success of nuclear deterrence is debated, but generally considered successful in that the use of nuclear weapons did not occur;[152] as Joseph Nye argues, the non-use of nuclear weapons represents the prevention of annihilation.[153] Likewise, John Lewis Gaddis credits nuclear deterrence for the long peace after 1945.[154] But nuclear weapons forced those who possessed them to turn deterrence into a new and comprehensive strategy that touched and shaped many policies and activities,[155] not all of these helpful for strategists outside the nuclear domain.

[145] Thomas C. Schelling, 2008, *Arms and Influence,* Yale University, p.70
[146] Patrick M. Morgan, 1977, *Deterrence: A Conceptual Analysis,* Sage Press, p.34
[147] Ibid 33
[148] Ibid 33
[149] Kenneth Waltz, 1981, 'The Spread of Nuclear Weapons: More May Be Better', International Institute for Strategic Studies, Adelphi Papers, p.171
[150] Patrick M. Morgan, 2003, *Deterrence Now,* p.5; see also Roy E. Jones, 1968, *Nuclear Deterrence: A Short Political Analysis,* London: Routledge; and Muthiah Alagappa, 2008, *The Long Shadow: Nuclear Weapons and Security in 21st Century Asia*, Stanford University Press, p.2
[151] Patrick M. Morgan, 2003, *Deterrence Now,* p.5
[152] Jim Chen, 'Does Conventional Deterrence Work in the Cyber Domain?', *National Defense University,* Fort McNair, pp.106-107
[153] Joseph S. Nye, 2019, 'Deterrence in Cyberspace', *The ASPI Strategist* [blog], 1; see also Hugh Smith, On Clausewitz, p.265
[154] John L. Gaddis, 1983, *Strategies of Containment,* New York: Oxford University Press
[155] Patrick M. Morgan, *Deterrence Now* 2003 p.3 Note: While we cannot dismiss the influence of nuclear weapons and nuclear theory on considerations of deterrence in the cyber age, it is beyond the scope of this research to examine the role that nuclear weapons will have in future global security. The potential intersection of nuclear deterrence in the cyber age is a promising area of future research.

In particular, there are two major conceptual issues that emerged from the impact of nuclear weapons on deterrence theory: firstly, the idea of success as a zero-sum proposition where attacks could be entirely prevented became entrenched and secondly, the period witnessed the conflation of broad deterrence theory with the narrower concept of nuclear deterrence.[156] Despite deterrence theory having a long history prior to nuclear weapons, deterrence theory had to evolve to account for nuclear weapons as a critical component of international strategic stability.[157] Bernard Brodie's argument that the very destructiveness of nuclear weapons might be exploited to discourage states from initiating war, and the resulting identification of such weapons as the 'ultimate deterrent',[158] was a concept that had a lasting influence on deterrence theory in defining successful deterrence in zero-sum terms, but the complete lack of activity or attacks is a concept of success that has never been the standard in other domains. George and Smoke argue the advent of nuclear weapons led to a narrowing of deterrence theory that became a fundamental problem in the American application to policy during the Cold War.[159]

A further problem with the academic research in the nuclear era was that it struggled to define non-nuclear deterrence. In 1983 John Mearsheimer sought to redefine conventional deterrence as a function of the capability of denying an aggressor its battlefield objective with conventional forces:[160] a definition of deterrence that had the effect of 'othering' deterrence by nuclear means. The resulting conceptual separation between nuclear and conventional deterrence[161] is problematic because it led strategists and policymakers to understand and make policies for deterrence based on the means through which it was created, rather than as a theory agnostic of means. Jonathan Shimshoni has noted such conflation bred inaccuracy, as the desire to dissuade opponents from instigating war was neither an invention nor an innovation of the nuclear era.[162] Such conceptual separation is understandable given that, as Waltz argued, nuclear weapons allowed states under attack to threaten great harm without needing to defend themselves with conventional means.[163] But it is also problematic because in no other domain

[156] Robert Jervis identified the influence of nuclear weapons as being evident in three 'waves' of nuclear deterrence. the first attempted to manage the new implications of the atomic bomb and represented a focus shift from winning wars to averting them; the second considered the most effective application of methodologies in an attempt to introduce rigour including the introduction of the 'rational deterrence' model; and the third wave centred on testing the idea of a rational actor and practical applications of theory. For more detail on the evolution of deterrence theory, see Bernard Brodie, 1946, *The Absolute Weapon: Atomic Power and World Order*, Harcourt; see also Thomas C Schelling, *Arms and Influence,* 1991:Yale University Press

[157] Thomas Schelling, *Arms and Influence*, Chapters One and Two; see also Smoke and George, Deterrence in American Foreign Policy p. 13

[158] Bernard Brodie, 1946, *The Absolute Weapon: Atomic Power and World Order*, Harcourt

[159] George and Smoke, 1974, *Deterrence in American Foreign Policy*, p.591

[160] John J. Mearsheimer, 1983, *Conventional Deterrence,* Cornell University Press, p.15

[161] Ibid

[162] Jonathan Shimshoni, 1988, *Israel and Conventional Deterrence: Border Warfare from 1953 to 1970,* Ithaca: Cornell University Press, p.1. Such conflation can be seen in Lebow and Stein's definition of conventional deterrence through the frame of nuclear weapons as 'occurring where states were seeking to prevent the use of force by non-nuclear threats'. See Richard Ned Lebow and Janice Gross Stein, 1990, 'When does deterrence succeed and how do we know?'*, Occasional Paper No. 8*, Canadian Institute for International Peace and Security

[163] Waltz, 'The Spread of Nuclear Weapons: More May Be Better'.

of warfare do we address the topic of deterrence across an entire spectrum.[164] This weapons-centric definition of deterrence has been repeatedly noted as problematic, particularly in the US literature.[165] And despite the extraordinarily destructive potential of nuclear weapons, both conventional and nuclear deterrence rests on the same basic requirements identified earlier in this chapter: capability, credibility and communication.[166] This highlights the central issue, that whereas deterrence practices vary based on the means by which they are enacted, the principles of deterrence theory do not change. While nuclear weapons undoubtedly influenced the application and understanding of deterrence theory, they did not change its fundamental precepts.

Deterrence theory, and its role during and after the Cold War, has been the subject of a great deal of research – and academics are still divided over whether deterrence theory was 'successful'.[167] The persistence, particularly by US scholars, to continue viewing deterrence through a nuclear lens helps explain the view that deterrence has no place in strategies for cyberspace. This can be seen in Patrick Cirenza's argument that the nuclear analogy is flawed, and applying it to cyber does not bear further investigation because of the lack of an 'ultimate deterrent' comparable to that of a nuclear weapon,[168] or Martin Libicki's view that the fields of nuclear and cyber are so fundamentally different that the principles are not transferable.[169] And deterrence has an iconic status in the American strategic experience because it is credited with having prevented war with the USSR.[170] But as Tor points out, although the absolute paradigm of nuclear deterrence is ill-fitting when applied to cyber, this does not necessarily imply a failure of deterrence theory.[171] Rather, he argues, it implies that the theoretical framework may need to be reconsidered to fit appropriately.[172]

[164] Dorothy E. Denning, 2015, 'Rethinking the Cyber Domain and Deterrence,' *Joint Forces Quarterly,* 2nd Quarter, p.11

[165] Colin S. Gray, 1993, *Weapons Don't Make War: Policy, Strategy, and Military Technology*, Lawrence, Kansas: University Press of Kansas, p.155

[166] Patrick M. Morgan, *Deterrence: A Conceptual Analysis*, 1983: Beverly Hills: Sage Press

[167] See George H. Quester, 1986, *The Future of Nuclear Deterrence*, Lexington, Mass: Lexington Books, Tritten and Stockton, *Reconstituting America's Defense: The New U.S. National Security Strategy.* An example of such division is the problem of rational actor theory, a contested addition to deterrence theory. Firstly, rationality – the idea your opponent will behave in a rational manner – is subjective. Secondly, it did not prove particularly helpful for explaining the behaviour of states, either during the Cold War, or after it ended. Further, as Freedman argued, the problem of rational decision-making is that it requires us to accept that an actor can be rational within his own framework of understanding, which may differ markedly from our own. As deterrence can be modelled without rationality for the purposes of description, explanation and prescription, while research on deterrence for cyberspace should certainly consider states positions on rationality as a possible indicator of behaviours, rationality is subjective to the point of being unhelpful and thus cannot be considered as an essential deterrence requirement. See Freedman, p. 32 and Schelling, Arms and Influence, p. 37 and Dag Henriksen (2012) Deterrence by Default? Israel's Military Strategy in the 2006 War against Hizballah, Journal of Strategic Studies, 35:1, 95-120, p. 104

[168] Patrick Cirenza, *An Evaluation of the Analogy Between Nuclear and Cyber Deterrence*, 2015: Stanford University, p.iii

[169] Martin C. Libicki, *Cyberdeterrence and Cyberwar,* 2009: RAND Project Air Force, 7, this issue is also covered by Dorothy E. Denning, 'Rethinking the Cyber Domain and Deterrence,' *Joint Forces Quarterly,* 2nd Quarter, 2015, 11

[170] Renshon, *National Security in the Obama Administration: Reassessing the Bush Doctrine*, 104–6.

[171] Uri Tor, 2017, 'Cumulative Deterrence as a New Paradigm for Cyber Deterrence, *Journal of Strategic Studies*, 40: p.95

[172] Ibid

1.10 Caveats on deterrence theory

While the nuclear era popularised deterrence theory, it also exposed the limitations of the theory and difficulties of applying the theory to a complex and rapidly evolving strategic space. Yet despite these difficulties, deterrence is widely regarded as having been a successful strategy for preventing the use of nuclear weapons, even if not entirely successful at deterring conflicts below the nuclear level.[173] It seems logical therefore that states should seek to apply deterrence theory to cyberspace – a space that is also complex, dangerous and rapidly evolving. But those strategists most familiar with deterrence theory have sounded substantial notes of caution regarding its application, cautions which any consideration of 'success' must take into account. As early as 1974, George and Smoke argued that American strategists had erred by relying too heavily on deterrence strategy, and in treating deterrence as a stand-alone theory rather than one influenced by the international context.[174] By 1977, Morgan was reiterating that while deterrence works some of the time, our confidence in it is misplaced; it can be tenuous, and thus states ought not to rely on it too heavily.[175] If these strategists are correct that theory is essential to encouraging efforts both in deterring attacks and in reducing the damage if deterrence failed[176] but that states tend to rely on it too heavily, then research which is seeking to evaluate efficacy must also consider the extent to which states rely on it.[177] Thus deterrence – although popular, considered successful and with agreed requirements – should be treated with caution. Research seeking to understand perceptions of success should consider the relevant context as that success depends heavily on how states define their aims, the threats they are attempting to deter, and whether they consider success as a process or a point in time.

Given the complexities of conceptualising success for deterrence practice, including the difficulties revealed by the nuclear era on operationalising the theory, one might question why states would consider deterrence as relevant for cyberspace. There are certainly several strategists who have argued against including deterrence in cybersecurity strategies; however, these strategists tend make this case based on the argument that the narrow subset of nuclear deterrence is not applicable to cyberspace due to the vastly different nature of the weapons domains. This view illustrates the ongoing influence of the nuclear era, particularly on American strategists who are leading the development of deterrence theory. Richard Clarke and Robert Knake typify this approach, arguing that deterrence theory in cyberspace is likely to

[173] Schelling, Arms and Influence, p.xi

[174] George and Smoke, 1974, *Deterrence in American Foreign Policy*, p.589

[175] Patrick M. Morgan, 1977, *Deterrence: A Conceptual Analysis,* Sage Press, p.15

[176] Ibid

[177] Deterrence is a theory which has also attracted criticism, although most of these centred on problems implementing the theory, rather than the theory itself. For instance, Amos Malka argued in 2008 for a more nuanced understanding of deterrence, framing it as a complex interplay of many competing forces, structures and ideologies, rather than one state simply choosing to take measures to change the behaviour of another. See Amos Malka (2008) Israel and Asymmetrical Deterrence, Comparative Strategy, 27:1, 1-19 p.2 This argument is not new: in 1974 Smoke and George noted problems in existing empirical deterrence studies which did not accurately include the context of deterrence situations, see Smoke and George, p. 88. See also Robert Powell, Nuclear Deterrence: The search for credibility p. 7; and Amir Lupovici (2019) *Toward a Securitization Theory of Deterrence: Theory Note*, International Studies Quarterly, 63, 177-186 p.178.

have a very different meaning than it did for nuclear deterrence due to the substantially different nature of cyber weapons to nuclear weapons and the resulting differences in fear and credibility.[178] However they do not make a compelling case that it is the theory itself that needs to change. Rather they are comparing nuclear deterrence to cyberspace and finding the differences between nuclear and cyber weapons demand a different approach. Patrick Cirenza posed a similar criticism but again his argument relies on the comparison of a nuclear framework to cyberspace, not a deterrence framework.[179] Mariarosaria Taddeo takes a slightly different view, arguing that cyberspace is so unique it requires a domain-specific deterrence framework based on new theories.[180] This ultimately suggests that is not deterrence theory that needs to change, but rather that strategies intended to create deterrence adopted by states for cyberspace need to be adapted to the specific conditions of cyberspace. There is also a potential disconnect between the theory and strategy which research must take into account. Deterrence theory was, after all, meant to shape the development of effective strategy in the practice of deterrence.[181] However, considerations of effectiveness in the cyberspace domain have been limited despite many states adopting deterrence policies for cyberspace. This lack of evaluation is important, particularly in the construction of threats and considerations of how best to deter them. The adoption of deterrence policy through issuing a deterrent threat in cyberspace has the effect of constructing the threat as legitimate and existential,[182] and thus it would seem states had assessed the threat as legitimate enough to warrant significant policy attention to manage such threats. However, as the adoption of deterrence policy in cyberspace occurred before there was a body of evidence of its practical effectiveness; adopting a strategy of deterrence with respect to a particular threat carries with it significant long-term consequences.[183] Thus modern research on deterrence theory should aim to build understanding on the links between deterrence theory and strategy, including where it may have a negative impact on the construction of threats.

This chapter has so far argued for a principles-based approach to deterrence for cyberspace, with strategies based on the agreed requirements of classic deterrence, rather than states attempting to extrapolate from the narrow field of nuclear deterrence. However we should also note that as well as the issues identified with applying deterrence theory to strategy both broadly and in the nuclear realm, there remain substantial complexities with adapting deterrence theory for cyberspace specifically. These complexities include a lack of agreed definitions for basic terminology; the need to manage the divide between the human and technical aspects of cyberspace; the problem of military strategy attempting to secure civilian technology and infrastructures; the treatment of cyberspace as a domain of warfare; the

[178] Richard A. Clarke and Robert K. Knake, 2010, *Cyber War: The Next Threat to National Security and What To Do About It,* New York: HarperCollins, 189-190

[179] Patrick Cirenza, *An Evaluation of the Analogy between Nuclear and Cyber Deterrence,* Stamford University

[180] Mariarosaria Taddeo, 2018, 'Deterrence and Norms to Foster Stability in Cyberspace', *Philosophy & Technology,* 31:3

[181] Patrick M. Morgan, 2003, *Deterrence Now*, Cambridge University Press, p.xvi

[182] Amir Lupovici, 2019, Toward a Securitization Theory of Deterrence: Theory Note, *International Studies Quarterly*, 63, 178

[183] Ibid p. 177

difference between potential and actual threats; and the problem of attribution. This chapter will explore each issue and consider how they influence states' conceptions of success.

1.12 Defining cyber

In order to evaluate the success of states' deterrence approaches, we must first understand how states define that space. This is important, as definitions for cyberspace are not settled. This is not surprising given that cyberspace is a relatively new strategic space, and even the most basic cybersecurity terms are contested or even used to mean different things.[184] The term 'cyberspace' itself is attributed to author William Gibson, who defined it in 1982 as a 'consensual hallucination… a graphic representation of data abstracted from the banks of every computer in the human system… unthinkable complexity'.[185] But Gibson later identified issues with this definition, stating that 'it seemed like an effective buzzword… it seemed evocative and essentially meaningless.'[186] One could argue this problem of essential meaningfulness has continued to persist. As Libicki correctly notes, the concept of cyberspace is plastic and contentious but can be characterised as a man-made construct.[187] Alternatively Derek S. Reveron provides more detail in his conception of cyberspace as including:

> the physical hardware, such as networks and machines; information, such as data and media; the cognitive, such as the mental processes people use to comprehend their experiences; and the virtual, where people connect socially.[188]

P. W. Singer's definition of cyberspace goes further, comprising three key elements: an imagined space; with a physical presence; that is created and used by people[189] –a definition centred on the human experience. This is in contrast to Daniel Moran's definition comprising of a 'wholly imaginary space, whose functioning is dependent on physical systems'.[190] One could perhaps argue this definition has an implicit role for human activity, but it is not clear that this is the intention. Yet while Reveron's broader approach is all-encompassing, and includes physical hardware, information, and cognitive processes.[191]Yet the breadth of this definition poses challenges for states attempting to secure that space. It is difficult to

[184] Lucas Kello, 2018, *The Ultimate Weapon*, Yale University Press, p.3

[185] Scott Thil (March 17 2009) 1948: William Gibson, Father of Cyberspace, p.1
The first recorded use of the term cyberspace was by artist Susanne Ussing and her conceptual artistic installations under the name 'Atelier Cyberspace', a project that encouraged creativity, openness and human interaction in physical spaces. In 1982 novelist William Gibson used the term cyberspace in his short story *Burning Chrome*; it gained popularity through repeated use in his 1984 novel *The Neuromancer*. The essence of Gibson's definition is a 'consensual hallucination... a graphic representation of data abstracted from the banks of every computer in the human system... unthinkable complexity'.

[186] Scott Thil (March 17 2009) 1948: William Gibson, Father of Cyberspace, p.1

[187] Martin Libicki, Cyberdeterence and Cyberwar, p.11; see also Libicki, 2007, *Conquest in Cyberspace*, pp.1-72

[188] Derek S Reveron, *Cyberspace and National Security*, p.5

[189] P.W. Singer and Allan Friedman, 2014, *Cybersecurity and Cyberwar: What everyone needs to know,* Oxford University Press, p.13

[190] Daniel Moran, 'Geography and Strategy' in *Strategy in the Contemporary World*, 138

[191] Derek S. Reveron, 2012, 'An Introduction to National Security and Cyberspace', *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World,* Georgetown University Press, p.5

imagine how a state could attempt to provide security for not only its hardware and software, but also the 'cognitive processes' of its citizens. Perhaps this explains why Kello has argued a better approach is to separate out the concepts of 'cyberspace' and 'cyber domain' on the basis that each area requires different concepts and policy.[192] And yet while such separation seems logical it does not currently reflect state practices, nor does it include a role for human agency. This means that even if states followed Kello's logic, they would then need to develop separate policy for the people using cyberspace, and the technology underpinning those peoples' activities;[193] a separation that while conceptually more accurate is likely to be impractical.

The difficulty of defining cyberspace, and examining how states define cyberspace differently, is directly linked to the key area of definitional disagreement in the literature: whether technological aspects alone will suffice, or whether human elements should be included as well. What does this imply for our understanding of cyberspace? To begin with, the different framing of referent objects – in other words, what it is that states are trying to protect – produces different ideas about national security policy, and broader state strategy. Such differences indicate the challenges not only to states' national policies but also their international policies. This makes forming cohesive and cooperative international policy doubly challenging, because states are approaching cyberspace and cybersecurity from fundamentally different starting points. Second, such arguments are critical for strategies like deterrence in cyberspace, because states cannot deter computer networks or software. Rather, they should be attempting to deter the human state-directed activity behind those networks. A further common area of confusion is between the potential threats that could be enacted through cyber means, and the actual threats posed by adversaries. This distinction matters because to be successful, a deterrent threat must be tailored to the particular individuals of the opponent government.[194]

The problem of human agency and how best to manage it in deterrence is important because it influences how states construct both the space to be protected and the threats that may damage their security. However it is not a new problem. Bernard Brodie specifically included the human element in his definition of deterrence in 1959 as the attempt by decision makers in one nation to restructure the alternatives available to the decision makers in another nation in an attempt to exclude armed aggression from consideration.[195] Likewise in 1977 Morgan noted that behind any policy sits policymakers, and the human component is thus essential for a deterrence relationship.[196] This framing matters if Robert Jervis is correct that decision-makers are human actors that tend to fit incoming information to their existing theories, with a tendency to see other states as more hostile than they are.[197] Thus research seeking to evaluate deterrence strategies for cyberspace should consider the role of human agency in declared

[192] Lucas Kello, 2018, *The Ultimate Weapon*, Yale University Press, p.45

[193] Ibid p.25

[194] Patrick M. Morgan, 1977, *Deterrence: A Conceptual Analysis,* Sage Press, p.50

[195] Bernard Brodie, 1959, *The Anatomy of Deterrence, World Politics,* 11:2, 178

[196] Patrick M. Morgan, 1977, *Deterrence: A Conceptual Analysis,* Sage Press, p.32

[197] Robert Jervis, 1968, Hypotheses on Misperception, *World Politics,* 20, 454-479

strategy, as the inclusion or exclusion of human agency and activity provides context for how states are approaching policies to secure cyberspace, particularly regarding construction of the threat space.

However, this is complex in practice as many states have adopted a definition of cyberspace that emphasises technical elements without mentioning human ones. For example, the US relies on its 2009 definition of cyberspace as 'a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.'[198] Similarly, the United Kingdom (UK) defined cyberspace in its 2011 Cyber Security Strategy as:

> an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also other information systems that support our businesses, infrastructure, and services.[199]

Neither definition contains more than an implied role for human activity. Part of the reason for these overly technical definitions may be their origin in the field of ICT, focused on technical aspects of cyberspace rather than from strategic studies or international relations, which focus on broader state-centric challenges related to national power and policy.[200] And technical definitions can be an important part of operationalisation: the US Department of Defense (DoD), for instance, offers a highly technical definition of cyber as including:

> all digital automation, including those used by the Department of Defense and its industrial base. This includes information technology embedded in weapons systems and their platforms; command, control, and communications (C3) systems; intelligence, surveillance and reconnaissance (ISR) systems; and logistics and human resources systems; and mobile as well as fixed-infrastructure systems.[201]

This definition allows the US DoD to clearly identify what is in and out of scope for policy and operations.[202] But such definitions are problematic for broader deterrence strategy, as they tend to become outdated as technology evolves and are difficult for non-experts to understand. Kello argues that

[198] 'U.S. Strategic Command, The Cyber Warfare Lexicon: A Language to Support the Development, Testing, Planning and Employment of Cyber Weapons and Other Modern Warfare Capabilities, January 5, 2009. Unclassified/For Official Use Only. | National Security Archive', accessed 10 September 2021, https://nsarchive.gwu.edu/document/21360-document-1.

[199] 'The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World' (Cabinet Office, Whitehall, November 2011), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf. p.11

[200] Martin C. Libicki, 2016, *Cyberspace in Peace and War,* Naval Institute Press, p.70

[201] Cyber elements include all digital automation, including those used by the Department of Defense and its industrial base. This includes information technology embedded in weapons systems and their platforms; command, control, and communications (C3) systems; intelligence, surveillance and reconnaissance (ISR) systems; and logistics and human resources systems; and mobile as well as fixed-infrastructure systems. See US Department of Defense Task Force on Cyber Deterrence, Defense Science Board, 2014 p.2

[202] US Department of Defense Task Force on Cyber Deterrence, Defense Science Board, 2014 p.2

when governments adopt technical definitions as the official language, they are building on the mis-perception of cyber as an area that is so complex it is fundamentally unknowable.[203] As deterrence is a human endeavour in a domain constructed by humans, Kello is correct that technical definitions of cyberspace that do not include the human element are unhelpful. While this research notes the difficulties of defining cyberspace for states, there is an important balance to be found between strict theoretical definitional accuracy in academic research, and reflecting the practical reality of how states create and implement cybersecurity policy. After all, different conceptions of how governments make decisions produce different images of deterrence, how it works and what the chances are of success.[204] Given the variation in definitions, research which seeks to evaluate deterrence success in cyberspace should include state's own definitions of cyberspace and consider whether or not this includes the human element, and the implications of this choice. Without this specificity, research on states' approaches may not be comparable.

1.13 Defining the space: The 'cyber domain'

Research considering deterrence success must also consider why, and how, states choose to define cyberspace as a domain and if so, whether it should be treated as part of an integrated part of the overall threat space or as a domain that can be segregated from the more traditional domains of warfare. This distinction matters because it directly shapes ideas and expectations of deterrence in cyberspace. The use of 'domain' as a term and its usefulness for cyberspace is contested. William J. Lynn pointed out in 2010 that the Pentagon had, as a doctrinal matter, accepted cyberspace as a new domain of warfare that the military 'must be able to defend and operate within'.[205] Jun Osawa notes that the conception of cyberspace as a domain is not limited to the military and argues that as many national security experts view cyber as the fifth domain of warfare, this demonstrates the importance of the cyber 'domain' in national security.[206] But Eric Gartzke argues that while treating cyberspace as an operational domain is an excellent idea from an organisational viewpoint, doing so quickly reveals the differences between internet conflict and warfare on land, air, sea or space.[207] Indeed, the conceptualisation of cyberspace as a realm of war is more common among researchers from defence backgrounds who view cyberspace as a clearly delineated field that can be categorised in the same way the air, land, sea and space domains are categorised[208] and this has direct policy impacts. Consider that this view was used in the US to justify the

[203] Lucas Kello, 2018, *The Ultimate Weapon*, Yale University Press, p.44
[204] Patrick M. Morgan, 1977, *Deterrence: A Conceptual Analysis*, Sage Press, p.49
[205] William J. Lynn, 2020, 'Defending a New Domain: The Pentagon's new Cybersecurity Strategy', *Foreign Affairs*, September/October, 101
[206] Jun Osawa, 2017, 'The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?', *Asia-Pacific Review*, 24:2, 124; see also Christian Leuprecht, Joseph Szeman and David B. Skillicorn, 2019, 'The Damoclean sword of offensive cyber: Policy uncertainty and collective insecurity', *Contemporary Security Policy*, 40:3, 382
[207] Eric Gartzke, 2013, 'The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth', *International Security,* 38:2, 44
[208] Martin C. Libicki, 2009, *Cyberdeterrence and Cyberwar,* RAND Project Air Force, 7, this issue is also covered by Dorothy E. Denning, 2015, 'Rethinking the Cyber Domain and Deterrence,' *Joint Forces Quarterly,* 2nd Quarter, 11;

creation of an independent Cyber Command.[209] But it is arguably too simplistic to suggest cyberspace can be segregated and treated as a separate physical domain. For instance, Chris Demchak points out that cyberspace does not fit neatly into the framework of a military domain because while the term 'domain' is used by the US military to blend 'cybered' conflicts into the traditional mould of armed struggle, cyberspace is not so conveniently bounded.[210] Hence the designation does not help guide national leaders in dealing with cybered conflict.[211] The problem of cyberspace influencing other domains is recognised by Osawa, who concedes that any operations, in all other domains of warfare, now depend on cyberspace.[212] This notion of interrelated dependence is important for considerations of deterrence application. As Will Goodman contends, attempts to separate cyber and kinetic deterrence are unhelpful, as cyber-attacks are inseparable from the physical domain.[213] The contested nature of the cyber domain is a recognised issue in the literature. Martin Libicki argued in 2009 that despite the US defining cyberspace as a domain of warfare, it still needed to be understood in its own terms.[214] This argument is perhaps more helpful than Robert Jervis, who takes the view that it is far from clear that cyber should be considered a domain as cyber is merely an instrument that can be used to support national policies.[215] While this may be more conceptually accurate, his argument is somewhat undermined by the fact that multiple nations have adopted the definition of domain, and such legitimisation is difficult to reverse. But he is correct that the conceptualisation is a problematic one for states, largely because the majority of systems and infrastructure in cyberspace are civilian-owned and operated. This is different to any other domain of warfare, and the lack of direct government control adds complexity to any cybersecurity policy.[216] Clarke and Knake noted in 2010 the concern that the perception of cyberspace as a domain 'where fighting must take place and the US must dominate' pervades American military thinking.[217] But this is not without risk in a domain which is largely civilian. Even William J. Lynn, known for his blunt views on this topic, has admitted that the question of how and when a government might use military resources to protect civilian

see also Major Lee Hsiang Wei, 'The Challenges of Cyber Deterrence', *Pointer, Journal of the Singapore Armed Forces,* 41:1, 12; Reveron; Libibki etc; see also LtCol Shane P. Courville, 'Air Force and the Cyberspace Mission Defending the Air Force's Computer Network In the Future', *Occasional Paper No. 63*, Center for Strategy and Technology, Air War College

[209] William J. Lynn, 2020, 'Defending a New Domain: The Pentagon's new Cybersecurity Strategy', *Foreign Affairs*, September/October, 102

[210] Chris Demchak, 2012, 'Cybered Conflict, Cyber Power, and Security Resilience as Strategy', in Derek S. Reveron, *Cyberspace and National Security: Threats, Opportunities and Power in a Virtual World*, Georgetown University Press, p.124

[211] Ibid., p.124

[212] Jun Osawa, 2017, 'The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?', *Asia-Pacific Review*, 24:2, 124

[213] Will Goodman, 2010, 'Cyber Deterrence: Tougher in Theory than in Practice?', *Strategic Studies Quarterly*, Fall 2010, 102

[214] Martin C. Libicki, 2009, *Cyberdeterrence and Cyberwar,* RAND Project Air Force, 7, this issue is also covered by Dorothy E. Denning, 2015, 'Rethinking the Cyber Domain and Deterrence,' *Joint Forces Quarterly,* 2nd Quarter, 11

[215] Robert Jervis, 2016, Some Thoughts on Deterrence in the Cyber Era, *Journal of Information Warfare*, 15:2, 66-73, 66

[216] Christopher Haley, 2 November 2016, 'A Theory of Cyber Deterrence', *Georgetown Journal of International Affairs*, 5

[217] Richard A. Clarke and Robert K. Knake, 2010, *Cyber War: The Next Threat to National Security and What to do About It,* New York: HarperCollins, p.44

infrastructures is complex.[218] For many states, the delineation between military versus civilian roles and responsibilities in this space is yet to be decided, making appropriate deterrence strategies difficult to design or implement.

Further, some strategists define 'domain' quite differently altogether. Kello, for example, argues the cyber domain encompasses the bevy of human and institutional actors that operate and regulate cyberspace itself.[219] He argues that while cyberspace is a technical plane, comprised of machines and networks, the cyber domain is a political and social plane subject to wholly different interventions and behaviours.[220] But this is a different use of the term 'cyber domain' than currently in use in policy and strategy.[221] Libicki takes a more pragmatic approach arguing that whether cyberspace does or does not have the elements of a warfighting domain is largely irrelevant; what matters is whether understanding cyberspace as a domain promotes or hinders understanding of how to defend or attack networked systems.[222]

These differing views on whether the use of the term 'domain' is helpful or indeed accurate further demonstrate the complexities for both researchers and strategists in this field seeking to evaluate deterrence. After all, how does one define successful deterrence in cyberspace if it is unclear whether the parties even agree on the nature of the domain, let alone its relation to each state's security? But exploring how states approach this question may reveal useful findings regarding why states have chosen deterrence as their approach in cyberspace. For example, the conceptualisation of cyberspace as a domain to be defended may help explain why in some states the military has taken a lead role in developing policies to secure it. Further, it is not just the question of whether states define cyberspace as a domain. Researchers also need to consider whether the cyber domain is treated as part of a broader, integrated threat space or as a stand-alone space that can be segregated. In 2010 Lynn argued that predicting cyber-attacks was difficult, especially when both state and non-state actors pose threats.[223] This difficulty is understandable if cyberspace is treated as a separate domain. However, there is a compelling counter argument that while individual attacks might be hard to predict, the threat actors or adversaries that states must deal with, and seek to deter, are no different in cyberspace than in any other domain.[224] If states view the cyber domain as just another arena through which adversaries may attack their interests, then attacks are far more predictable.

[218] William J. Lynn, 2020, 'Defending a New Domain: The Pentagon's New Cybersecurity Strategy', *Foreign Affairs*, September/October, 104

[219] Lucas Kello, *The Virtual Weapon and International Order*, p.46

[220] Ibid., p.46

[221] Richard A. Clarke and Robert K. Knake, 2010, *Cyber War: The Next Threat to National Security and What to do About It*, New York: HarperCollins, p.159

[222] Martin C. Libicki, 2016, *Cyberspace in Peace and War,* Naval Institute Press, p.158

[223] William J. Lynn, 2020, 'Defending a New Domain: The Pentagon's new Cybersecurity Strategy', *Foreign Affairs*, September/October, 101

[224] Erik Gartzke, 2013, 'The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth', *International Security,* 38:2, p. 43

1.14 Defining the threat: Cyber-attacks

The next question pertains to the types of threat a state may face in cyberspace. Defining such threats is surprisingly difficult: the term 'cyber-attack' is yet another area where definitions are both crucially important and yet problematic for any researcher attempting to understand the relative success of deterrence strategies for cyberspace. Governments, strategists and ICT specialists use the term very differently. Lee Hsiang Wee provides a definition of cyber-attack as 'any action taken to undermine the functions of a computer network for a political or national security purpose.'[225] However, this definition is so broad it could include almost any activity a state deemed contrary to its interests. Whilst such breadth is beneficial for states in that it provides significant room to manoeuvre, adopting it for deterrence purposes would be useless as it requires states to deter all of that activity – a task arguably beyond deterrence, which is most effective when it is focused and targeted.

This research considers that Libicki's more precise definition of cyber-attack as 'an operation that uses digital information to interfere with an information system's operations and thereby produce bad information, and possibly decisions'[226] is both more accurate and useful for policymakers and strategists. There is also the question of how states define attacks: – cyber-attacks can (at the time of writing) generally cause only temporary and reversible damage.[227] As Gartzke points out, the conditions of cyberspace have not yet adequately met the threshold of significantly destructive attacks taking place over a period of time by a well organised group, be they state or non-state actors.[228] It is difficult to find evidence to support authors such as Vinton Cerf, for instance, who argue that cyber-attacks could be looked at as the legal equivalent of armed attacks.[229] The question of appropriate thresholds is one that could have been reflected in the Tallinn Manual 2.0, however creating certainty around thresholds in cyberspace has not been a priority for states who prefer ambiguity.[230]

The literature is further divided over the scope of the threat posed by cyber-attacks, and to what level deterrence can – and indeed should – be applied. In presenting classic deterrence theory, Morgan makes the important distinction that while deterrence is usually where we have in mind the threat of a military retaliation to forestall a military attack, it is possible for states to attack and deter in non-military ways, thus deterrence could apply at any level of conflict.[231] If indeed the impacts of cyber-attacks are temporary and reversible, then they probably do not meet the threshold of war. However they do still

[225] MAJ Lee Hsiang Wei, 'The Challenges of Cyber Deterrence', *Pointer: Journal of the Singapore Armed Forces*, 41:1, p. 12
[226] Martin C. Libicki, 2016, *Cyberspace in Peace and War,* Naval Institute Press, p. 19
[227] Gartzke, 'The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth', 42.
[228] Ibid.; see also Thomas Rid, 2012, 'Cyber War Will Not Take Place', *Journal of Strategic Studies*, 35:1, pp. 5-32
[229] Vinton G. Cerf, 2011, 'Safety in Cyberspace', *Daedelus*, 140:4, 59-69
[230] Dan Efrony, Yuval Shany, 2018, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice', *The American Journal of International Law* 112:4, 538
[231] Patrick M. Morgan, *Deterrence: A Conceptual Analysis* 1977 Sage Press, p. 27

pose serious threats to states' interests,[232] potentially serious enough for states to consider attempting to deter. Again, the extent of this seriousness depends on many factors, including how cyber-attack is defined. For example, strategists are divided over the inclusion of 'information warfare', the practice of states seeking to influence each other's behaviours through online information campaigns such as Russia's attempts to influence the 2016 US Presidential election.[233] Herbert Lin describes this concept as cyber-enabled information/influence warfare and manipulation – the practice by states of deliberately using information against an adversary to confuse, mislead or influence the choices and decisions an adversary makes.[234] In 2006 Kenneth Knapp and William Boulton further argued that information warfare had transformed from a military issue into a major commercial issue, and argued this demonstrated a growing threat of cyber war.[235] However, although information warfare is a hostile activity, Lin's assertion that it does not constitute warfare; is arguably more accurate:[236] rather, it is part of expected behaviours by states seeking to influence by any means possible. Information warfare therefore belongs in the same category as espionage in cyberspace: annoying, and potentially damaging certainly, but on the whole an expected part of state behaviour. The decision by states of whether or not to include information warfare as part of their definitions of cyber-attacks is yet another area where states' varied approaches can have a marked impact on deterrence policy. If states are attempting to deter only cyber-attacks which meet a threshold of war, one can immediately mount a case that almost all deterrence cyberspace has been successful. However, if deterrence includes the deterrence of cyber-enabled information warfare then deterrence would seem to have demonstrably failed as such attacks, far from being deterred, are rapidly becoming an expected part of state's expected behaviours. Thus the nature of how states define threats directly influences their perceptions of success. This definitional problem is repeated when considering the use of force, or compellence.

1.15 Compellence

The literature on compellence reveals yet another area of deterrence which potentially complicates assessing deterrence success in cyberspace. If deterrence is the use of threats to prevent states from starting a course of action then compellence is the use of threats to compel states to stop a course of action already underway, or to do something they were not doing.[237] Schelling described the difference as

[232] This research excludes 'cyber espionage' espionage by cyber means from the definition of cyber-attack; espionage is a standard and expected part of states' behaviours.

[233] Mark Landler and Scott Shane, 16 February 2018, 'U.S. Condemns Russia for Cyberattack, Showing Split in Stance on Putin', *The New York Times*, sec. U.S.; John Leyden, 'Russia's to Blame for pro-ISIS Megahack on French TV Network', accessed 24 June 2021, https://www.theregister.com/2015/06/10/russian_trolls_staged_tv5monde_megahack_shocker/.

[234] Herbert Lin and Jackie Kerr, 2017, On Cyber-Enabled Information/Influence Warfare and Manipulation, Centre for International Security and Cooperation, p. 3

[235] Kenneth J. Knapp and William R. Boulton Cyber-Warfare Threatens Corporations: Expansion into Commercial Environments, *Journal of Information Systems Management*, 23:2, 76

[236] Herbert Lin and Jackie Kerr, 2017, *On Cyber-Enabled Information/Influence Warfare and Manipulation*, Centre for International Security and Cooperation, p. 3; this issue is also covered in more detail in Chapter 3: Methodology

[237] Morgan, 2003, *Deterrence Now,* p. 2

compellence using threats to produce changed behaviour, rather than preventing a behaviour.[238] Morgan argued this distinction matters for studies of deterrence because achieving compellence is far harder than deterrence[239] because in cyberspace states are seeking to both stop ongoing cyberattacks and prevent new, and more dangerous attacks. If Morgan is correct that it is difficult to get states to cease actions they are already doing, like doing, and prepared carefully to do,[240] cyber-attacks are likely to pose great difficulty as they often fit all three criteria. However, Schelling also noted that the distinction between deterrence and compellence can be difficult to make practically since this depends on the perspective of an actor and often disappears once an engagement starts[241] – all of which are characteristics of the ongoing conflict in the cyber domain. Further, Powell has noted that while in some contexts the distinction may be useful, it is conceptually elusive; deterrence and compellence are sufficiently alike to consider both as attempts by a state to coerce its adversary into acting in certain ways and not others by shaping the adversary's estimates of the costs and benefits.[242] This research considers that identifying the distinction between deterrence and compellence is as complex – if not more so – in cyberspace as in any other domain. The increasing normalisation of activity and engagement and states' differing perspectives on acceptable behaviour, as well as deniability of cyber-attacks, renders the distinction unhelpful. The recognition of the problems related to compellence is not unique to its application in cyberspace; it is described as risking high tension, loss of control and rapidly spiralling escalation in the nuclear sphere.[243]

1.16 Attributing attacks

Researchers seeking to evaluate deterrence should also note significant differences in states' approaches towards attribution, defined by Clark and Landau in 2011 as the 'identification of the agent responsible for the action'.[244] They argue the potential for cyber-attackers to obscure their identity is a serious problem for cyberspace, particularly where states are seeking to respond to, and potentially punish cyber-attacks – critical requirements for deterrence.[245] This so-called 'attribution problem' is argued to be the central barrier to applying deterrence theory to cyberspace, as retaliation arguably requires knowing with full certainty who the attackers are.[246] And they are not alone in this view; Gartzke agreed in 2013 that attribution is vitally important for deterrence in cyberspace, as adversaries are more likely to strike if retaliation or punishment are unlikely.[247]

[238] Thomas C. Schelling, 2008, *Arms and Influence,* Yale University, p. 69

[239] Morgan, 2003, *Deterrence Now,* p. 2

[240] Ibid p. 3

[241] Ibid p.1

[242] Robert Powell, 1990. *Nuclear Deterrence Theory: The Search for Credibility*, Cambridge University Press, p. 7

[243] Rajesh M. Basrur, 2006, 'Minimum Deterrence and India's Nuclear Security', in *Minimum Deterrence and India's Nuclear Security*, p. 45

[244] David D. Clark and Susan Landau, 2011, 'Untangling Attribution', *Harvard National Security Journal,* 2, 1-2

[245] Jason Healey, 'The Implications of Persistent (and Permanent) Engagement in Cyberspace', *Journal of Cybersecurity* 5, no. 1 (26 August 2019): 4, https://academic.oup.com/cybersecurity/article/5/1/tyz008/5554878.

[246] David D. Clark and Susan Landau, 2011, 'Untangling Attribution', *Harvard National Security Journal,* 2, 1-2

[247] Eric Gartzke, 2013, 'The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth', *International Security,* 38:2, p. 46

While these views have proved influential, there are several misconceptions surrounding attribution, and according to Rid and Buchanan the literature is 'evolving surprisingly slowly'.[248] Firstly, when authors refer to the difficulties of attributing an attack, they are often referring to attribution via technical means only: the tracing of an attack through cyberspace.[249] While technical attribution is complex, it has become rapidly easier and more accurate to the point where in 2018 the US Office of the Director of National Intelligence published the unclassified 'Guide to Cyber Attribution' which clearly states that establishing attribution for cyber operations is:

> difficult but not impossible... in some cases, the intelligence community can establish cyber attribution within hours of an incident but the accuracy and confidence of the attribution will vary depending on the available data.[250]

Secondly, technical attribution is only one of many methods states may use to determine where an attack has originated. Cyber-attacks are very rarely purposeless; rather, they are part of one state's concerted efforts against another that fit within a known overall strategic context and thus intent can be inferred. As Rid and Buchanan argue, attribution is a nuanced process that requires skill at all levels,[251] and technical abilities are just one part of this process. Thirdly, attribution is also a legal standard, although it can be difficult to apply. Virginia Greiman points out that the question for states of when and how to accuse governments of a cyber-crime, cyber espionage or even an act of cyber war is a critical issue in reducing cyber conflicts, but that there is no international legal obligation to reveal the grounds on which attribution is based prior to taking appropriate action. She further argues states are not obligated to provide evidence of attribution when responding to another state's cyber intrusions.[252] This problem around the legal standards is again reflected in the unclear remit and influence of the Tallinn Manual 2.0. Efrony and Shany argue states that are heavily engaged in cyber operations appear to have a 'limited interest in promoting legal certainty regarding the regulation of cyberspace'[253] and that this illustrates that the Tallinn Rules have only a limited usefulness for guiding expectations of state practice. For states seeking 'rules' on attribution it would thus seem that while the Tallinn Manual provides guidance for states it is by no means definitive.

[248] Thomas Rid and Ben Buchanan, 2015, 'Attributing Cyber Attacks', *Journal of Strategic Studies* 38:1-2, 5
[249] MAJ Lee Hsiang Wei, 'The Challenges of Cyber Deterrence', *Pointer: Journal of the Singapore Armed Forces*, 41:1, p. 14; see also Erik Gartzke, 2013, 'The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth', *International Security,* 38:2, p. 46; and Martin C. Libicki, 2009, 'Cyberdeterrence and Cyberwar', RAND Project Air Force, p. xv; David D. Clark and Susan Landau, 2011, 'Untangling Attribution', *Harvard National Security Journal,* p.2
[250] Office of the Director of National Intelligence, A Guide to Cyber Attribution, 14 September 2018
[251] Thomas Rid and Ben Buchanan, 2015, 'Attributing Cyber Attacks', *Journal of Strategic Studie*s, 38:1–2, 4
[252] Virginia Greiman, 2021, 'The Politics and Practice of Cyber Attribution: A Global Legal Perspective', in *International Conference on Cyber Warfare and Security,* Reading, United Kingdom: Academic Conferences International Limited, 102–8, p. 102
[253] Dan Efrony, Yuval Shany, 2018, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice', *The American Journal of International Law* 112:4, 538

Leuprecht et al note that it is hard for a defender to know for certain from where an attack is originating, and even more difficult to convince others, say the North Atlantic Treaty Organisation (NATO) or the United Nations (UN), of the attack's source.[254] Given these differing ideas about how to understand attribution, Rid and Buchanan make a convincing argument that attribution is what states make of it and on a technical level, an art as much as a science.[255] While the Tallinn manual offers legal standards for attribution, the reality of state practice of public attribution has differed markedly. The Sony Pictures hack is a well-known example of public attribution for which the narrative changed repeatedly. This hack involved agents acting for the North Korean government conducting a cyber-attack against the US arm of Sony Pictures, in retaliation for a film depicting the North Korean leader in an unflattering manner.[256] The attack became public in late November 2014, and the Federal Bureau of Investigation (FBI) investigated within a period of days. By December 18 2014 'unnamed US officials' pointed to North Korea as being responsible,[257] and by 21 December 2014 US President Barack Obama had named North Korea as the culprit, and was reportedly considering putting North Korea on a terrorist list.[258] This attack demonstrated several important points regarding attribution. First, the US managed to attribute the hack relatively quickly; despite attempts to obscure the origin, it would seem that the US had managed to trace the origins within a matter of days. Second, it is likely that the US did not only attribute through technical means, but also used the variety of mechanisms any state uses to identify attackers. States can, and do, attribute cyber-attacks using the same methods they use to attribute conventional attacks, through a reasoned analysis of any given threat situation.[259] As well as technical indicators like infrastructure identification and malware indicators, the US has publicly stated it also uses tradecraft such as behavioural pattern analysis, considerations of broad intent and indicators from public or external sources.[260]

Third, the US not only attributed responsibility for the hack but chose to make that knowledge public. This demonstrates a further important point regarding attribution in that as well as being a legal standard, it is also both technical, and political. The decision to attribute publicly is a separate step to attributing internally; it requires careful consideration for several reasons.[261] States may choose not to attribute because emphatic attribution would at times require the exposure of classified sources and techniques, leaving public statements that seem vague. Attribution is also complicated by the lack of agreed

[254] Christian Leuprecht, Joseph Szeman, and David B. Skillicorn, 2019, 'The Damoclean Sword of Offensive Cyber: Policy Uncertainty and Collective Insecurity', *Contemporary Security Policy,* 40:3, 384
[255] Thomas Rid and Ben Buchanan, 2015, 'Attributing Cyber Attacks', *Journal of Strategic Studies,* 38:1-2, 7
[256] 'A Breakdown and Analysis of the December 2014 Sony Hack', Security, 5 December 2014, https://www.riskbasedsecurity.com/2014/12/05/a-breakdown-and-analysis-of-the-december-2014-sony-hack/.
[257] David E. Sanger and Nicole Perlroth, 'U.S. Said to Find North Korea Ordered Cyberattack on Sony', *The New York Times*, 17 December 2014, https://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html.
[258] 'U.S. Mulls Putting N. Korea Back on Terror Sponsor List ', *Kyodo News Service*, 2017
[259] Thomas Rid and Ben Buchanan, 2015, 'Attributing Cyber Attacks', *Journal of Strategic Studies* 38:1-2, 4-37
[260] Office of the Director of National Intelligence, A Guide to Cyber Attribution, 14 September 2018
[261] Florian J Egloff and Max Smeets, 'Publicly Attributing Cyber Attacks: A Framework', *Journal of Strategic Studies,* no. Ahead of Print (2021): p. 1

international standards, and at different times states may seek different levels of attribution for different purposes. For example, if a state wished to identify an attacker for pursuit through their judicial system, the standard of attribution required will be different from that of wishing to warn another nation more broadly.[262] But the question of the appropriate standards for legal attribution is not yet settled either.

Further, it is in some states' interests to continue to push the narrative that attribution is so complex that states can never really know with total certainty who directed an attack. Thus while the attribution problem is no longer the barrier argued by Clarke and Landau, the lack of agreed international standards means researchers should still consider how individual states approach this issue in order to include the appropriate political context. I argue therefore that attribution is fundamentally a political question, not a technical one, and the current differing approaches by states to the legal standards render these unhelpful as an indicator of state practice.

1.17 'Cyber' deterrence: A confused literature

The difficulties presented so far in this chapter including the complexity of operationalising deterrence requirements in any sphere and the shortfalls of deterrence demonstrated by the nuclear era. And yet it is the particular difficulties presented by cyberspace that best explain the confused state of the literature on the application of deterrence to states' cybersecurity practices. This problem is demonstrated by the confused use of the term 'cyber deterrence'. There is no shortage of strategists who argue against the application of deterrence to cyberspace, most of whom base their arguments on the difficulties presented by the space. Harknett and Goldman argue deterrence is inherently not credible in cyberspace because it based on a threat of use of force, with the operational objective of avoiding operational contact.[263] Jim Chen presents the argument that the unique characteristics of the man-made cyber domain requires 'a new and holistic deterrence strategy', as conventional deterrence was not suitable.[264] Leuprecht et al. also point to the nature of cyberspace as the issue, arguing the persistence of possible attack in cyberspace limits the extent to which deterrence is possible in cyberspace.[265] And Michael P. Fischerkeller argued the nature of constant 'engagement' in cyberspace renders deterrence unachievable, and states should instead pursue theories that accommodate that engagement.[266] But as Sterner argues, the fact that nuclear deterrence was unique to the Cold War and does not translate to cyberspace does not mean deterrence has no value; rather it is an argument for seeking better understanding of how deterrence may operate in cyberspace.[267] I contend these arguments are limited as they are framed by existing deterrence strategies,

[262] John S. II Davis and Rand Corporation, 2017, 'Stateless Attribution: Toward International Accountability in Cyberspace' RR-2081-MS., no. Generic, 2

[263] Richard Harknett and Emily Goldman, 2016, 'The Search for Cyber Fundamentals', *Journal of Information Warfare*, 15:2

[264] Jim Chen, 'Cyber Deterrence by Engagement and Surprise', *PRISM*, 7:2, 101

[265] Christian Leuprecht, Joseph Szeman and David B. Skillicorn, 2019, 'The Damoclean sword of offensive cyber: Policy uncertainty and collective insecurity', *Contemporary Security Policy*, 40:3, 397

[266] Fischerkeller, p. 6

[267] Sterner, 2011, 'Retaliatory Deterrence In Cyberspace', *Strategic Studies Quarterly,* Spring 2011, 77

rather than being based on the core requirements of deterrence as a theory.[268] As Robert Jervis argues, the term 'cyber deterrence' immediately presents a problem – deterrence is a theory, and cyber is merely another means for states to pursue that theory.[269] The conceptual separation between authors who refer to 'deterrence in cyberspace' – the extension of deterrence theory in an attempt to deter cyber-attacks, or 'cyber deterrence' – the use of cyber weapons and capabilities in an attempt to deter all types of unwanted behaviours, changes how authors view success and expectations of deterrence. For example, Libicki categorised cyber capabilities as being part of a broader suite of options that comprises overall US deterrence,[270] but this definition was not agreed upon in the US. The term 'cyber-deterrence' was first used by James Der Derian in a 1994 article which described the deterrent effect network technologies could have on the battlefield,[271] which is a weapons-centric view of deterrence through cyber capabilities. In 2017 Jun Osawa made the reductive argument that because both current and former policy used the terminology 'cyber deterrence', strategists should adopt the term.[272] And even if this term was accepted, the meaning behind it was not. This is evident, for instance, in Tim Stevens' description of cyber deterrence as the 'methods by which states deter adversarial actions in cyberspace'[273] compared to Ewan Lawson's definition as the 'effort to deter malicious actors in cyberspace by whatever method is appropriate'.[274] Thus even within the modern US literature there is still no agreed definition of what comprises cyber deterrence, let alone agreement on whether the term is conceptually helpful.

Here I would argue for the purposes of this thesis that the term cyber deterrence, just like cyber war and cyber espionage, is a misleading and elusive notion.[275] Consider the case of the Shamoon virus, which in 2012 attacked and rendered useless 20,000 computers owned by Saudi Aramco.[276] The attackers are thought to have been non-state actors who operated with the tacit agreement of the Iranian government.[277] Yet how should a state deter a non-state actor? And this is just one example of the challenges facing states attempting to adopt deterrence policy. The literature is also not clear on how successful deterrence in cyberspace should be defined, although this is perhaps not surprising given the difficulty of establishing or measuring deterrence success in the field of deterrence more generally.[278] After all, did a state decide not to pursue a course of action because of a successful deterrence position – or because of other events in the broader strategic context? Morgan characterises this difficulty as the

[268] Healey, 'The Implications of Persistent (and Permanent) Engagement in Cyberspace', p. 8.
[269] R Jervis, 'Some thoughts on deterrence in the cyber era', p. 66
[270] Martin Libicki, Expectations of Cyber Deterrence, p. 54 https://www.wired.com/1994/09/cyber-deter/
[271] James Der Derian, Cyber-Deterrence Wired Magazine 2.09 September 1994
[272] Jun Osawa, 2017, 'The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?', *Asia-Pacific Review*, 24:2, 124
[273] Stevens 148
[274] Ewan Lawson, 2017, 'Deterrence in Cyberspace: A Silver Bullet or a Sacred Cow?', *Philosophy & Technology*, 31:3, 432
[275] 'Cyber conflict and deterrence' Strategic Comments, 22:7, iii-v, September 2016
[276] Ibid
[277] Ibid
[278] Patrick M. Morgan, 2003, *Deterrence Now*, Cambridge University Press, p. xix

more successful general deterrence is, the less traces it leaves.[279] This complexity helps explain why the literature to date has focused on high level theory and has not produced a body of practical evidence to answer the question of usefulness one way or another. Indeed, deterrence theory has been repeatedly examined throughout the twentieth and twenty-first centuries.[280] Further, it has been subjected to comprehensive examination against practical scenarios during the nuclear age.[281]

This suggests that such a practical examination of state deterrence practice should also be possible for cyberspace. On this point Tim Stevens has argued that while a body of cyber deterrence theory had developed after 2007, it had largely failed to translate into concrete policy and strategy.[282] There is certainly a developing body of literature arguing deterrence may have a place in cyberspace. Colin S. Gray may be correct that cyberspace is just another technological construct where states will seek to affect each other' behaviours.[283] Indeed this position seems logical when compared to the earliest principles of deterrence as a fundamentally human endeavour. Nathanial Youd pointed out that if a state can credibly communicate its capability to deny or punish an adversary in cyberspace, the adversary will respond and bargain[284] – classic deterrence behaviour[285] which arguably at least merits examination in the cyber context. And while not a comprehensive answer to the cybersecurity dilemma, Jeffrey R. Cooper makes the case that deterrence at least merits attention as part of an effective and comprehensive security strategy to secure our cyber environment.[286]

But perhaps the strongest argument for considering the role of deterrence theory in cybersecurity is the fact that, despite the contested state of the literature, deterrence theory has been adopted and

[279] Patrick M. Morgan, 1983, *Deterrence: A Conceptual Analysis*, Beverly Hills: Sage Library of Social Science, (revised ed.)

[280] Lawrence Freedman, 2008, 'Strategic Studies and the problem of power', in Thomas G. Mahnken and Joseph A. Maiolo, *Strategic Studies: a reader,* Routledge, 23; and M. Alagappa, 2008, *The Long Shadow: Nuclear Weapons and Security in 21st Century Asia*, Stanford University Press, p. 479; see also Timothy W. Crawford, 'The Endurance of Extended Deterrence: Continuity, Change and Complexity in Theory and Policy', in *Complex Deterrence: Strategy in the Global Age,* 278

[281] Alexander L. George and Richard Smoke, 1974, *Deterrence in American Foreign Policy: Theory and Practice*, Columbia University Press

[282] Tim Stevens, 'A Cyberwar of Ideas? Deterrence and Norms in Cyberspace', *Contemporary Security Policy*, 3:1, 148

[283] Colin S Gray, 'Making strategic sense of cyber power: Why the sky is not falling' *Strategic Studies Institute,* 2013: Carlisle, PA

[284] Nathanial Youd, 'Cyber Deterrence: Is a Deterrence Model Practical in Cyberspace?' From the *2014 Gen. Larry D. Welch Writing Award*, USSTRAATCOM, Junior Division, 49

[285] Joseph S. Nye, 2011, 2011, *The Future of Power*, New York: Public Affairs, 322; see also Martin C. Libicki, 2009, *Cyberdeterrence and Cyberwar,* RAND Project Air Force; Patrick Cirenza, 2015, *An Evaluation of the Analogy Between Nuclear and Cyber Deterrence*, Stanford University, p. ii; Nathanial Youd, 'Cyber Deterrence: Is a Deterrence Model Practical in Cyberspace?' From the *2014 Gen. Larry D. Welch Writing Award*, USSTRAATCOM, Junior Division, 51; David Elliott, 'Deterring Strategic Cyber-Attack', *IEEE Security and Privacy,* September-October 2011, 36-38; and Amir Lupovici, 2019, 'Toward a Securitization Theory of Deterrence: Theory Note', *International Studies Quarterly*, 63, 177-186, 179; Liam Nevill and Zoe Hawkins, 2016, 'Deterrence in cyberspace: different domain, different rules', *Australian Strategic Policy Institute: Special Report*; see also Uri Tor, 2017, 'Cumulative Deterrence as a New Paradigm for Cyber Deterrence, *Journal of Strategic Studies*, 40:1-2, 92-117, p. 92

[286] Jeffrey R. Cooper, 'A new Framework for Cyber Deterrence', *Cyberspace and National Security: Threats, Opportunities and Power in a Virtual World* Derek S. Reveron (ed.), Georgetown University Press2012, p. 105

implemented into cybersecurity policy by a number of states. Regardless of the theoretical debates, it is accepted state practice for the United States[287], Australia[288], the United Kingdom[289], Israel[290], Japan[291], New Zealand[292], South Korea[293], Germany[294], and Finland[295]. Although not a comprehensive list,[296] the act of these states enshrining deterrence in cybersecurity policy demonstrates that deterrence, far from a theory that can be consigned to the history books, is a live strategy. This adoption of deterrence as policy despite the disagreement over its usefulness indicates a promising area for research, particularly because there are multiple nations that have chosen this course. Further, there is more than decade of practice in several cases, providing substantial data for examination of how policy approaches have changed over time. And deterrence appears to be of central importance to these cybersecurity policies, often being listed as a core goal or requirement. Consider Former US President Donald Trump's statements in 2018 that the US would:

> preserve peace and security by strengthening the ability of the US – in concert with allies and partners – to deter, and if necessary punish those who use cyber tools for malicious purposes.[297]

Likewise, Australia has stated it will 'deter and respond to unacceptable behaviour in cyberspace' as a core goal of cybersecurity policy.[298] In 2019 the UK Foreign Secretary Jeremy Hunt argued it is time for a 'new doctrine of deterrence against cyber-attacks in our democracies'.[299] While it is beyond the scope of this research to examine the policy approaches of all these states[300], the existence of them indicates a belief that deterrence has potential value.

1.18 Conclusion: Deterrence in cybersecurity – a common practice

The inclusion of deterrence theory in states' cybersecurity policies indicates that these states perceive the threats posed to their interests through cyberspace as pressing and serious enough to merit significant attention. However, both states and the academic literature disagree over the seriousness of the threat to

[287] 'National Cyber Strategy of the United States of America', September 2018, The White House, US

[288] 'Australia's Cyber Security Strategy 2020', 6 August 2020, Commonwealth of Australia

[289] 'National Cyber Security Strategy 2016-2021', 2016, Her Majesty's Government, UK

[290] 'Israel National Cyber Security: In Brief', September 2017, State of Israel

[291] 'Japan: Cybersecurity Strategy', 27 July 2018, Government of Japan (provisional translation)

[292] 'New Zealand's Cyber Security 2019', 2019, Department of the Prime Minister and Cabinet, NZ

[293] 'National Cybersecurity Strategy', n.d., Republic of Korea: National Security Office

[294] 'Cyber Security Strategy for Germany', February 2011, Federal Ministry of the Interior

[295] 'Finland's Cyber Security Strategy 2019', 3 October 2019, Secretariat of the Security Committee

[296] This author was restricted to strategy documents available in English; it is worth noting that deterrence may be a principle of many non-English strategies and this may be an area of future research significance for scholars with relevant language skills.

[297] 'National Cyber Strategy of the United States of America', September 2018, The White House, US, p.i

[298] Commonwealth of Australia, Department of Foreign Affairs and Trade, October 2017, *Australia's International Cyber Engagement Strategy*

[299] Foreign Secretary Jeremy Hunt 'Deterrence in the cyber age', Glasgow University, 7 March 2019 https://www.gov.uk/government/speeches/deterrence-in-the-cyber-age-speech-by-the-foreign-secretary

[300] The selection of cases for this research is considered in detail in Chapter 2: Methodology.

states' interests through cyberspace, whether a cyber-attack meets the threshold of an act of war[301], and how states should attempt to secure their interests in this arena.[302] These differences are important. As Morgan argues, for deterrence to apply there needs to be a legitimate threat.[303] However as Amir Lupovici also notes, the adoption of the strategy of deterrence is a securitising move – and the very act of creating policies aimed at deterring cyber-attacks may have the effect of alarming adversaries and potentially triggering an arms race which could lead to war.[304] As war is at best ugly, costly and dangerous, and at worst disastrous, it is something for states to avoid; [305] but the literature on whether cyber-attacks could reach the level of acts of war, and definitions of cyber war more broadly, is contested.[306] Stephen Walt argued that activities in cyberspace simply do not meet the threshold of war by any definition.[307] It is certainly true that death or physical destruction of states' interests by a known set of adversaries in a clearly defined war using weapons in cyberspace has not yet occurred.[308] Thus it seems there is an argument that the spectre of 'cyber war' is problematic and misleading – a view supported by Gartzke, who has noted that despite the growing literature on the threat of cyber war, cyber-attacks were unlikely to prove particularly potent in grand strategic terms unless they can impose substantial, durable harm on an enemy, and that in most cases this would need to be accompanied by terrestrial forces.[309] Cyber warfare is thus more likely to have serious impacts when used in conjunction with traditional warfare. The likelihood of such a threat eventuating is difficult to measure, and nothing has occurred in cyberspace so far to meet the level of use of force defined in the 2013 Tallinn Manual.[310] But this uncertainty did not prevent Leon Panetta, former US Secretary of Defense, making repeated statements about the likelihood of a 'cyber Pearl Harbor', something he viewed as a real possibility.[311] Nor did it prevent more than 20 nations having established cyber warfare units as part of their militaries by 2012.[312]

Richard A. Clarke provides some much-needed context to the cyber threat when he argued that cyber threats are hard for states to understand as they do not cause deaths; there is no 'smoking ruin'.[313]

[301] Will Goodman, 2010, 'Cyber Deterrence: Tougher in Theory than in Practice?', *Strategic Studies Quarterly,* 4:3, 103

[302] Erik Gartzke, 2013, 'The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth', *International Security,* 38:2, 41

[303] Patrick Morgan, 1977, *Deterrence: A Conceptual Analysis*, Sage, p.27

[304] Amir Lupovici, 2019, 'Toward a Securitization Theory of Deterrence: Theory Note', *International Studies Quarterly*, 63, 177

[305] Schelling, *Arms and Influence*, p.35

[306] Consider Eric Gartzke's (2013) argument that that cyberwar is the most recent phase in the ongoing revolution of military affairs in 'The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth', *International Security,* 38:2, 41; but also see Will Goodman, 2010, 'Cyber Deterrence: Tougher in Theory than in Practice?', *Strategic Studies Quarterly,* 4:3

[307] Stephen M. Walt, 2010, 'Is the Cyber Threat Overblown?', 30 March 2010, *Foreign Policy*, https://foreignpolicy.com/2010/03/30/is-the-cyber-threat-overblown/.

[308] 'Cyber conflict and deterrence' Strategic Comments, 22:7, iii-v, September 2016

[309] Eric Gartzke, The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth, *International Security,* Vol. 38, No.2 (Fall 2013) p.43

[310] 'Cyber conflict and deterrence', September 2016, *Strategic Comments*, 22:7, iii-v

[311]Eric Gartzke, 2013, 'The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth', *International Security,* 38:2 (Fall 2013), 54

[312] Fred M. Kaplan, 2016, *Dark Territory: The Secret History of Cyber War*, New York: Simon & Schuster, p.4

[313] Richard A. Clarke, Testimony to the Committee on Government Reform, 9

Additionally, it is far from clear that conflict over the internet can actually function as war, and that cyber war should not be considered in isolation from more traditional forms of political violence.[314] If Gartzke is correct that the conventional military balance is the best indicator of where the most important threats exist in cyberspace,[315] then research should be able to examine public statements regarding adversaries in cyberspace and situate these easily within a state's broader known threat context.

But the uncertainty regarding the seriousness of the threats is not necessarily a barrier to deterrence. Deterrence is unique in strategy in that it offers the hope of avoiding conflict. As Knopf argues, if a state attacks or invades a country that could have been contained and deterred, it would pay potentially high and avoidable costs in blood, treasure, and diplomatic friction.[316] Patrick Morgan points out that deterrence gained a great deal of attention during the Cold War, becoming the subject of one of the most elaborate attempts at rigorous theory in the social sciences because of the importance of preventing nuclear war.[317] But he also points out non-nuclear deterrence is complex, subtle and affected by the strategic context.[318]

It would therefore seem then that the complexity of the threat space and uncertainty over whether cyber-attacks reach the threshold of war should not be considered barriers to states seeking to apply or evaluate deterrence. Rather, the complexities and subtleties of deterrence in cyberspace demand attention to preventing unintended consequences, and potentially war. If Morgan is correct that deterrence is a flawed policy instrument, often uncertain or unreliable in its effects,[319] then the question of why states have pursued deterrence for cyberspace becomes pressing as more states consider the most effective policy approaches to securing their interests in cyberspace. The implementation of theory into policy is thus an area where evaluation may provide useful and practical insights into the applicability or otherwise of the theory. Chapter 2 explains how this research will assess the efficacy of deterrence theory as it is expressed within state policy.

[314] Eric Gartzke, 2013, The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth, *International Security,* 38:2, 42

[315] Ibid p. 63

[316] Jeffrey W. Knopf, 'Three Items in One: Deterrence as Concept, Research Program and Political Issue in Complex Deterrence: Strategy in the Global Age', p.32

[317] Patrick M. Morgan, 1977, *Deterrence: A Conceptual Analysis,* Sage Press, p.25

[318] Ibid, p. 60

[319] Morgan, *Deterrence Now,* p.xix

Chapter 2 Methodology

2.1 Introduction

The previous chapter surveyed the literature on cybersecurity and deterrence and identified a lack of evidence-based research into the appropriateness and efficacy of states applying deterrence theory to cybersecurity policies. This chapter now builds on that review to examine how a study of the rationales states use to understand and justify their employment of deterrence in cyberspace strategy might be operationalised. It develops a framework of structured, focused analysis to consider the approaches of states with a defined role for deterrence theory as part of their cybersecurity policies; argues for evaluating these approaches against this framework; and considers how such research might produce findings regarding perceptions of efficacy for the two cases under consideration. The chapter also notes that attempts to generalise from these findings in search of broader implications for deterrence strategy in cyberspace should be approached with caution.

The chapter addresses the design for three stages of data collection (public policy evaluation, contemporary literature review and expert interviews) and overall analysis. In doing so, the chapter develops its case study methodology, explains the logic behind the selection of the US and Israel as cases, and details how each case study is conducted and analysed in subsequent chapters. The chapter considers the expected potential findings, including that the cases under review will be more likely to judge their deterrence efforts a success if their policies: (i) fulfil the three basic requirements of deterrence as a minimum; (ii) are part of a comprehensive cross-domain deterrence strategy; and (iii) are based on a definition of success that allows ongoing cyber-attacks and engagements rather than a zero-sum approach. The chapter concludes with a brief consideration of how such findings may contribute to understanding of cyber strategies, and deterrence more generally.

As detailed in Chapter 1, the applicability or otherwise of deterrence theory to state practices of cybersecurity is deeply contested in existing scholarship, the majority of which focuses on theoretical understanding rather than policy.[320] And while this literature provides important insights and context for how states may choose to approach deterrence in cyberspace (such as the argument for a return to classic deterrence theory; the importance of considering states own definitions of key terms; the lack of currently agreed international norms; and the need to manage the civil-military ownership of assets) it does not provide evidence for the effectiveness of existing state approaches. Yet since Russia's politically

[320] Scholars are deeply divided over the applicability and usefulness of deterrence theory to states' cybersecurity policies. See Colin S Gray, 2013, 'Making strategic sense of cyber power: Why the sky is not falling' *Strategic Studies Institute,* Carlisle, PA; Richard A. Clarke and Robert K. Knake, 2010, *Cyber War: The Next Threat to National Security and What To Do About It,* New York: HarperCollins; Martin C. Libicki, 2009, *Cyberdeterrence and Cyberwar,* RAND Project Air Force; Patrick Cirenza, 2015, *An Evaluation of the Analogy Between Nuclear and Cyber Deterrence*, Stanford University; Liam Nevill and Zoe Hawkins, 2016, 'Deterrence in cyberspace: different domain, different rules', *Australian Strategic Policy Institute: Special Report.*

motivated cyber-attacks on Estonia in 2007 – attacks linked to known strategic goals and specifically designed to retaliate against a decision to relocate a Soviet-era Red Army monument[321] – many states have taken significant steps to increase their cybersecurity. These steps are visible to researchers in the form of public policies such as national security and cybersecurity strategies. As strategies to secure cyberspace became commonplace, the period from 2008–2018 provides 10 years of potential data on state approaches to deterrence through official cybersecurity strategies. There is also a wealth of information available in public media commentary, political statements, legislation and other related public policies such as information technology policies and defence policies and white papers that may help answer the central research question.

2.2 Research problem

This research seeks to understand the extent to which states employing deterrence as a cyberspace strategy consider it successful, and the implications for both cyber strategies and our understanding of deterrence more generally. This thesis began from the puzzle of why states were choosing to pursue the application of deterrence theory despite the fact that its utility is contested in contemporary scholarship. If deterrence is included in states' approaches to cybersecurity in future – and this seems likely based on its popularity – then there is a need for research that explores how effective existing approaches are. If deterrence theory is not helpful for improving perceived cybersecurity policy success, then it should not be adopted in future. In a multi-polar and incredibly complex world, policymakers need evidence-based research to inform the design and implementation of policies, particularly those that may prevent unintended conflict or war.

The argument for such research is not new, nor is it confined to cyberspace – George and Smoke argued in 1974 that it is necessary to try and bridge the gap between theory and practical policy.[322] And Gaddis argued in 2018 that the gap between the study of history and theory was problematic: both were needed if states hoped to align the ends with the means in order to produce effective strategy.[323] But there is also a common theme in much of the literature on deterrence in cyberspace specifically that more research is needed into the link between theory and strategy[324]; how deterrence should, or indeed whether it could, be adapted for cyberspace[325]; and how such attempts should be evaluated.[326] Further, strategists have argued there is a need for research regarding the relationship between deterrence strategy and the actual

[321] This attack was followed by a massive Russian conventional attack against Georgia in 2008, occupying two large break-away regions of the nation (Abkhazia and South Ossetia). See Douglas Mastriano, 2017, 'Putin – the Masked Nemesis of the Strategy of Ambiguity', *Defense and Security Analysis* 33:1, 68-76

[322] Alexander L. George and Andrew Bennett, 2005, *Case studies and Theory Development in the Social Sciences,* MIT Press, p.263

[323] John Lewis Gaddis, 2018, *On Grand Strategy,* Penguin Books, p.23

[324] Wilner, 'US Cyber Deterrence: Practice Guiding Theory', p.247; see also Stevens, 'A Cyberwar of Ideas? Deterrence and Norms in Cyberspace', p.148

[325] Will Goodman, 2010, 'Cyber Deterrence: Tougher in Theory than in Practice?', *Strategic Studies Quarterly*, Fall 2010, 103

[326] Stevens, 'A Cyberwar of Ideas? Deterrence and Norms in Cyberspace', p.150

use of force; Amir Lupovici contends this is vital in the field of cybersecurity as existing theoretical work on deterrence lacks the ability to capture the dynamics that lead actors to adopt, or abandon, deterrence strategies.[327] Yet the reason such research is either limited or does not yet exist is that research on deterrence efficacy in any sphere is difficult.[328] There is an important (but often poorly delineated) distinction between theory as inferred by policymakers, and theory as an abstract divorced from the policy process. Further, the ability to gain perfect knowledge of a state's decision-making processes is important[329] yet complex, and understanding that of an adversary is even less likely.[330] As Morgan notes it is difficult to research something which has not occurred and judge whether such inaction was by design, or mere happenstance.[331] Conducting research on the approaches of states to any policy issue also requires a considerable amount of context in order to give the appropriate consideration to the many factors that influence states' policy approaches and decisions. And the question of how best to investigate the perceived success of states' deterrence approaches in policy is also not new. In considering these factors the case study has proved a useful method for studying deterrence, because it allows for the investigation of complexity.

2.3 Defining the case study: A useful method for the complexity of deterrence

Defining what a case study comprises for this research is important as the term carries different meanings depending on the field. As Schramm noted in 1971, the essence of a case study is that it tries to illuminate a decision or a set of decisions: why they were taken, how they were implemented, and with what result.[332] A case study can be, as Robert Yin describes, an empirical enquiry that investigates a contemporary phenomenon within its real life context, especially where the boundaries between phenomenon and context are not evident.[333] This means they can be exploratory, descriptive, and/or explanatory in nature.[334] George and Bennett offer a more refined way to understand cases in political science, arguing they offer scope for the detailed examination of an aspect of a historical episode to develop or test historical explanations that may be generalizable to other events.[335] Yet it is important to consider both the benefits and limitations of such an approach. While case studies have much to offer as a means of understanding and explaining contemporary international relations, they must be carefully designed to produce findings that have the potential to be generalisable.[336]

[327] Amir Lupovici, 2019, Toward a Securitization Theory of Deterrence: Theory Note, *International Studies Quarterly*, 63, 178

[328] Will Goodman, 2010, 'Cyber Deterrence: Tougher in Theory than in Practice?', *Strategic Studies Quarterly*, Fall 2010, 103

[329] Strategic Comments: Cyber conflict and deterrence, p. 1, Vol 22 Comment 26 September 2016

[330] Payne, The Fallacies of Cold War Deterrence, p. 19

[331] Patrick M. Morgan, 1977, *Deterrence: A Conceptual Analysis*, Sage Press, p.48

[332] Schramm, 1971, cited in Yin 2009

[333] Yin, 1994, p.13

[334] Yin, 2009, p. 6

[335] George and Bennett p. 5

[336] There are several modern reviews of case study methodology: see George and Bennett 2005; Bennett and Elman, 2006 and 2007; Mahoney and Goertz 2006.

George and Bennett also note that the case study approach has come in and out of favour over the past fifty years, but point to the strengths of case studies, particularly that they tend to be strong where statistical methods are weak.[337] Further, as Yin argues, case studies have particular merit in allowing researchers to cope with 'technically distinctive situations in which there are many more variables of interest than data points'.[338]

This is a description which suits the complexity of deterrence in cyberspace well. Here the case study method offers three specific advantages: the ability to consider states' approaches to deterrence decisions to a depth that surveys could not achieve; the fact that the current nature of the topic renders archival analysis unhelpful; and the concern that while a historical analysis would no doubt be interesting it would not necessarily provide the strategic context necessary to inform policy.[339] As a subset of qualitative research methods[340] that aspires to 'cumulative and progressive generalizations about social life and seeks to develop and apply clear standards for judging whether some generalizations fit the social world better than others'[341], the case study is thus well-suited to an attempt at exploring the complexities of states' approaches to deterrence in cybersecurity. The next question is then how to design the most effective case study to ensure it answers the research question.

Here one can consider several different typologies. One of these, offered by Arendt Lijphart, develops categories around atheoretical, interpretive, hypothesis-generating, theory-confirming, theory-informing, and deviant case studies.[342] Harold Eckstein, conversely, has argued for a taxonomy of five types of case study: configurative-idiographic, disciplined-configurative, heuristic, plausibility probe, and crucial.[343] But George and Bennett's return to the purpose of the case study as the defining characteristic is perhaps most useful for political science researchers. George and Bennet define case study methods as including both within-case analysis of single cases, and comparisons of small numbers of cases. They point to the growing consensus that the strongest means of drawing inferences from case studies are those where a combination of within-case analysis and cross-case comparison is used.[344] Although single case studies can be instructive[345], this thesis adopts two cases to allow for both within-case and between case comparison. As these case studies would be more likely to contribute to theory building through cumulative findings if they were tested against the same theory,[346] this research is designed to test two or

[337] George and Bennett p. 5

[338] Robert K. Yin, 2009,*Case Study Research: Design and Methods*, 4th ed., vol. 5., Los Angeles, California: Sage Publications, p.15

[339] Ibid, p. 9

[340] Bryman 2009, p. 67-68, see also John Gerring, *Case Study Research: Principles and Practices*, (New York: Cambridge University Press, 2007), https://doi.org/10.1017/CBO9780511803123;

[341] George and Bennett, *Case Studies and Theory Development in the Social Sciences*, p. 19

[342] Arend Lijphart, 'Comparative Politics and the Comparative Method', *The American Political Science Review* 65, no. 3 (1971): 691, https://doi.org/10.2307/1955513.

[343] H. Eckstein 'Case Studies and Theory in Political Science' in Fred I. Greenstein and Nelson Woolf Polsby, *Handbook of Political Science*, (Reading, Mass: Addison-Wesley, 1975), pp.96-123

[344] George and Bennett, *Case Studies and Theory Development in the Social Sciences*, 18.

[345] Ben Willis, 'The Advantages and Limitations of Single Case Study Analysis', *International Relations*, n.d., 7.

[346] George and Smoke argue for this approach in *American Foreign Policy* p. 93

more cases against the most basic requirements of deterrence theory. Further, given that the most instructive case studies are those that include more than one information source, and preferably multiple sources, to triangulate[347] and provide depth for findings, this thesis adopts an exploratory research design that uses multiple data sources, including in-person interviews.[348] One clear limitation of including personal views, or verbal reports of events, is that although they may be rich, such reports often can be inconsistent[349] or only loosely anchored to the social and historical context that created them.[350] But the inclusion of alternative data sources can mitigate this criticism, as can the inclusion of multiple view points on the same event.[351] Here, structured focused comparison stands out as a simple yet clear framework for considering the role and success of deterrence in cybersecurity policy.

2.4 Structured focused comparison

Structured focused comparison is geared around general questions that reflect the research objective, and these questions are asked of each case to standardise the data collected, making systematic comparison and cumulation of the findings of the cases possible.[352] It is essentially the use of a well-defined set of theoretical questions or propositions to structure an empirical inquiry on a particular analytically defined aspect of a set of events.[353] The method was presented in George and Smoke's 1974 *Deterrence in American Foreign Policy: Theory and Practice*, a critical examination of deterrence theory and strategy applied in American foreign policy since the end of World War II. [354] Adopting the structured focused comparison methodology, George and Smoke used 11 case studies to demonstrate the problematic nature of many of the assumptions on which deterrence rests.[355] This work emphasised the limitations of abstract deductive theory and argued that both explanatory theory and policy-relevant theory required conditional generalisations that were context dependent and informed by history.[356] Further, this type of comparison enabled a more discriminatory analysis of the effectiveness of deterrence,[357] as well as the systematic

[347] Yin, *Case Study Research: Design and Methods*,:15.

[348] Matthew David and Carole D. Sutton, 2011, 'Social Research: An Introduction', in *Social Research: An Introduction*, 165-66; see also Arch G. Woodside, 2010, *Case Study Research: Theory, Methods, Practice,* Emerald Group Publishing, p.6; John Van Maanen Ed, 1979 'Reclaiming Qualitative Methods for Organizational Research: A Preface', ed. John Van Maanen, *Administrative Science Quarterly,* 24:4, 542

[349] E.J. Arnould and M. Wallendorf, 1994, 'Market-Oriented Ethnography – Interpretation Building And Marketing Strategy Formulation', *Journal of Marketing Research,* 31:4, 484-504

[350] Wolf, 1990, p. 351

[351] See Webb & Weick, 1979; Webb, Campbell, Schwartz, and Sechrest 1966.

[352] George and Bennett, *Case Studies and Theory Development in the Social Sciences*, 67.

[353] Jack S. Levy, 2008, 'Deterrence and Coercive Diplomacy: The Contributions of Alexander George', *Political Psychology,* 29:4, 537–52

[354] Smoke and George p.2

[355] The abstract deterrence model was based on seven propositions which aimed to generate knowledge through a systematic consideration of historical cases of deterrence. See Smoke and George Chapter Three: The Normative Use of the Abstract Deterrence Model.

[356] Jack S. Levy, 2008, 'Deterrence and Coercive Diplomacy: The Contributions of Alexander George', *Political Psychology,* 29:4, 537–52

[357] Alexander L. George and Andrew Bennett, 2005, *Case studies and Theory Development in the Social Sciences,* MIT Press, p.85

comparison and cumulation of the findings of the case studies.[358] George and Smoke argued this method helped address the common issue with single case studies: while single case studies produced some useful insights into the deterrence approaches of states, the variation in how they addressed deterrence questions and the employment of different decision-making models meant their findings did not cumulate.[359] The clear similarities between deterrence in the foreign policy field and this thesis makes it useful for evaluating deterrence. The interest in deterrence theory as a potential mechanism for policymakers to increase or improve cybersecurity has proved resilient – it has not only been adopted by several states into policy as previously demonstrated, but has also been maintained and regularly updated over a period of years.

2.4.1 Operationalising the method: Determining deterrence requirements

However, in order to test the extent to which states employing deterrence as a cyberspace strategy consider it successful, this research must go beyond a state's own assessments of success or failure. While such assessments are interesting for comparison, and are included in this research, they vary widely across cases. As outlined in Chapter 1, definitional problems are common in the field of deterrence, resulting in inconsistency across states' policies.[360] This research could not therefore expect to compare two definitions of deterrence success and find that both contained the same (or even similar) ideas about what that success might look like, or what elements of policy had produced or contributed to it. This would result in findings which would be unlikely to be generalisable. Further, if states took different approaches to operationalising deterrence theory this would cause variations between states, meaning a single case would be insufficient. And comparing a state's approach to its own ideas about operationalisation of theory, while interesting, also would not produce cumulative findings. Thus, this thesis seeks instead to identify elements that could be considered in relation to both state's approaches, and that could equally apply to multiple cases to produce within-case analysis over time. And, as noted in Chapter 1, there are three themes that are consistently described as being the most basic requirements for the operationalisation of deterrence theory into policy: capability, credibility, and communication.[361] Assessing state practice against these requirements enables an exploration of how states practices align with, or differ from, theory and potentially allows for cautious inferences on the utility of that theory.

While different authors have expressed these basic, or core, requirements in differing language and to different levels of detail, confining this research to this seemingly simple operationalisation of deterrence requirements ensures that it is both able to be repeated, adopted to assess other cases, and sufficiently detailed to be measureable. As a counterpoint here we can consider Ewan Lawson's broad view of

[358] Ibid p.67

[359] Ibid p.93

[360] Consider the example of French policy, where the term for 'deterrence' specifically refers only to nuclear deterrence; policy discussions with French counterparts on deterrence for cyberspace require substantial translational effort.

[361] Morgan 2003

successful deterrence requirements for cyberspace as having 'both physical and cognitive elements'.[362] While this view has merit, attempting to measure such elements would be extremely difficult as they are broad enough to be almost all-encompassing across a society. Another alternative can be found in Will Goodman's eight deterrence components for cyberspace (an interest, a deterrent declaration, denial measures, penalty measures, credibility, reassurance, fear and a cost-benefit calculation).[363] However Goodman's list is unnecessarily complex, conflating the core requirements with the methods used to create those requirements, and thus is not conceptually helpful for observing deterrence in cybersecurity policy. Hence, returning to the three basic requirements provides a suitable balance between a measurable and manageable level of detail for comparable analysis; and indeed most descriptions of ideas about deterrence success for cyberspace include a combination of these terms.[364]

Considering how to best operationalise assessing the requirements for deterrence as part of cybersecurity is difficult due to competing ideas and definitions, but not impossible, particularly if researchers consider each state's approaches on its own merits. In order to understand the extent to which states consider their approach to deterrence successful, it is necessary to understand how each state defines, develops, and delivers these requirements through government policy. This research thus considers within individual case study chapters each state's definitions of deterrence for cyberspace, as well as its definitions of capability, credibility and communication, as evidenced through published policy. As an example of the utility of capability, credibility and communication it is instructive to recall Aaron F. Brantly argument that the presence of will in the absence of capability is nothing more than bluster. [365] Thus the development of capabilities is necessary for credibility, and expenditure on such capabilities indicates the intent to build credibility. Further, states may categorise their own measures differently, or across multiple categories: the development of a cyber weapon is a capability; when used against an adversary it may influence credibility and communicate intent; when possession is made public it is a tool of communication, further enhancing credibility, or potentially damaging credibility if it is not used in line with a state's communicated policies.

As deterrence approaches must by their nature be sufficiently public in order to be successful, it is possible to determine at least the essence – and in some cases, great detail – of a state's deterrence approach from its public policy. As an example, we can examine a state's visible efforts to create capabilities, which are usually defined in military terms.[366] Morgan described such capabilities as the ability of a state to do unacceptable damage, having proper forces for that purpose, and have the opponent believe the will to carry out that threat exists.[367] This belief is central for credibility. Morgan argues that

[362] Ewan Lawson, 2017, 'Deterrence in Cyberspace: A Silver Bullet or a Sacred Cow?', *Philosophy & Technology*, 31:3, 432

[363] Goodman, 'Cyber Deterrence: Tougher in Theory than in Practice?', 105

[364] Maj Lee Hsiang Wei, The challenges of cyber deterrence, Singapore Journal of Armed Forces vol 41. No 1 p. 13

[365] Aaron F. Brantly, Democracy and Security, p.212

[366] Morgan, *Deterrence Now*, 89.:15.

[367] Ibid 89.:16.

what deters is not the threat, but that the threat is believed.[368] Credibility in turn then relies on effectively communicating a state's commitment.[369] As effective communication of deterrent messages is difficult, deterrent messages and postures need to be carefully crafted.[370]

2.4.2 Defining the case

The next step is to identify the class of which the cases to be studies are instances.[371] The cases in this study are instances of states' deterrence approaches as expressed in cybersecurity policy over the designated period from 2008 to 2018. As it is necessary to bound research projects temporally,[372] I selected a 10-year period that would ensure this research would go beyond an examination of deterrence approaches in cyber strategies at a single point in time, to consider their evolution in the context of significant technology changes, domestic political shifts, and international cybersecurity trends. A 10-year period provides a reasonable span of government approaches without becoming unwieldy, and the period from 2008 provides a decade of empirical experience through which we can evaluate the practices of states.[373] In terms of the number of cases to evaluate, for a study of this type it would be difficult to compare a large suite of cases. As the claim of any thesis to significant theoretical insight is best demonstrated by a wealth of evidence that is both complementary as well as facing significantly different threats and challenges. Hence two cases are identified to provide both the data and the depth to produce rich, comparable findings.

2.4.3 Case selection

An acknowledged requirement for good case study design is that they are considered and purposeful. George and Bennett emphasise the need for selection guided by the research objective and strategy;[374] while Yin argues for selecting cases that will illuminate the research questions.[375] Yet while careful case selection is important, it is also necessarily something of an art. In this thesis I have confined the research to cases that faced direct, active and serious cyber threats, thus ensuring that their deterrence policies for cyberspace were tested by these threats to their interests. The initial search for potential cases showed some states have considered the importance of cybersecurity policy as part of national security or strategy more broadly, but do not face a direct, high-level threat from state actors. For example, Papua New Guinea makes specific mention of the need to deter cyber crime in order to achieve the most basic level of cybersecurity, but does not face a serious and active state-directed cyber threat.[376] Although all states

[368] Ibid 89.:15.
[369] Ibid 89.:17.
[370] Ibid 89.:15.
[371] George and Bennett, *Case Studies and Theory Development in the Social Sciences*, p.69
[372] Robert K. Yin, 2018, *Case Study Research and Applications: Design and Methods,* 6th ed., Sage, p.31
[373] Emily Tamkin, 27 April 2017, '10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?', *Foreign Policy*, https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/.
[374] George and Bennett, *Case Studies and Theory Development in the Social Sciences*, p. 69
[375] Yin, *Case Study Research: Design and Methods,* p. 26
[376] 'National Cybercrime Policy of Papua New Guinea' July 2014, Government of Papua New Guinea

face some level of threat to national security through cyberspace, this level varies widely and selecting states that have active and sustained threats against them from significant and technologically advanced adversaries, as opposed to opportunistic or accidental threats, makes it more likely that the impacts of any deterrence measures will be visible and potentially measurable.[377]I identified the presence of a detailed publicly identified deterrence approach as part of states' cybersecurity strategies between 2008 and 2018 as the essential first selection requirement. This requirement produced the eight available cases. (see Table 2.1).

Table 2.1 States with a public role for deterrence in cybersecurity policy[378]

State	Primary policy document
United States of America	National Cyber Strategy of the United States of America, September 2018[379]
Commonwealth of Australia	Australia's Cyber Security Strategy 2020[380]
United Kingdom	National Cyber Security Strategy 2016–2021[381]
State of Israel	Israel National Cyber Security Strategy – In Brief[382]
Commonwealth of New Zealand	New Zealand's cyber security strategy 2019[383]
Republic of Korea	National Cybersecurity Strategy[384]
Japan	Cybersecurity Strategy 2018 (provisional translation)[385]
Federal Republic of Germany	Cybersecurity Strategy for Germany[386]
Republic of Finland	Finland's Cybersecurity Strategy 2019[387]

As discussed in Chapter 1, the preliminary literature review identified eight states (listed above) which had a publicly identified deterrence approach as part of their cybersecurity strategy. In addition to requiring deterrence as a central component of cybersecurity policy, the cases needed to have a well-developed approach to national security strategy that was publicly available and covered the 10-year period identified. States that identify an explicit role for deterrence theory are necessarily states with advanced

[377] Joseph S. Nye, 2019, 'Deterrence in Cyberspace', *The ASPI Strategist* [blog], p.49
[378] As at 11 November 2020
[379]'National Cyber Strategy of the United States of America', September 2018, The White House, US
[380] 'Australia's Cyber Security Strategy 2020', 6 August 2020, Commonwealth of Australia
[381] 'National Cyber Security Strategy 2016-2021', 2016, Her Majesty's Government, UK
[382] 'Israel National Cyber Security: In Brief', September 2017, State of Israel
[383] 'New Zealand's Cyber Security 2019', 2019, Department of the Prime Minister and Cabinet, NZ
[384] 'National Cybersecurity Strategy' (Republic of Korea: National Security Office, n.d.).
[385] 'Japan: Cybersecurity Strategy', 27 July 2018, Government of Japan (provisional translation)
[386] 'Cyber Security Strategy for Germany' (Federal Ministry of the Interior, February 2011) Germany
[387] 'Finland's Cyber Security Strategy 2019', 3 October 2019, Secretariat of the Security Committee, Finland

national security policies and this may potentially skew the applicability of the research findings towards states with similarly advanced national security.[388]

Having adopted the framework of basic deterrence, the thesis utilises a 'most-different' case design to produce its findings. In considering states with advanced cybersecurity strategies, there are remarkable similarities between some states' policy approaches, particularly between the nations in the 'Five Eyes' grouping (the US, UK, Canada, Australia and New Zealand).[389] A functional comparison of the cybersecurity strategies of these nations would thus not be likely to generate findings that would have merit outside of that group, reducing the contribution to theory that the research may otherwise be able to make. This study thus deliberately includes only one state from the Five Eyes group. In considering which Five Eyes nation to include, Australia and New Zealand were excluded on the grounds that while both had the relevant strategies required, neither nation had developed a substantial literature on deterrence theory and its role in cybersecurity.[390] In considering the US and the UK, I found that while both had sophisticated strategies and a significant literature, the literature from the US was more advanced and thus was more likely to provide material sufficient to illuminate the research questions.[391] Indeed, the US has a rich history of leading deterrence theory development and directly applying that theory throughout the Cold War. Further, the US committed early to deterrence in cyberspace, and US scholars have produced the majority of the literature on the topic, making it a leader in the field – both in practice as well as in terms of intellectual contributions. Further, within the abundance of policy and literature one can find numerous significantly contrasting views on deterrence, which further underscores the potential utility of the US as a case.

With the US selected as the first case, which out of the remaining states of Finland and Israel provide for the most useful comparison? Each nation faces active and serious cyber threats, and both offered experiences outside of the Five Eyes. This was an important consideration to facilitate explanatory richness for two reasons. Firstly, although the US met the case study requirements outlined above, cases with strong strategic weight could be more likely to achieve deterrence in cyberspace through factors other than its cybersecurity policies. Secondly, the inclusion of a smaller state that lies outside the Western states made it more likely that findings regarding deterrence success or failure could be generalised. Both Finland and Israel offer research data through their public policies; have a relevant domestic literature on deterrence in cyberspace; and are of similar strategic weight (although it is worth noting Finland does not

[388] The Republic of Korea and Japan were excluded due to the authors' inability to speak Korean or Japanese.
[389] Canada is a partial exception - their cybersecurity policy makes only limited references to deterrence for cybersecurity. See 'National Cyber Security Strategy' Canada and Sécurité publique Canada (2007), *National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age*, 2018; see also Andrew O'Neil, 2017, 'Australia and the "Five Eyes" Intelligence Network: The Perils of an Asymmetric Alliance', *Australian Journal of International Affairs,* 71:5, 529-43.
[390] Further, this researcher is a current member of the Department of Prime Minister and Cabinet for the Australian Public Service; a role which included providing direct input into iterations of Australia's Cyber Security Strategy. The inclusion of Australia as a case study may have represented a conflict of interest.
[391] Yin, *Case Study Research: Design and Methods*, p. 26

have nuclear weapons). However, Israel's deterrence policy is further developed than Finland's and its literature on the topic is significantly more advanced.[392] For these reasons, the second case explored by the thesis is Israel.[393] Israel was also an early adopter of deterrence theory in cybersecurity policy, and publicly proclaims its policies to be broadly effective.[394] But similarly to the US, although Israel has a long-standing commitment to the doctrine of deterrence, there is disagreement over its perceived effectiveness.[395] As a state with a broader experience of deterrence, Israel's doctrine has evolved over many decades as a response to various kinds of threats.[396] And its strategy in cyberspace has also been challenged by both state and non-state actors in recent years, providing much data to review.[397] More generally, Israel's turbulent history, its ongoing experience with kinetic warfare, and existential struggle for existence have produced a strategic culture which demands a forceful military response to attacks.[398] This approach to the use of force, particularly in relation to deterrence, provides an excellent opportunity to test the application of deterrence theory in cybersecurity practice.

2.5 Research design

The research design aims to produce findings into whether a deterrence approach that met the basic deterrence requirements was considered more successful than one that did not. By examining the declared deterrence approaches of the two cases against this classical deterrence framework, the research expects to generate several different types of expected findings. First, it allows the identification of how closely the cases approaches aligned with this framework, and whether states' approaches were balanced across the three requirements or emphasised some requirements over others. This type of finding helps provide context as to whether what states argue is deterrence policy in fact contains the key requirements of deterrence, or whether a state is using the term 'deterrence' to mean something else entirely. Second, it allows a careful examination of a state's perception of success or failure. If a state had an approach that contained a balanced approach to the three requirements and was considered a deterrence success then

[392] Lupovici, 'Toward a Securitization Theory of Deterrence', p. 177

[393] Although the cases selected produce policy documents in English and have English as at a minimum the second official language, there was nevertheless a risk that key concepts could be mistranslated or misunderstood. For example, public debates and narratives regarding defence policy in Israel are mainly in Hebrew, which potentially limits the lessons available to international observers. This research sought to mitigate this risk through confirming the perceived approaches throughout the expert interviews, and through inclusion of the contemporary literature, the majority of which scholarship is published in English.

[394] Lior Tabansky, 2016, 'Towards a Theory of Cyber Power: The Israeli Experience with Innovation and Strategy', in *International Conference on Cyber Conflict, CYCON*, vol. 2016-, pp.51-63

[395] Asher Arian, 1995, *Security Threatened: Surveying Israeli Opinion on Peace and War*, Cambridge Studies in Public Opinion and Political Psychology, Cambridge: Cambridge University Press; see also Gawdat Bahgat, 2020, 'Iranian-Israeli Confrontation: The Cyber Domain', *Middle East Policy,* 27:3, 115-24

[396] Amos Malka, 2008, 'Israel and Asymmetrical Deterrence', *Comparative Strategy,* 27:1, 2; see also Thomas Rid, 2012, 'Deterrence beyond the State: The Israeli Experience', *Contemporary Security Policy,* 33:1, 124; Dag Henriksen, 2012, 'Deterrence by Default? Israel's Military Strategy in the 2006 War against Hizballah', *Journal of Strategic Studies,* 35: 1, 113; Dmitry (Dima) Adamsky, 2017, 'The Israeli Odyssey toward Its National Cyber Security Strategy', *The Washington Quarterly,* 40:2, 113-27

[397] Malka, 'Israel and Asymmetrical Deterrence', *Comparative Strategy,* 27:1, 1

[398] Dag Henriksen, 2012, 'Deterrence by Default? Israel's Military Strategy in the 2006 War against Hizballah', *Journal of Strategic Studies,* 35:1, 96

the research would indicate that deterrence theory may have value as part of cybersecurity strategies. However, if the approach aligned with theory and was considered a failure, then deterrence theory may need to be either adapted for the cyber environment, or different theories of security considered. The next step is to carefully consider the types of data that could provide insight into each case's approach to each requirement. The next section of this chapter details the three phases of data collection and explains how each phase contributes to answering the research questions.

2.5.1 Data collection: Policy review

As we cannot understand deterrence without considering how governments enact decisions through policy,[399] the first stage of each case study contains a review of each state's approach to deterrence historically, before a more detailed review of the approach over the specified time period. For the purpose of this research, policies are defined as statements of intent by states that are implemented by procedure or protocol.[400] I examine such policies in the form of national security strategies, cybersecurity strategies, White Papers, stated defence and foreign policy, and other relevant policy documents that shed light on each case's approach to cybersecurity policy.

Reviewing public deterrence policy against basic deterrence theory allows the examination of whether the state's policy identifiably includes those three requirements (i.e., capability, credibility and communication), and whether this varied over the period under consideration. It further allows for consideration of the importance of cybersecurity relative to other threats.[401] Given the definitional issues in the field of cybersecurity in general, and deterrence for cybersecurity in particular, the next step was to consider each case's deterrence approach in their own words through these published government strategies. I then constructed a brief policy timeline to allow for exploration of broader impacts related to technological advancement and key events in cybersecurity which shifted many state's practices. Reviewing public policy also provides important context for each case's definition of key terms as well as findings into whether the approach had a balanced approach towards capability, credibility and communication.

2.5.2 Data collection: Contemporary literature

As reviewing public policies in isolation is unlikely to provide definitive answers on efficacy, the next research step is to situate the policies within each case's broader national security approach through a review of its contemporary academic literature.[402] This is an essential step for establishing the relative importance and perceived efficacy of these policies. By examining this literature for each case, the case studies situate policy developments against each state's relevant conceptions of deterrence. This phase begins to identify why policy practices align with or differ from theory. It explores how the requirements

[399] Morgan, *Deterrence: A Conceptual Analysis*, p.48

[400] Paul Williams, 2008, *Security Studies: An Introduction*, London: Routledge, p.63

[401] Lupovici, 'Toward a Securitization Theory of Deterrence', p. 179

[402] George and Bennett, *Case Studies and Theory Development in the Social Sciences*, 97.

of classic deterrence theory, both separately and as a whole, are treated in the literature, and considers the main areas of contention. The research then grouped these areas of contention under three main themes – identified as defining the problem for which deterrence was the answer, defining deterrence, and delivering deterrence (see Table 2.2). These areas of contention in the literature provide further framing for how and why states conceptualised deterrence in cyberspace, the extent to which this met the basic deterrence principles and the resulting impact on policy development and evaluation.

Table 2.2 Contested themes in the literature

Broad theme	Sub theme
Defining the problem	How states define the threat to their interests in cyberspace; whether cyber should be considered a domain of warfare; how and when states should attribute attacks
Defining deterrence	How states define deterrence, what is considered success for that state, what is the role for nuclear or broader deterrence or whether cyber deterrence is a stand-alone strategy
Delivering deterrence	The role of the military in delivering deterrence, the drive for superiority, offensive activity and whether this can be considered part of deterrence

2.5.3 Data collection: Expert interviews

The third and final phase of data collection needed to go beyond each state's public policies and academic literature in order to find evidence for not just states' policy approaches, but the evaluations of those approaches and the reasoning behind why that state had defined, developed and delivered deterrence policy in the way they had. Hence the thesis employs expert interviews featuring cyber strategists and national security policy experts as informants to gauge the efficacy and rationale for the respective cyber deterrence measures adopted by the US and Israel. As the potential pool of people with such experience from each nation is actually quite small and concentrated in a highly specialised group of people, 10 interviews per case are used to allow for data saturation without excessive repetition.

The interviews are designed to gain insight into the justification for and perceived efficacy of each traditional measure of deterrence. I sought participants with broad experience and differing roles related to their case's declared cybersecurity policy to mitigate the possibility that participants may have had a tacit agreement to state their own case's policy was considered effective, even if this was perhaps not their personal view.[403] Given the relatively low number of cybersecurity professionals influencing government policy in both cases, I sought to interview as broadly as possible in that limited policy space. I identified

[403] Ibid

professionals across three broad categories of cyber professionalism: current and former government service employees, researchers from academia and think tanks, and industry representatives. The participants all had significant influence on cybersecurity policy development and evaluation. Participants were not confined to one category since the generally small number of people in each case with relevant experience meant that participants often sat across two or more categories of employment. In some cases, the full role and background were not clear until the interview had commenced, and in others their roles remain classified.

For each case, I identified relevant authors, commentators and policymakers and sent initial introductions by email, following up with personalised approaches. In the case of Israel, I attended a major national cyber conference before commencing interviews in order to confirm key concepts and themes were well understood, and to ensure I was seeking interviews with the most appropriate people. This additional step helped mitigate some of the misunderstandings potentially caused by the language barrier and allowed for identification of several further participants recommended through word-of-mouth introductions.

The research followed the approved Ethics plan granted by the ANU for the study.[404] Participants were offered anonymity to encourage open sharing of views, including those which were unflattering about their state's approach to deterrence.[405] Participants are identified by a simple numerical code, and the full list of participants is available to examiners only under Appendix 1. In addition to the numeric code, each participant's broad area of expertise is noted. Participants signed ethical disclaimers prior to participating, and most participants agreed to be recorded for clarity.[406] The interviews were conducted in a range of locations chosen by participants and varied in length from one hour to several hours. The interviews were transcribed, and all transcripts saved in secure offline digital storage.[407] In two cases interviewees followed up to request that certain sections of interviews were redacted due to potential political sensitivities. The relevant sections were immediately removed and do not form part of this research.

The expert interview participants were asked a series of general questions designed to generate views in three specific areas of deterrence as an overall conceptual approach; the case's ability/effort against each classical deterrence requirement; and perceptions of their state's overall success or failure in creating

[404] Ethics approval number: 2019/066, Granted 20 May 2019, ANU

[405] In transcribing interviews and quoting participants, quotes are verbatim. For Israeli participants in some cases the grammar and syntax is slightly different than for native English speakers, however the quotes were presented as stated to preserve accuracy. Further, Israeli participants regularly expressed views regarding their identified adversaries in the region using language that could be considered as racist. These views, where relevant, are included to inform an understanding of the conception of the threat space. However, the inclusion of these views should not be considered as representative of the researcher, The Australian National University or the Australian Public Service.

[406] In each case study one participant declined to be recorded; both of these participants allowed handwritten note-taking.

[407]Robert K. Yin, 2018, *Case Study Research and Applications: Design and Methods*, 6th ed., Los Angeles: Sage Publications, p.43

deterrence.[408] Given the difficulty of evaluating deterrence in the abstract[409] and in order to allow for comparison within and each case, the research design was semi-structured, using the snowball technique, with open-ended questions that deliberately facilitated an open style of conversation where participants felt comfortable sharing broad insights (see Table 2.3).[410] The interviews also included questions specific to each case, to allow for within-case comparison (see Table 2.4). Participants were also allowed significant scope to provide additional input or identify other key areas they saw as important for understanding their state's approach to deterrence in cybersecurity policy.

[408] Bryman, *Social Research Methods,* p. 47

[409] Dorothy E. Denning, 2015 'Rethinking the Cyber Domain and Deterrence', *Joint Force Quarterly*, 77, 12

[410] George and Bennett, *Case Studies and Theory Development in the Social Sciences*, 69.

Table 2.3 Interview questions: both cases

Theme	Question	Link to structured focused comparison
Defining deterrence; framing success	How does your government define deterrence for cyberspace? Is it clearly defined?	Evidence for whether the definition contains elements of the three requirements of classic deterrence. Establishes case specific definition.
	How does your government define deterrence success?	Evidence of success definition: and whether it matches expected definition of success, i.e. zero-sum or resilience focused, or a combination. Establishes case specific definition.
	How do you know your deterrence is working in cyberspace?	Evidence for states indicators of success – whether these are aligned with classic deterrence definition of success.
	How has the definition of deterrence changed over time? Is it part of an integrated deterrence approach, or separate/stand-alone?	Evidence for whether the definition emphasised one requirement more than another at any point, whether definitions have become more or less comprehensive.
	Is the use of force part of deterrence? How important are physical consequences?	Evidence for whether use of force matches states deterrence approach.
	Is it possible to deter cyber-attacks? Why/Why not?	Evidence for expectations of potential success.
Framing deterrence: how important is the strategic context?	What was the strategic context for the first introduction of deterrence into national policy in (your state)?	Evidence for external influences on the adoption of deterrence policy for cybersecurity.
	What role does domestic politics play in deterrence?	Evidence for internal influences on the adoption of deterrence policy for cybersecurity; context for credibility and communication measures – are they deigned for internal or external audience?
	How important is written policy? What role does written policy play in states strategy?	Evidence for the importance of policy; how much researchers should rely on written policy as an indicator of states intent.
	How important is cybersecurity broadly to your national security strategies?	Evidence for the perceived seriousness of the cyber threat to national security; evidence for the importance of deterrence.
	What area of government has responsibility, and how has this shifted over the case study?	Evidence for governance of deterrence; indicators of credibility and capability.
	Who is your state trying to deter in cyberspace – state or non-state actors? Has cyber changed the threat space?	Evidence for the perception of the threat, and whether cyber has changed the potential threat actors – essential knowledge for deterrence

	Deterrence was first introduced in your official policy in (year) was this a new concept, or was it previously implied under other policy areas?	Evidence for how historical experience of deterrence affects ideas about success and implementation.
	Was the introduction of the deterrence concept contentious? Why? Was there bipartisan or multi-party party support?	Evidence for the role deterrence has within society, and consideration of how this affect expectations of success.
	Was the concept well understood?	Evidence for the expectations of deterrence.
Delivering deterrence	How does your state approach establishing capability? What does your state define as capabilities in this space?	Evidence for comparison to deterrence requirements; case specific definition.
	How does you state approach establish credibility? How effective is it in establishing credibility?	Evidence for comparison to deterrence requirements; case specific definition.
	How does your state communicate its deterrent intent and expectations? How effective its communication for deterrence?	Evidence for comparison to deterrence requirements; case specific definition.
Perceived efficacy: Outcome on national security:	Does your state judge its deterrence approach a success? Why/why not?	Evidence for judgments of deterrence success and reasoning behind those judgments.
	What other factors could have contributed to success or failure, i.e. stability, rationality, grand strategic power?	Evidence for success and failure judgments being influenced by factors external to deterrence.
	What evidence do you see to support your ideas?	Evidence of expectations of success.
Contested topics	Does your state consider cyber a domain? Why/Why not?	Evidence into expectations of success
	Attribution – how does your state approach the attribution issue?	Evidence for how attribution influences the three deterrence requirements.
	Does cyberspace represent a new era, requiring new strategy – or is existing deterrence strategy adaptable?	Evidence for states broader views on how cyber is shaping strategy.
	Does nuclear deterrence have any useful lessons for deterrence in cyberspace?	Evidence for the influence of nuclear deterrence on deterrence for cybersecurity.
	How important is to have known acceptable behaviours in cyberspace? Is there a role for norms? Do you view your states behavior as creating new norms?	Evidence for states views on norms in cyberspace.

	Responses to cyber-attacks – should they be proportionate? Cross-domain? Kinetic?	Evidence for expectations of deterrence in cybersecurity, either as an integrated or stand-alone policy.
	How important is superiority?	Evidence for comparison to deterrence requirements.
	Do you see a risk of escalation in cyberspace? If so, is this risk linked to deterrence policies?	Potential evidence for counterfactual – arms race theory.
	Has your government succeeded in deterring cyberattacks? Why/Why not? How could your state do deterrence better?	Evidence for views on success and gaps in states approaches.

Table 2.4 Additional interview questions: Unique to cases

Case	**Question**	**Link to structured focused comparison**
Israel	Can you explain the reasoning for the kinetic response to the 2019 Hamas cyber-attack?	Use of capability/ importance of use of capability for cross-domain deterrence
US	Why is the US pursuing collective attribution? What is the role for allies and partners in US deterrence?	Influence on ideas of success

The aim of the interviews was to examine expert perceptions of why deterrence policies were considered effective or otherwise, such as the idea that deterrence in cyberspace was merely part of a state's broader deterrence posture – and thus whether the policies themselves were largely irrelevant to creating positive deterrence in cyberspace outcomes.[411]

2.6 Conclusion

This chapter has examined how a study of the extent to which states consider their employment of deterrence into cyberspace could be operationalised through a structured focused comparative analysis. It argues for the use of states own policies and literature to frame each case's deterrence approaches against the basic deterrence requirements. The chapter notes the types of expected findings, and explains how the use of policy review, literature analysis and expert interviews will provide evidence for the extent of perceived success of states approaches to deterrence in cybersecurity. The next chapters apply this analysis to the individual cases, presenting detailed within-case analysis. Chapter 5 then presents a cross-case analysis which compares each case's own experiences and perceptions against the classic deterrence requirements.

[411] Yin, *Case Study Research and Applications: Design and Methods*, p. 43.

Chapter 3 Israel's deterrence in cyberspace: The risks of 'success'

3.1 Deterrence in a contested environment

This chapter explores how and why Israel chose to apply and maintain a commitment to deterrence as part of its cybersecurity policies throughout 2008 and 2018. It does this by considering how Israel defines the threat against it in cyberspace, why it defined deterrence as a solution to that threat, how Israel has chosen to deliver deterrence, and the potential risks in its approach. The chapter begins by briefly considering the historical importance of deterrence to Israel, before exploring the implications of this experience on its constructions of deterrence in cyberspace. It notes how and why Israel's cumulative approach differs from the classic Western definition of deterrence, and considers how Israel has attempted to mitigate the issues of applying deterrence to cyberspace identified in the literature.

The chapter then explores the evolution of Israel's cybersecurity policies and perceptions of its success through primary and secondary sources to consider how its approach compares to the basic deterrence framework outlined earlier in the thesis. Next, it considers through the lens of expert interviews how the Israeli experience of deterrence has resulted in an approach to cyberspace which, while consistent with Israel's broad strategy, carries significant risk due to its reliance on the extensive use of kinetic force. The chapter explores the effectiveness of the policy approach through the views of Israeli strategists, and considers the reasoning for the substantial caveats these experts placed on Israel's 'success'. Finally, the chapter presents the preliminary finding that – while the Israeli approach to deterrence in cybersecurity is fundamentally the same as its broad deterrence approach, contains the requirements of classic deterrence, and is claimed by the government as a success – its reliance on 'refreshing' deterrence through the regular use of pre-emptive and overwhelming force may well be misunderstood by its interlocutors, resulting in unintended escalation.

Israel is an important case for considering how states approach deterrence in cyberspace. Globally, it is one of the most advanced states in terms of cybersecurity and cyber defences[412], and has adopted a comprehensive cybersecurity approach which includes a strong commitment to deterrence. As outlined in Chapter 1, successful deterrence requires three basic elements: persuading an opponent that you had an effective military capability; that you could credibly impose unacceptable costs on him; and that you will use it if attacked.[413] However Chapter 1 also noted conflicting views on how best to operationalise deterrence for cybersecurity, given the acknowledged complexities of cyberspace: differing definitions of cybersecurity; conflicting views over whether the cyber domain should be managed as a separate or integrated battlespace; the difficulty of defining threat actors and cyber 'attacks'; the lack of agreed standards for attributing such cyber-attacks; and the problematic conceptualisation of 'cyber deterrence' rather than deterrence for cybersecurity. This chapter begins by placing the Israeli approach to these

[412] Jasper Frei, 'Israel's National Cybersecurity and Cyberdefense Posture: Policy and Organizations', p.5
[413] Morgan, *Deterrence Now*, p. 4

identified issues into the relevant strategic context. This is particularly important for Israel, as its strategic history has significantly influenced its conceptions of deterrence and deterrence success, and these ideas have in turn shaped its approach in relation to deterrence and cybersecurity.

3.2 Defining deterrence: Israel's legacy of survival as 'success'

While the complex history of Israel is beyond the scope of this study, any exploration of its application of deterrence must briefly acknowledge the lasting influence of multiple conflicts on the construction of the modern Israeli state and their role in shaping its security strategies.[414] Since 1947, Israel has fought eight recognised wars, two Palestinian intifadas, and a series of armed conflicts in the broader Arab–Israeli conflict. Its experiences during the War of Independence (1947–49), the Sinai War (1956), the Six Day War (1967), the War of Attrition (1968–70) and the Yom Kippur War (1973) yielded two critical lessons.[415] First, being surrounded by adversaries in overwhelming numbers has meant survival as a state remains Israel's most pressing strategic goal, and has required substantial military capabilities. Second, these capabilities have needed to be regularly demonstrated to deter its adversaries for a period of time.[416]

These experiences have directly influenced not only the adoption of Israel's own deterrence approach but also the centrality of its role within broader Israeli security strategy.[417] Deterrence in Israel is defined as an impermanent state that requires the use of force to regularly refresh it.[418] Somewhat counterintuitively, then, conflict is not considered a failure of deterrence, but rather is accepted as an inevitable part of strategy.[419] This view of deterrence has produced strategic doctrine that is pragmatic, and does not assume that deterrence will automatically work. Indeed it plans for deterrence to be regularly tested by known threat actors that wish to destroy it, and acknowledges that it will sometimes fail.[420] This, in turn, bolsters Israel's consistent search for military superiority.[421] Indeed, demonstrations of overwhelming

[414] For an introduction to Israeli attempts to create security in its region see Martin Sicker, *Israel's Quest for Security*, (New York: Praeger, 1989), p. 9; see also Charles K. Rowley and Jennis Taylor, 'The Israel and Palestine Land Settlement Problem, 1948-2005: An Analytical History', *Public Choice* 128, no. 1/2 (2006): 77–90.

[415] Netanel Lorch 'The Arab-Israeli Wars', accessed 7 August 2021, see also Zeev Maoz, 'Evaluating Israel's Strategy of Low-Intensity Warfare, 1949-2006', *Security Studies* 16, no. 3 (2007): p. 325

[416] Gadi Eizenkot and Gabi Siboni, 2019, 'Guidelines for Israel's National Security', *The Washington Institute for Near East Policy*, no. Policy Focus 160.

[417] There is an extensive literature on the centrality of deterrence to broad Israeli national security strategy. See Malka, 'Israel and Asymmetrical Deterrence'; Efraim Inbar and Eitan Shamir, 2014 '"Mowing the Grass": Israel's Strategy for Protracted Intractable Conflict', *Journal of Strategic Studies,* 37:1, 65-90; Bernard Reich and Gershon R. Kieval, 1988, *Israeli National Security Policy: Political Actors and Perspectives*, vol. no. 210, New York: Greenwood Press, p.3; Maoz, 'Evaluating Israel's Strategy of Low-Intensity Warfare, 1949-2006', p.320; Uri Tor, '"Cumulative Deterrence" as a New Paradigm for Cyber Deterrence', p.94

[418] Henriksen, 'Deterrence by Default? Israel's Military Strategy in the 2006 War against Hizballah', p.100; Tor, '"Cumulative Deterrence" as a New Paradigm for Cyber Deterrence'; Israel Tal and Martin Kett, 2000, *National Security: The Israeli Experience*, Westport, Conn: Praeger, p.53; Jean-Loup Samaan, 2014, 'From War to Deterrence? Israel-Hezbollah Conflict Since 2006', Fort Belvoir, VA: Defense Technical Information Center, 1 May 2014, p. 488.

[419] Michael I. Handel, 1973, *Israel's Political-Military Doctrine*, vol. no. 30, Cambridge, Mass.: Center for International Affairs, Harvard University, p.64

[420] Tal and Kett, *National Security: The Israeli Experience*, Preface; see also Shmuel Bar, 2020, 'Israeli Strategic Deterrence Doctrine and Practice', *Comparative Strategy,* 39:4, 321-322

[421] Bar, 'Israeli Strategic Deterrence Doctrine and Practice', p. 334

force have engendered the creation of a conventional military capability powerful enough to 'deter any and all of Israel's adversaries, and to decisively win every military encounter against them'.[422] Hence, deterrence for Israel does not translate to the absence or prevention of conflict, but rather winning any conflict that occurs. This approach, known as 'cumulative deterrence', is Israel's solution for living with constant conflict.[423] Although differing somewhat from a Western understanding of deterrence, this definition is similar to Morgan's use of the term 'serial deterrence 'to describe a practice whereby a threat is met with an attack by an adversary, which is responded to with punishment, and the pattern repeats.[424] This is an approach which is widely accepted as being both necessary and largely successful in Israel. Israel has repeatedly demonstrated its willingness to use violent means to achieve the political end of deterrence.[425] *The Economist* captured this in 2009, noting Israel defined deterrence in terms of its readiness to not only participate in conflict, but in doing so to inflict enough death and destruction so that foes think twice about attacking again.[426] Shmuel Bar argued that this heavy reliance on the projection of deterrence is a result of its wish to avoid the heavy social and economic price tag of war,[427] which seems logical given Israel's historical fight for survival.

As already noted Israel perceives the threats against it as serious and existential.[428] It is this perception, coupled to a view of deterrence as a cumulative practice that requires the regular use of deliberately disproportionate force[429] that explains why Israel prioritises expending considerable resources on developing and maintaining military capabilities. Since 1948 the size of the Israeli Defense Force (IDF) – without reserves – has remained constant at 4.5% of its population. In contrast its neighbouring countries Egypt, Syria Jordan and Iraq maintain standing armies of between 0.2–0.4% of total population.[430] This effort to develop and maintain superior military capabilities is a deliberate choice by the Israeli state to deter, and when necessary respond, to threats against it through armed power, retaliation and retribution.[431] As the Israeli strategist Gabi Siboni notes:

[422] Ariel Levite, 1989, *Offense and Defense in Israeli Military Doctrine*, Boulder: Westview Press, p.47; see also Maoz, 'Evaluating Israel's Strategy of Low-Intensity Warfare, 1949-2006', p.320. The IDF's security objectives are to defend the sovereignty and territorial integrity of the State of Israel, deter all enemies, and curb all forms of terrorism that threaten daily life. Its main tasks include reinforcing the peace arrangements; ensuring overall security in the West Bank in coordination with the Palestinian Authority; spearheading the war against terrorism, both inside Israel and across its borders; and maintaining a deterrent capability to prevent the outbreak of hostilities. From the Israeli Ministry of Foreign Affairs, see https://mfa.gov.il/mfa/aboutisrael/state/pages/the%20state-%20israel%20defense%20forces%20-idf-.aspx

[423] Tor, '"Cumulative Deterrence" as a New Paradigm for Cyber Deterrence'.

[424] Morgan, *Deterrence Now*, p. 293

[425] Henriksen, 'Deterrence by Default? Israel's Military Strategy in the 2006 War against Hizballah', 95; Inbar and Shamir, '"Mowing the Grass": Israel's Strategy for Protracted Intractable Conflict', 65–90.

[426] 'Two Eyes for an Eye; Israel's Military Strategy', 2009, *The Economist,* 390:8613, 23

[427] Bar, 'Israeli Strategic Deterrence Doctrine and Practice', 321.

[428] Sicker, *Israel's Quest for Security*, 1.

[429] Yaakov Katz, 4 August 2010, 'Israeli Deterrence Needs a Boost', *Jerusalem Post*

[430] Bar, 'Israeli Strategic Deterrence Doctrine and Practice', 327.

[431] Arian, *Security Threatened: Surveying Israeli Opinion on Peace and War*, p. 27

> deterrence involves discouraging the nation's enemies from acting against it based on military and security force build-up, and the preparedness and willingness to counter the enemy's intention to violate the sovereignty, daily life and security of the nation's citizens.[432]

The result of this historical experience, as Thomas Rid has pointed out, is that deterrence has an almost unquestioned role in Israeli security policy[433] and is widely viewed by Israeli society as successful.[434] For Ariel Levite this explains why Israeli policymakers have consistently attached critical security importance to deterrence as an approach to redress any perceived security vulnerabilities.[435] But it also means that Israeli decision makers do not separate deterrence from the use of force, which leads to questions about the relevance of the deterrence concept.[436] Put simply, is Israel espousing deterrence but really pursuing a more overtly hostile strategy based on immediate (and sometimes pre-emptive) punishment against those that threaten its interests?

Before we can begin to answer this question for cyberspace it is important to assess the definition and role of deterrence more broadly within Israel's strategic policies. We must also take into account that any such examination is complicated by not all Israeli strategy being overt or explicit; Israel Tal explains that Israel's approach can best be understood as part oral planning, part formal strategy comprised of laws, decisions by the Knesset (Israeli Parliament) and government, and part standing doctrine such as high command and general staff directives and the training manuals used by various sections of the IDF.[437] But while the intellectual foundations of deterrence in Israel were laid by practitioners rather than scholars,[438] Israel's security rests on well-established and understood principles. Israel's first Prime Minister, David Ben-Gurion, formed the principles of Israel's security concept which were centred around survival as a priority and drove Israeli strategic practice for decades.[439] These principles were fundamentally centred on survival: in 1953, Ben-Gurion stated 'Unless we show the Arabs there is a high price for murdering Jews we won't survive.'[440] Thus Israel's approach to deterrence was highly specific, targeted against known adversaries, and centred on the survival of the Israeli state.[441] This helps explain Dima Adamsky's view of deterrence as 'a set of institutionalised improvisations, rather than a developed strategic theory supported by prescriptive scholarship.'[442] The core purpose of Israeli deterrence was

[432] Eizenkot and Siboni, 'Guidelines for Israel's National Security', p.33

[433] Rid, 'Deterrence beyond the State: The Israeli Experience', 124.

[434] Henriksen, 'Deterrence by Default? Israel's Military Strategy in the 2006 War against Hizballah', 112; Malka, 'Israel and Asymmetrical Deterrence', 1.

[435] Levite, *Offense and Defense in Israeli Military Doctrine*, 47.

[436] Samaan, 'From War to Deterrence?', 489.

[437] Tal and Kett, *National Security: The Israeli Experience*, preface

[438] Uri Bar-Joseph, 'Variations on a Theme: The Conceptualization of Deterrence in Israeli Strategic Thinking', *Security Studies* 7, no. 3 (1998): 145–81, p. 147

[439] Dmitry (Dima) Adamsky, 'From Israel with Deterrence: Strategic Culture, Intra-War Coercion and Brute Force', *Security Studies* 26, no. 1 (2017): 157–84, p. 122

[440] Daniel Byman, *A High Price: The Triumphs and Failures of Israeli Counterterrorism*, (New York: Oxford University Press, 2011), p. 1

[441] Samaan, 'From War to Deterrence?', 488.

[442] Adamsky, 'From Israel with Deterrence: Strategic Culture, Intra-War Coercion and Brute Force', 164.

defined in 1990 as 'direct military activity designed to achieve a swift, decisive and visible victory either through pre-emption or transferring war into enemy territory.'[443] The use of extensive force as part of the definition is critical: here we can note the use of force implied in Israeli strategist Gil Baram's definition of deterrence in Israel's national security concept as 'developing defensive and offensive capabilities that will discourage the countries enemies from attacking it'. [444] And Isaac Ben-Israel, an Israeli military scientist, general and former politician described Israel's deterrence as cumulative because it regards each of its wars as one round in a series of hostile episodes.[445] In other words, deterrence as understood in Israel should not be limited to convincing adversaries that an attack on Israel would be counter-productive – instead, the concept revolves around Israel setting a low threshold for retaliation on enemy behaviour, and clearly communicating this so that the enemy knows about and believes in that threshold.[446] Thus we can see that while deterrence is a term frequently used in Israeli military literature,[447] it does not carry quite the same meaning or framing as deterrence in Western nations. The Israeli notion of deterrence includes a specific role not just for threatening the use of force, but for using force to create periods of limited peace. This is in contrast to the essence of deterrence theory, based around the issuing of a threat to inhibit attacks, to threaten to fight and thus not have to do so at all by forestalling attacks.[448]

A further useful conception of deterrence comes from the Israeli strategist Dima Adamsky, who has categorised Israeli deterrence into four different types: current deterrence prevents low-intensity violence and escalation from non-state actors; specific deterrence prevents limited moves that endanger vital interests; strategic deterrence prevents general war with state actors; and cumulative deterrence aims to persuade enemies that attempts to achieve their goals on the battlefield are doomed.[449] This clearly illustrates the different purpose and goals at each level of deterrence; understanding these is essential for evaluating Israel's success or failure.

The willingness to use force and the conception of deterrence as operating differently across different levels of Israeli strategy matters for considerations of Israeli deterrence success in several ways. By defining deterrence as being created not just through threats but through offensive engagement – including pre-emptive strikes – against an adversary, Israel is re-framing how deterrence is defined.[450] If successful deterrence does indeed include a role for offensive and pre-emptive measures, then states which do not have these as part of their deterrence approach are doomed to fail. But if the inclusion of offensive strikes shifts the Israeli approach from deterrence to something else – perhaps warfare – then despite the terminology, this approach does not comprise deterrence and cannot be judged as such.

[443] Levite, *Offense and Defense in Israeli Military Doctrine*, p.7.

[444] Gil Baram, 'Israeli Defense in the Age of Cyber War', *Middle East Quarterly* 24, no. 1 (2017): p.3.

[445] Cited in Baram, 'Israeli Defense in the Age of Cyber War'.

[446] Bar, 'Israeli Strategic Deterrence Doctrine and Practice', p.328.

[447] Samaan, 'From War to Deterrence?', p.487

[448] Morgan, *Deterrence Now*, 89.:27; Schelling, *Arms and Influence.*

[449] Adamsky, 'From Israel with Deterrence: Strategic Culture, Intra-War Coercion and Brute Force', 164.

[450] Tal and Kett, *National Security: The Israeli Experience*, p.40; Tor, '"Cumulative Deterrence" as a New Paradigm for Cyber Deterrence', p.94; Rid, 'Deterrence beyond the State: The Israeli Experience', p.129

Further when considering the success or failure of deterrence, such considerations are only meaningful if they consider the goal in question at the time. If Israel is discussing cumulative deterrence, it is very difficult – if not impossible – to find a situation which is considered a deterrence failure, as Israel still exists. And as long as the Israeli state can continue to operate as it wishes to in spite of attacks, its approach is arguably a success even in the face of major cyber-attacks. However, if evaluating current deterrence in the cyber domain and the attempt to prevent low-intensity violence from non-state actors, then there are many examples of where it has failed and Israel has responded.

Israel's broad deterrence approach includes significant and effective military capabilities; their use of these capabilities renders the threat of future use quite credible; and Israel has actively communicated that threat. Taken as a whole, this would seem to indicate a reasonable attempt at deterrence. But Israel's reliance on offensive measures and definition of deterrence as cumulative changes the shape of how Israel expects deterrence to operate, both within and outside cyberspace. This point is critical for research into deterrence success in cyberspace, as conflict in any space is not regarded in Israel as a failure of deterrence theory, but rather a sign that deterrence practices need to be refreshed. But is this practice even deterrence, or is it more accurately described as compellence?

As outlined in Chapter 1, both Schelling and Morgan tried to distinguish between deterrence and compellence[451]: deterrence is the use of threats to prevent states from starting a course of action, and compellence is the use of threats to compel states to stop a course of action already underway.[452] There is an argument that the Israeli approach to, and conceptualisation of, deterrence could more accurately be described as compellence due to its reliance on the regular use of force and status of ongoing conflict against adversaries. Indeed, the Israeli strategist Professor Uri Bar-Joseph notes Israeli military officers sometimes confuse the idea of deterrence with simple coercion.[453] Yet as Shmuel Bar argues, it may be more accurate to view compellence as part of a deterrence spectrum, as the Israeli acceptance that deterrence may fail explains why escalation management and compellence are included in its conception of deterrence.[454] Either way, the Israeli approach seems at first glance to reinforce Robert Powell's argument that deterrence and compellence are sufficiently alike to consider both as attempts by a state to coerce its adversary into acting in certain ways and not others, by shaping the adversary's estimates of the costs and benefits.[455]

Given the complexity of separating deterrence and compellence, both at the conceptual level and within Israeli practice, it is simply not possible to explore or evaluate Israeli deterrence without considering the substantial role played by the use of force in Israeli strategy and the ongoing conflict it is involved with.

[451] Schelling, *Arms and Influence*; Morgan, *Deterrence Now*.
[452] Morgan, *Deterrence Now*, p. 2
[453] Samaan, 'From War to Deterrence?', 492.
[454] Bar, 'Israeli Strategic Deterrence Doctrine and Practice', 334.
[455] Robert Powell, 2008, *Nuclear Deterrence Theory: The Search for Credibility*, Cambridge: Cambridge University Press, p.7

That said, labelling this approach simply as compellence is conceptually unhelpful. While the purpose of Israeli deterrence aligns with classic deterrence as an attempt to influence the cost-benefit calculations with the aim of avoiding war[456], in the Israeli case the purpose is not to avoid conflict entirely, but rather to avoid a conflict so destructive that Israel as a state would be destroyed. Thus attempting to distinguish between deterrence and compellence in this environment is not possible as conflict is expected and ongoing in every domain. In this way, Israel considers that the use of force is considered as essential to establish sufficient credibility, blurring the lines between deterrence and compellence to the point they are indistinguishable. Far from representing a failure of deterrence, such use of force is regarded as another method of communicating intent, demonstrating capabilities and establishing credibility.

Thus the choice to adopt deterrence theory into cybersecurity policy is rooted in Israel's broader experience of deterrence as a practice which is considered to have been largely effective for ensuring Israel's survival.[457]

Having examined Israel's definition of deterrence, I now turn to exploring the significant influence of Israel's strategic history on the conceptualisation of deterrence for the purposes of cybersecurity policy, most significantly on both its potential for success, and the fact that success is defined as resilience to, not prevention of, attacks. The Israeli experience is that deterrence is a successful approach[458] that has also survived significant shifts in the strategic environment[459] and thus is applicable to cyberspace. Further, the unique features of cyberspace are not considered by Tel Aviv as a barrier to the applicability of deterrence. Instead, as Israeli strategist Uri Tor argues, cumulative deterrence is an effective policy for cyberspace[460] because it accepts acts of cyber aggression as inevitable, and seeks to shape and limit these through attacking the adversary repeatedly in response to specific behaviours, sometimes disproportionately.[461] But it is worth pausing to consider the nature of the threats posed through cyberspace to Israeli interests, and how serious the Israeli state judges these to be against the broader context of threats it faces.

According to Shmuel Bar, Israel is one of the most cyber-attacked nations in the world.[462] As early as 2012 Israeli officials announced there had been 100 million cyber-attacks targeting Israeli government services.[463] While numbers alone are not necessarily indicative of the severity of the threat, the Israeli

[456] Morgan, *Deterrence Now*, p. 4.

[457] Lior Tabansky, 2018, 'Israel's Cyber Security Policy: Local Response to the Global Cybersecurity Risk', in *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications*, pp.112545

[458] Samaan, 'From War to Deterrence?', 488.

[459] Maoz, 'Evaluating Israel's Strategy of Low-Intensity Warfare, 1949-2006', 319–20.

[460] Tor, '"Cumulative Deterrence" as a New Paradigm for Cyber Deterrence', 95.

[461] Uri Tor, Cumulative deterrence, p. 95; see also 'Disproportionate Force: Israel's Concept of Response in Light of the Second Lebanon War', *INSS* (blog), accessed 7 August 2021, https://www.inss.org.il/publication/disproportionate-force-israels-concept-of-response-in-light-of-the-second-lebanon-war/.

[462] Bar, 'Israeli Strategic Deterrence Doctrine and Practice', p.347.

[463] Veronika Netolicka and Miroslav Mares, 2018, 'Arms Race "in Cyberspace" – A Case Study of Iran and Israel', *Comparative Strategy,* 37:5, 424

government takes threats to its interests in cyberspace sufficiently seriously to have Prime Minister Netanyahu described cyber-attacks as 'one of the four main threats to Israel' in 2014,[464] emphasising again in 2017 that they were a 'growing threat.'[465] Israel relies heavily on cyber technology, which may also help explain why it is attacked more frequently.[466] But where are these threats coming from? Who are the adversaries Israel is seeking to deter? First, Israel considers cyber threats as an extension of the threats it faces in other domains, which can stem from either military or civilian actors – or a combination of both.[467] In other words, while Israel faces serious threats to its interests through cyberspace, the high-intensity of non-cyber threats through terrorism, missile strikes and Iran's nuclear program is still ongoing.[468] Second, Israel claims it does not differentiate threats through the vector by which they attack, meaning their adversaries in cyberspace reflect known threats from other domains. The publicly identified main adversaries of Israel are the states of Iran and Lebanon, the failing state of Syria, state-like entities of Hamas and Hezbollah, and terrorist organisations without links to a specific country including Islamic State (ISIS) and the Palestinian Islamic Jihad.[469] This conception of threats that Israel admits it faces has remained largely unchanged over the past several decades. In 2016 Prime Minister Netanyahu released a world map which divides the world's countries into four categories: those with which Jerusalem had: 'recently developed/upgraded' relations; 'good relations'; 'overtly hostile enemy states'; and those with which 'Israel does not have special relations,' according to the prime minister's aides.[470] Of the 'overtly hostile enemy states, only five are listed: Iran, Iraq, Syria, Afghanistan and North Korea. [471]

As Israel considers cyber threats as another aspect of known and identified threats, its adversaries in cyberspace should be the same as its adversaries in any other space and, as with the historic threat against it, limited in scope and essentially confined to the Arab world.[472] As an example, Cohen et al noted a potential correlation between Israel facing an increase in cyber-attacks as it was conducting operations against Hamas in 2014;[473] whereby kinetic Israeli attacks seemingly led to increased cyber-attacks by Hamas.[474] So far then, these are threats in cyberspace that align with known strategic threats against Israel.

[464] Matthew S. Cohen, 2015/2016, Charles D. Freilich, and Gabi Siboni, 'Israel and Cyberspace: Unique Threat and Response', *International Studies Perspectives,* 17:3, 311

[465] EFE News Service, 2017, 'PM Netanyahu: Cyber Security Is a Serious Business Matter for Israel', *EFE News Service*

[466] Cohen, Freilich, and Siboni, 'Israel and Cyberspace: Unique Threat and Response', 307.

[467] Deborah Housen-Couriel, 'National Cyber Security Organisation: ISRAEL', n.d., p. 7

[468] Lior Tabansky, 2020, 'Israel Defense Forces and National Cyber Defense', *Connections,* 19:1, 45-62

[469] See Gadi Eizenkot, 'Deterring Terror: How Israel Confronts the Next Generation of Threats' (Belfer Center for Science and International Affairs, August 2016). For a definition of Hezbollah, a Shia Islamist political and paramilitary organisation, see David E. Johnson et al., *Hard Fighting: Israel in Lebanon and Gaza*, vol. MG-1085-A/AF., (Santa Monica, Calif: RAND, 2011).

[470] Raphael Ahren, 'In Netanyahu's New Illustrated World, Israel Has Just Five Enemies', accessed 7 August 2021, http://www.timesofisrael.com/in-netanyahus-new-illustrated-world-israel-has-just-five-enemies/.

[471] Ibid

[472] Reich and Kieval, *Israeli National Security Policy: Political Actors and Perspectives*, 210:2

[473] Cohen, Freilich, and Siboni, 'Israel and Cyberspace: Unique Threat and Response', p. 304.

[474] Hamas is an ideological movement which arose as a branch of the Muslim Brotherhood in Egypt and became a mainstay of Palestinian resistance of Israeli occupation. Hamas achieved a level of political control in Gaza in 2005

As in all other spheres, Israel's most contested relationship is with Iran. The potential for Israel and Iran to continue engaging in hostilities in cyberspace is widely acknowledged.[475] For example, in 2013 Iran claimed to have the world's fourth biggest cyber army, which allowed it to 'counterbalance Israel and the US in the region'.[476] However, a comparison of this public stance with known cyber-attacks reveals a broader threat picture. Michael Raska argues the focus on declared historic threats particularly that posed by Iran, may be skewing Israel's strategy.[477] As he notes, Israel is facing at least two distinct threat types in cyberspace – a lower technology threat from its traditional enemies, and a potential higher technology threat from actors including Russia and China – vastly different threats that require different deterrence approaches.[478] Yet despite Israel not declaring these states publicly as posing a risk to Israel's cyber interests, they are by no means ignored by Israeli strategists. Consider that in 2011–12 a group linked to China's People's Liberation Army (PLA) hacked three Israeli defense systems with the apparent aim of stealing blueprints of Israel's anti-rocket and anti-missile systems;[479] or the 2017 case of Israeli officers watching Russian hacking attempts in real time.[480] The fact such attacks are acknowledged by Israel in the public domain indicate its awareness of the potential cyber threat posed by states like China and Russia. Further, Israel's National Cyber Security Strategy notes 'a national level campaign is required against severe threats by determined, resource-rich attackers who pose serious danger to the nation'.[481] Although the strategy does not specify examples of such threat actors, the reference to resource-rich attackers certainly indicates the recognition of, and planning for, threats far beyond the capabilities of Israel's traditional enemies. Contrary to Raska's view, then, this suggests Israel is perfectly aware of the potential threats posed by more advanced nations but prefers to keep such assessments ambiguous.

However the argument that threats in cyberspace could vary beyond the traditional threat actors and Israel is potentially unprepared or underprepared for a technologically advanced actor is not supported; Israel's formal list of adversaries is short. Notably, it does not include many other nations identified as having conducted cyber-attacks against it, such as Turkey.[482] Nor does Israel publicly identify other states

and formed government in 2006.For an in-depth explanation of the evolution of the Hamas movement, see Imad Alsoos, 'From Jihad to Resistance: The Evolution of Hamas's Discourse in the Framework of Mobilization', *Middle Eastern Studies* ahead-of-print: 1–22.

[475] Oved Lobel, 'Israel and Iran: "Cyber Winter Is Coming"', *The ASPI Strategist [BLOG]*, (2020),; Netolicka and Mares, 'Arms Race in Cyberspace" - A Case Study of Iran and Israel'.

[476] 'Iran/Israel/United Sates: Presidential Candidate: US, Israel Wary of Iran's Cyber Power', *Asia News Monitor*, 2013, see also Netolicka and Mares, 'Arms Race in Cyberspace" - A Case Study of Iran and Israel' p.425

[477] Michael Raska, 2015, 'Confronting Cybersecurity Challenges: Israel's Evolving Cyber Defence Strategy', *Policy File,* S. Rajaratnam School of International Studies, 2; Seth J. Frantzman, 2020, 'Cyber Warfare, Israel, Iran and the New Way of Total War', *The Jerusalem Post (Online)*, English ed.; Yossi Mekelberg, 2020, 'Cyberspace: The New Frontier in the Israeli-Iranian Battleground', *Arab News*

[478] Raska, 'Confronting Cybersecurity Challenges: Israel's Evolving Cyber Defence Strategy', p. 2

[479] Cohen, Freilich, and Siboni, 'Israel and Cyberspace: Unique Threat and Response', 310.

[480] Nicole Perloth and Scott Shane, 'How Israel Caught Russian Hackers Scouring the World for U.S. Secrets', *New York Times (Online)*, 2017

[481] 'Israel National Cyber Security: In Brief'.

[482] Cohen, Freilich, and Siboni, 'Israel and Cyberspace: Unique Threat and Response', 313.

such as Saudi Arabia as hosts for cyber-attacks against it.[483] Maintaining some ambiguity regarding emerging threat actors is thus more likely to be deliberate choice while Israel considers its approach to managing emerging threat actors. There is also an alternative view worth noting – that Israel's approach is attacker-agnostic. Adamsky argues Israel's approach is 'perpetrator-indifferent' by focusing on protection of critical assets, the types of possible attacks and preventing those.[484] Such an approach does not require the identification of an attacker. This was the approach advocated by the IDF Brigadier General Eyal Zelinger, commander of the IDF's Teleprocessing Corps,[485] who stated in 2013 that the IDF 'wasn't surprised' by reports on Chinese cyber activity:

> The Chinese have great technological capabilities, and so do the Russians, the Americans, the Europeans and several other states. I treat a threat like a threat and it matters little to me whether it's thought up by a Chinese mind or an Iranian one.[486]

Regardless of differing ideas about the origin of threats, it is clear that the Israeli conception of cyber threats is that they may be serious, related to other conflicts (including kinetic warfare), and are serious enough to warrant significant government efforts to prevent or mitigate them damaging Israeli interests. Further, the threat to Israel's interests in cyberspace was judged sufficiently serious that it required the extension of Israel's established deterrence approach to cybersecurity. Managing the complex threat environment is discussed in greater detail in the next section.

3.3 Extending deterrence to cyberspace: A comprehensive approach

Having considered the circumstances in which Israel's deterrence approach was developed; explored how the Israeli definition both reflects and differs from deterrence theory; and examined how Israel's views of the cyber threat in the context of its broader threat environment, I have so far established that Israel's approach to deterrence in cybersecurity is predicated on an expectation of conflict as an ongoing problem, and the use of force as a necessary solution. Plainly put, Israel dedicated a significant effort towards creating a deterrence approach for cyberspace despite acknowledging from the outset that this deterrence would 'fail' to the extent of not preventing ongoing attacks. This chapter now turns to considering why this was so, and the impact it had on deterrence policies for cyberspace. Below I examine Israeli cybersecurity policy against the requirements of classic deterrence, explore the influence of Israel's broad deterrence approach, and consider the extent to which these policies can be argued to have met those requirements.

[483] Ibid

[484] Adamsky, 'From Israel with Deterrence: Strategic Culture, Intra-War Coercion and Brute Force', 122.

[485] The Teleprocessing Corps forms part of the IDF's elite technological unit. See 'C4I And Cyber Defense Directorate' 'C4I and Cyber Defense Directorate', Israel Defense Forces, October 29, 20174:56 PM, https://www.idf.il/en/minisites/c4i-and-cyber-defense-directorate/.

[486] 'IDF Forms New Force to Combat Cyber Warfare - Haaretz Com - Haaretz.Com', accessed 7 August 2021, https://www.haaretz.com/.premium-idf-takes-steps-against-cyber-attacks-1.5232323.

As outlined in Chapter 2, this research examines declared public policy for cybersecurity – a series of public policy measures aimed at protecting its interests in cyberspace with a particular emphasis on deterrence.[487] The existence of such policy in the public sphere, while not unusual for Western states such as the US or UK, is an unusual step for Israel. Israel has traditionally relied on a security strategy that was broadly understood but not explicit, a de facto security strategy consisting of four pillars: early warning; decisive battlefield victory; deterrence (cumulative, not absolute); and defence of the rear (the home front).[488] This de facto strategy was largely an oral doctrine absent from specific public policies or security documents.[489] Yet on the challenge of cyberspace the Israeli government decided to release a number of policy documents outlining its explicit approach. The step of codifying Israel's approach, practice and expectations in cyberspace is unique in Israeli's strategic history and reveals both the seriousness of the perceived problem, and the importance placed on communicating Israel's intended responses to cyber threats. These findings are demonstrated further through examining the content and reasoning of each policy below.

Israel was one of the first states to recognise the extent of potential threats to its interests through cyberspace, as demonstrated by its 2002 decision to adopt a government resolution to secure critical infrastructure, the Critical Infrastructure Protection Arrangement.[490] This arrangement was established under Israeli Resolution 84/b: 'Responsibility for the defense of computerized systems in the State of Israel'[491], which created a National Information Security Agency and directed private organisations with critical infrastructure responsibilities to appoint and employ dedicated IT-security personnel responsible for implementing the professional instructions.

While this was an important step, Resolution 84/b did not provide guidance for the government and defense sectors. Prime Minister Netanyahu sought to redress this in 2010 by establishing a National Cyber Initiative Expert review, with the aim of establishing cybersecurity as a national objective and placing Israel in the top five nations in the cyber field for technological advances.[492] Israeli strategist Lior Tabansky argues it was the public discovery of Stuxnet in 2010 that shifted worldwide attention to policy for cybersecurity and prompted the review.[493] However as Gil Baram notes, the increasing use of what she describes as 'cyber warfare technologies' on the battlefield since the early 2000s had also contributed to the need for new policies.[494] Further, as early as 2009 the then-Chief of the General Staff

[487] 'Israel | UNIDIR' Israel Cybersecurity Policy, Strategy Documents, updated September 2020, accessed 25 June 2021, https://unidir.org/cpp/en/states/israel.
[488] Tabansky, 'Israel Defense Forces and National Cyber Defense'.
[489] Baram, 'Israeli Defense in the Age of Cyber War', p.3.
[490] Resolution B/84 of 2002, cited in Tabansky, 'Israel Defense Forces and National Cyber Defense', p. 47
[491] Baram, 'Israeli Defense in the Age of Cyber War', 3.
[492] Tabansky, 'Israel Defense Forces and National Cyber Defense'.
[493] Ibid, p.2
[494] Baram, 'Israeli Defense in the Age of Cyber War', p.3.

for the IDF, Lieutenant General Gabi Ashkenazi had defined cyberspace as a 'strategic and operative combat zone for Israel'. [495]

It is likely there were a range of reasons for the review identified from multiple areas across Israeli politics and strategy given the breadth and depth of this work. It involved a six-month process including 80 experts from across defence, government, academia and research and development institutions conducting a systematic review of the challenges and opportunities for Israel in cyberspace.[496] More importantly, the review was an attempt to develop an evidence base for Israel's future policies to secure cyberspace, and resulted in the 2011 Knesset approval of Government Resolution No. 3611 'Advancing National Cyberspace Capabilities'.[497]

Resolution 3611 is Israel's public national cybersecurity strategy. It is the 'grand strategy' from which all other strategies in cybersecurity are derived. It is remarkable firstly because it included specific definitions of key terms; definitions which have not only remained unchanged over a decade of practice but also reveal important insights into the Israeli attempt to develop an approach that was both credible, and included the ability to substantially develop and improve capabilities. The strategy defines cyberspace as:

> the physical and non-physical domain that is created or composed of part or all of the following components: mechanized and computerized systems, computer and communications networks, programs, computerized information, content conveyed by computer, traffic and supervisory data and those who use such data.[498]

The specific inclusion of the human element as a part of cyberspace demonstrates that Israel views its deterrence in human terms, as an extension of human behaviour. This theme is continued in the definition of cybersecurity:

> the policies, security arrangements, actions, guidelines, risk management protocols and technological tools designated to protect cyberspace and allow action to be taken therein.[499]

The inclusion of 'action to be taken therein' demonstrates that from the outset Israel's policy approach for cyberspace has expected that cybersecurity would not only need to be strongly defensive but would require active measures to create and manage deterrence. This is consistent with Israel's broader security strategy of deterrence as cumulative rather than absolute. A further unique aspect of Israel's approach in this strategy was the definition – and separation – of civilian and military responsibilities in cyberspace, with civilian space defined as 'cyberspace that includes all the governmental and private bodies in the

[495] Hanan Greenberg, 'Virus bimokm matos, NRG, Nov 11 2011, cited in Gil Baram, 'Israeli Defense in the Age of Cyber War', *Middle East Quarterly*, Winter 2017, 3
[496] Tabansky, 'Israel Defense Forces and National Cyber Defense'.
[497] 'Advancing National Cyberspace Capabilities: Resolution No. 3611 of the Government of August 7, 2011' (State of Israel, n.d.) Note: this is an English translation of the original Hebrew and is thus marked 'Non-Official'.
[498] Ibid
[499] 'Advancing National Cyberspace Capabilities: Resolution No. 3611 of the Government of August 7, 2011'.

State of Israel, excluding special bodies'.[500] Special bodies are the IDF, the Israeli Police, Israel Security Agency ('Shabak'), the Institute for Intelligence and Special Operations ('Mossad') and the defense establishment by means of the Head of Security of the Defense Establishment (DSDE).[501]

Resolution 3611 also established the Israeli National Cyber Bureau to lead cyber efforts across public and private Israeli stakeholders and to coordinate policy instruments.[502] This careful delineation of responsibilities, together with the centralisation of decision-making responsibility directly under Prime Minister Netanyahu, demonstrates the extent to which Israel had recognised the need for a holistic and joint approach to cybersecurity[503] – a necessity for any attempt at deterring attacks on both government and private infrastructure. Further, Resolution 3611 also recommended advancing defensive cyber capabilities and promoting research and development, and provided a budget for implementing all measures – a clear effort to develop capabilities.[504] Given the holistic view Tel Aviv takes to defence more broadly, it is not surprising that Israel defines capabilities quite broadly too. Cohen et al. argue Israeli deterrence is heavily reliant on both defensive and offensive capabilities.[505] Max Smeets argues the integration of intelligence capabilities is crucial.[506] But strategist Lior Tabansky argues the Israeli approach is necessarily broader, and includes civilian capabilities including the private sector, non-government organisations and academia.[507]

By 2011 Israel had not only recognised the threats to its interests posed by cyberspace but also invested significant effort into gathering evidence for best practice and translated that evidence into broad government strategy,[508] a strategy that aimed to create and maintain cyber capabilities, build deterrence credibility, and communicate Israeli intent. This resolution represented a detailed attempt to manage the complexities of securing Israel's interests in cyberspace, and the key principles underpinning these efforts have not changed since 2011.

Nonetheless, Israel has continued to test these principles and adjust its policy measures according to identified needs. For example, in 2015 Israel adopted Resolution 2444, designed to advance national

[500] Ibid.
[501] 'Defense Establishment' – the bodies guided by the DSDE as determined in the Law for Organizing Security in Public Bodies of 1998, as well as suppliers and operators developing or manufacturing security equipment for them. See 'Advancing National Cyberspace Capabilities: Resolution No. 3611 of the Government of August 7, 2011'
[502] Tabansky, 'Israel Defense Forces and National Cyber Defense'.
[503] Isaac Kfir, 'Israel's Approach to Counter-Terrorism', in *Handbook of Terrorism and Counter Terrorism Post 9/11*, (Edward Elgar Publishing, 2019), pp.227-39
[504] Tabansky, 'Israel Defense Forces and National Cyber Defense'.
[505] Cohen, Freilich, and Siboni, 'Israel and Cyberspace: Unique Threat and Response', p.313
[506] Max Smeets, 2018, 'Integrating Offensive Cyber Capabilities: Meaning, Dilemmas, and Assessment', *Defence Studies,* 18:4, 395
[507] Tabansky, 'Israel Defense Forces and National Cyber Defense', p.54.
[508] Tabansky, 'Israel Defense Forces and National Cyber Defense'; 'Israel | UNIDIR'; Frei, 'Israel's National Cybersecurity and Cyberdefense Posture'.

regulation and government leadership and advance national preparedness in cyberspace.[509] This resolution also established the National Cyber Security Authority to protect Israeli civilian cyberspace in concert with the Israeli National Cyber Bureau.[510] The resolution was the result of a recognition that 3611 had not gone far enough in streamlining governance for cybersecurity. In 2017 these agencies were merged under Resolution 3270 into the new Israel National Cyber Directorate (INCD) of the Prime Minister to be responsible for all aspects of cyber defense in the civilian sphere.[511]

This series of Israeli government resolutions regarding the governance and protection of civilian cyberspace sent a clear message, both domestically and internationally, that Israel considered its interests in civilian cyberspace as a critical part of Israel's security, and it would take active measures to protect these. As Lior Tabanksy argues, these subsequent efforts were not an indication of failure but rather signalled Israel's resolve to continue working towards the goals of Resolution 3611.[512] And Israel's policies have not stopped at attempts to protect civilian cyberspace. In 2015 the IDF took yet another unusual step and published its first formal defence doctrine, authored by then-IDF Chief of General Staff Lieutenant General Gadi Eizenkot.[513] The Eizenkot Doctrine set out the IDF's approach to cyberspace and signified a major Israeli effort to improve its cyber defences.[514] The doctrine noted five main aims for the IDF in cyberspace: strengthening cyber to achieve parity with Israel's superiority in intelligence, aerial and naval abilities; preparing for expected attacks in cyberspace; the establishment of a cyber arm of the IDF; an operational effort to ensure the IDF could function even under cyber-attack; and development of cyber warfare capabilities for strategic and tactical deterrence as a critical component of cybersecurity.[515] In no other sphere had Israel felt it necessary to publish a defense doctrine since 1948. The decision to do so for cyberspace was a clear effort towards communicating Israel's intent and priorities in cyberspace.

3.4 Communicating deterrence: The 2017 National Cyber Security Strategy

The decision by Prime Minister Netanyahu in September 2017 to publish Israel's first 'Israel National Cyber Security Strategy: In Brief' in English further represents Israel's drive towards not only possessing a strategy for cybersecurity, but in ensuring it was broadly understood. The strategy brief details Israel's strategic approach to cybersecurity and notes that implementation of the strategy falls directly under the

[509] Benjamin Netanyahu, 'Advancing the National Preparedness for Cyber Security: Government Resolution No. 2444' (The State of Israel: The Government Secretary, n.d.), https://ccdcoe.org/uploads/2019/06/Government-Resolution-No-2444-Advancing-the-National-Preparedness-for-Cyber-Security.pdf.
[510] Ibid, p.2
[511] Tabansky, 'Israel Defense Forces and National Cyber Defense'.
[512] Ibid.
[513] Eizenkot, 'Deterring Terror: How Israel Confronts the Next Generation of Threats'. (This doctrine has been published by Israel in Hebrew only; this research relies on the translation provided by the Belfer Center for Science and International Affairs, Harvard.)
[514] Ibid.
[515] Ibid.

Prime Minister's authority, a deliberate decision to centralise command and control.[516] The strategy was a product of over a decade of policy work by Israel's government, and includes lessons learned through trial and error.[517] It describes Israel's approach and goals in cyberspace through three main objectives: keeping cyberspace safe by confronting threats; continuing as a global leader in technical innovation; and shaping cyberspace.[518] These are lofty goals, but Israel has made swift progress towards achieving them, particularly through supporting technical innovation and confronting threats. In 2017 Prime Minister Netanyahu argued the technological leap Israel had made had changed how the nation was perceived, pointing to 600–700 private technical enterprises as evidence of a flourishing sector.[519] Deborah Housen-Couriel argued Israel has been at the forefront of hi-tech and internet infrastructure and services development since 2007, noting the evidence of the Organisation for Economic Cooperation and Development (OECD) rankings for research and development as a percentage of Gross Domestic Product (GDP);[520] and Gil Baram argued Israel was a world leader in cyber capabilities.[521] Thus Israel was well-placed in 2017 to publicise the strategy which had essentially existed in Hebrew since 2011 and was balanced against the three requirements of capability, credibility and communication.

The 2017 Strategy separated Israel's approach to cybersecurity into three layers: aggregate cyber robustness; systemic cyber resilience; and national cyber defence.[522] The distinction and separation between these layers is important for this research as judgments of deterrence success depend, as previously argued, on how a state defines success. And although deterrence is an explicit goal only for the third layer of the strategy, the first two layers provide important insight into, and contribute to, the overall deterrence approach. Beginning at the first layer, 'robustness' is the most basic level of security and is defined in the strategy as:

> the ability of organisations and processes to continue operating despite a routine of cyber threats by repelling and preventing most of the attacks.[523]

This notion of robustness is evidence that the Israeli government expected and indeed planned for ongoing cyber-attacks as a daily feature of the operating environment. If cyber threats are routine, and considered part of daily business, then Israel's deterrence success was never defined as a zero-sum prevention but rather resilience- and survival-focused, building the ability to routinely withstand negative influences through procedures, education and training.[524] It also demonstrates how the concept of

[516] 'Israel National Cyber Security: In Brief', September 2017, State of Israel

[517] Tabansky, 'Israel Defense Forces and National Cyber Defense', 55.

[518] 'Israel National Cyber Security: In Brief', September 2017, State of Israel p.5

[519] 'PM Netanyahu: Cyber Security Is a Serious Business Matter for Israel: Israel Cyber Security'.

[520] Housen-Couriel, 'National Cyber Security Organisation: ISRAEL', p. 5

[521] Baram, 'Israeli Defense in the Age of Cyber War', 8.

[522] 'Israel National Cyber Security: In Brief', September 2017, State of Israel, p.10; see also Eviatar Matania, Lior Yoffe, and Michael Mashkautsan, 2016, 'A Three-Layer Framework for a Comprehensive National Cyber-Security Strategy', *Georgetown Journal of International Affairs,* 17:3, 7784

[523] 'Israel National Cyber Security: In Brief', September 2017, State of Israel, p.11

[524] Adamsky, 'The Israeli Odyssey toward Its National Cyber Security Strategy', 117.

cumulative deterrence has been carried into Israel's efforts in cyberspace, with deterrence as an ongoing effort that requires regular engagement in conflict and thus powerful military capabilities.[525]

As noted in the literature, creating deterrence by denial is complicated by civilian ownership of infrastructure. But although the types of hardening that produce more secure online environments would not generally be accepted by the majority of a democratic population,[526] Israel's tolerance for military interventions in its civilian spaces is higher than that of Western nations. This tolerance helps explain the acceptance of the need for measures to allow companies to continue operating, including the development of significant defensive capabilities at all levels of Israeli society; and such continuance also arguably increases the credibility of Israeli cyber abilities. The second layer, 'systemic cyber resilience', builds in the first layer. 'Resilience' is defined in the strategy as:

> The systematic ability to confront cyber-attacks before, during and after incidents, prevent them from spreading and reduce their cumulative damage to the nation… this layer is event driven by definition.[527]

The concept of resilience, of being able to withstand and recover from attacks, is an established and well-understood tenet of the Israeli approach to deterrence. If attacks are an expected part of the broader strategic environment, then Israel must be flexible and resilient enough to survive the attacks it cannot deter.[528] The second layer is thus an effort to build civilian capabilities and relies on information sharing and providing government assistance to organisations during cyber incidents. It is comprised of both an organisational ability to recover from threats and the state's ability to prevent potential cumulative national effect of such attacks.[529] This layer also contributes to deterrence because if civilian capabilities are increased and the state thus becomes more effective at confronting attacks and reducing harm, then Israel's credibility as a cyber power is also increased. It is also important to consider that while this layer does not include military threats, it does however concern serious threats to Israel, as Israeli banks, financial institutions, utility companies and other critical infrastructure are among those most frequently subjected to hostile cyber events globally.[530] As with the first layer of robustness, systemic cyber resilience is the responsibility of private organisations, but it also includes a role for the state. Adamsky argues the first two layers are 'purely defensive',[531] while the third layer is 'deterrence by punishment'.[532] But as demonstrated here, the first two layers represent key requirements for deterrence by denial.[533] This view

[525] Frei, 'Israel's National Cybersecurity and Cyberdefense Posture'.
[526] Herbert Lin and Jaclyn Kerr, 2019, 'On Cyber-Enabled Information Warfare and Information Operations', *Oxford Handbook of Cybersecurity*, p.29
[527] 'Israel National Cyber Security: In Brief', September 2017, State of Israel, p.10
[528] 'Israel National Cyber Security: In Brief', September 2017, State of Israel, p.10
[529] Adamsky, 'The Israeli Odyssey toward Its National Cyber Security Strategy', p.117.
[530] Housen-Couriel, 'National Cyber Security Organisation: ISRAEL', p.5.
[531] Adamsky, 'The Israeli Odyssey toward Its National Cyber Security Strategy', p.118.
[532] Ibid
[533] Dmitry Adamsky, 2017, 'The Israeli National Odyssey toward its National Cyber Security Strategy', *The Washington Quarterly*, 40:2, 118

underscores the centrality of punishment for deterrence in Israeli strategic thinking. Consider the third layer, 'national cyber defense', defined as being required where:

> A national-level campaign is required against severe threats by determined, resource-rich attackers who pose serious danger to the nation. National defense campaigns include defensive effort, to contain such attacks and their ramifications together with active efforts to confront the source of the threats.[534]

While this layer includes both defensive and active efforts to confront the source of the threats, with deterrence situated under the latter set of capabilities,[535] this research argues it is important to consider the framing of deterrence as part of Israeli 'campaign against attackers'. Thus, what Israel is labelling as 'deterrence' here as part of its cybersecurity strategy could also be considered as the use of offensive and kinetic means to punish cyber-attackers. Israeli strategist Eviatar Matania describes such measures as 'proactive offensive moves' which include kinetic attacks against state and non-state cyber-attackers.[536] Yet Israel's adversaries, most particularly Iran, claim such actions are not deterrence, but instead clear examples of provocation.[537]

This chapter has so far shown that the Israeli policy approach to deterrence in cyberspace is the product of extensive evidence-based reviews and multiple government resolutions, revealing a significant, government-led effort towards better understanding and protecting Israel's interests in cyberspace over the period 2008–2018. Further, although deterrence was not documented previously in broader Israeli policy, as an informal but long-standing and fundamental principle of the Israeli political and security experience it is not especially surprising that deterrence was an explicit part of Israel's cyber strategy from its earliest public policy documents.[538] More surprising has been the extent to which Israel chose to codify and make public its deterrence stance. As there is no further detail on how Israel intended to achieve deterrence for cyberspace through the Strategy, the next section of this chapter examines how deterrence has been operationalised in Israeli practice, including how it has managed the challenges identified in Chapter 1, and explores how such operationalisation both contributes to deterrence through the classic deterrence requirements – and potentially detracts from deterrence aims through the use of excessive force.

[534] 'Israel National Cyber Security: In Brief', September 2017, State of Israel, p.12
[535] Ibid.
[536] Matania, Yoffe, and Mashkautsan, 'A Three-Layer Framework for a Comprehensive National Cyber-Security Strategy', p.6.
[537] See Gawdat Bahgat, 2020, 'Iranian-Israeli Confrontation: The Cyber Domain', *Middle East Policy,* 27:3, 115-24; see also Oved Lobel, 2020 'Israel and Iran: "Cyber Winter Is Coming"', *The ASPI Strategist* [blog]
[538] Lupovici, 'Toward a Securitization Theory of Deterrence', p. 183; Adamsky, 'The Israeli Odyssey toward Its National Cyber Security Strategy'.

3.5 Managing complexity: The risks of operationalisation

A serious implication of Israel's cybersecurity policy approach is that while Israel is meeting its own definition of success, and this definition does arguably meet the requirements of classic deterrence, the reliance on offensive measures renders its actions closer to acts of war, and thus at serious risk of creating an arms race, rather than deterrence. This is significant as it contradicts Israel's self-perceived judgment of deterrence success. Shmuel Bar argues the approach that Israel has taken practically to attacks in cyberspace mirrors its approach outside of cyberspace – a doctrine of defence and deterrence.[539] And Isaac Kfir describes this approach as being a result of Israel's 'holistic and flexible approach to cybersecurity, an approach which is focused on threats, rather than attacks'.[540] But despite these claims, Israel does not seem to be facing reduced cyber threats, nor has it deterred adversaries from gaining increasingly effective cyber capabilities.

To attempt to reconcile these competing views, I now examine Israel's approach to managing the identified areas of complexity for cyberspace, such as the decision to manage cyberspace as an integrated domain of warfare; the complexity of 'unknown' threats through strategic ambiguity; technical threats through a drive for superiority; the problems of collective attribution through arms-length alliances; and the lack of accepted norms by supporting them in concept but acting in accordance with Israel's wishes.

3.6 Risks of treating cyberspace as integrated domain of warfare

The clearest example of how Israel's operationalisation of deterrence policy may be creating risk is through the practical decision to treat cyberspace in the same way as any other potential battlespace: as a domain of warfare that must be secured.[541] The result of this decision is that the cyber domain is treated as an integrated part of the Israeli battlespace.[542] This is significant, because Israel expects conflict to be ongoing, views attacks as a part of daily life on a new front line, and asserts superiority is thus judged to be critical.[543]

The characterisation of cyberspace as a domain of warfare is not unique to Israel, but the leadership of the military in securing the domain has deep ramifications both for ideas about success and acceptable behaviour. Embedded since the outset of Israeli policy and strategy for information and communication technology,[544] this characterisation is widely accepted and has several important implications for deterrence. First, by designating cyberspace as a 'strategic and operational battle zone' in 2009[545] the IDF

[539] Bar, 'Israeli Strategic Deterrence Doctrine and Practice', p.324.
[540] Isaac Kfir, 29 November 2018, 'Israel's Cyber Ecosystem: Why the Start-up Nation Eschews Doctrines and Silos When It Comes to Cybersecurity', *Asia & The Pacific Policy Society: Policy Forum* [blog]
[541] Housen-Couriel, 'National Cyber Security Organisation: ISRAEL'; Cohen, Freilich, and Siboni, 'Israel and Cyberspace: Unique Threat and Response', p.311.
[542] Adamsky, 'The Israeli Odyssey toward Its National Cyber Security Strategy', p.113.
[543] Frantzman, 'Cyber Warfare, Israel, Iran and the New Way of Total War', 1.
[544] Netolicka and Mares, 'Arms Race "in Cyberspace" - A Case Study of Iran and Israel', p.426.
[545] Baram, 'Israeli Defense in the Age of Cyber War', p.2.

claimed, and has since maintained, a lead role in both policy development and operational activities that aim to deter attacks on Israeli interests in cyberspace. Adamsky views this leadership role as a key risk, as the IDF's unchallenged superiority in national security affairs means the political oversight of Israel's deterrence approach is less than one would expect; further, this military leadership results in a widespread assumption that the more force is employed, the more deterrence will be generated.[546] Here we can consider a 2014 IDF blog post, which cited a Colonel N. in the IDF's cyber defense division stated that the IDF must focus on 'preventative strikes'.[547] The subsequent capture of an Iranian arms ship in the Red Sea – a naval interception 1500 kilometres from Israeli shores – relied heavily on advanced cyber and communications abilities.[548] Israel considers such activities, comprised of both cyber-only and hybrid capabilities, as essential for signalling and deterrence.[549] But while designating cyberspace as an integrated domain of warfare inherently linked to the other domains makes sense in the Israeli context, where threats are complex, linked to known adversaries and require a whole of society approach,[550] there is also the risk that Israel may be creating the conditions for unintended escalation.

To illustrate this further it is helpful to return to the Israel–Iran relationship. Iran is one of Israel's main adversaries,[551] it poses a recognised threat to Israeli interests through cyberspace, and has done so over a period of years dating back to at least 2009.[552] More recently, Iran has been thought responsible for a number of cyber-attacks on Israel, including attacks on critical infrastructure such as water and sewerage treatment facilities in late April 2020.[553] When this occurred, the head of the INCD, Yigal Unna, declared that it would be remembered as a 'point of change in the history of modern cyberwars… cyber winter is coming and coming faster than even I expected'.[554]

The Israeli response to this attack demonstrates both how escalation could occur very quickly, and the difficulty posed by attacks which occur in the cyber domain but have kinetic, or 'real-world' effects. Tel Aviv conducted a widely attributed (but not officially acknowledged) cyber-attack against Iran's Shahid Rajaee port on May 9, 2020.[555] The attack halted shipping traffic, leading to delays of several days.[556] Israel

[546] Adamsky, 'From Israel with Deterrence: Strategic Culture, Intra-War Coercion and Brute Force', p.177.

[547] Sally Zahav, 27 August 2014, 'Middle East and Terrorism: IDF Blog: The Attack against Israel You Haven't Heard About', *Middle East and Terrorism* [blog], http://israelagainstterror.blogspot.com/2014/08/idf-blog-attack-against-israel-you.html

[548] Dombi, Ami Rojkes, 14 April 2014, 'The IDF is ready for the cloud challenge', *Israel Defense*

[549] Raska, 'Confronting Cybersecurity Challenges: Israel's Evolving Cyber Defence Strategy', 6.

[550] 'Cabinet Approves Establishment Of National Cyber Authority', 2015, *Info – Prod Research (Middle East)*

[551] Frei, 'Israel's National Cybersecurity and Cyberdefense Posture', 7.

[552] 'Iran/Israel/United States: Presidential Candidate: US, Israel Wary of Iran's Cyber Power'; Netolicka and Mares, 'Arms Race "in Cyberspace" - A Case Study of Iran and Israel', p.415.

[553] Gil Baram Lim Kevjn, 'Israel and Iran Just Showed Us the Future of Cyberwar With Their Unusual Attacks', *Foreign Policy* (blog), accessed 8 August 2021, https://foreignpolicy.com/2020/06/05/israel-and-iran-just-showed-us-the-future-of-cyberwar-with-their-unusual-attacks/.

[554] Yigal Unna, cited in Lobel, 'Israel and Iran: "Cyber Winter Is Coming"'.

[555] 'A New Level in the Cyber War between Israel and Iran | INSS', June 3 2020, https://www.inss.org.il/publication/iran-israel-cyber-war/.

[556] 'Israel Strikes Back at Iran - the Constant Cyber Warfare Paradigm - The Jerusalem Post', accessed 8 August 2021, https://www.jpost.com/israel-news/israel-strikes-back-at-iran-the-constant-cyber-warfare-paradigm-628535.

considers this event as a demonstration of 'old-fashioned deterrence' and a disproportionate response to discourage attackers.[557] Gil Baram has argued the attack on the port is evidence Israel is pursuing conventional deterrence, as the attack served as a signal to Iran that attacks on critical infrastructure would not be tolerated; demonstrated Israel's options for retaliation; and communicated Israel's capabilities and commitment to respond to future cyber-attacks.[558] Yet these attacks from Iran are, firstly, not a new problem and, secondly, could equally be argued as occurring in response to Israeli 'deterrence' activities in cyberspace such as their reported participation in the Stuxnet attacks on Iranian nuclear centrifuges.[559] It is by no means clear that any measures Israel has taken – either in cyberspace or in any other domain – have had any demonstrable effect on deterring Iran from conducting cyber-attacks on Israel.[560] This is where Israel's definition of deterrence success as survival allows Israel to continue claiming its efforts are a success regardless of such attacks. Further, although Israel's cyber interactions with Iran are far more public than that with other nations, there are still many cases where Israel maintains ambiguity regarding its actions. This notion of strategic ambiguity is not without risk, however, particularly as other nations choose to treat cyberspace as a separate domain of warfare.

3.7 Risks of 'strategic ambiguity'

Israel's decision to respond to cyber-attacks without directly claiming responsibility is neither unique to cyberspace nor a new policy concept[561], but it still carries significant risk. This strategic ambiguity, or opaqueness,[562] has its origins in the Cold War[563] and refers to Israel's deliberately ambiguous position on whether or not it has nuclear weapons whereby Israel

> will not be the first state to use nuclear weapons into the region, but that it will keep a nuclear option just in case some other state in the region acquired a nuclear weapon.[564]

[557] Ibid

[558] Lim, 'Israel and Iran Just Showed Us the Future of Cyberwar With Their Unusual Attacks'.

[559] Cohen, Freilich, and Siboni, 'Israel and Cyberspace: Unique Threat and Response', p.314; Stuxnet, and its role as part of deterrence is also discussed in further detail in Chapter 5

[560] 'A New Level in the Cyber War between Israel and Iran | INSS'; Yaakov Lappin, 'Iran "Working Systematically to Build Serious Cyber-Attack Capabilities"', JNS.org, 6 August 2021, https://www.jns.org/iran-is-working-systematically-to-build-serious-cyber-attack-capabilities/; 'Netanyahu: Iran Attempts "Daily" Cyber Attacks on Israeli Infrastructure', Iran International, 29 January 2019, https://iranintl.com/en/world/netanyahu-iran-attempts-daily-cyber-attacks-israeli-infrastructure.

[561] Basrur, 'Minimum Deterrence and India's Nuclear Security', p.28.

[562] Ofer Israeli, 'Israel's Nuclear Amimut Policy and Its Consequences', *Israel Affairs* 21, no. 4 (2015): p.542

[563] For a more detailed treatise on Israel's nuclear policies and history, see Yoel Cohen, 2005, 'Whistleblowers and the Bomb: Vanunu, Israel and Nuclear Security' , London: Pluto Press; Shai Feldman, 1982, 'Israeli Nuclear Deterrence: A Strategy for the 1980s', New York: Columbia University Press

[564] Prime Minister Itzhak Shamir originally made this statement in 1983, cited in Yoel Cohen, 2005 'Whistleblowers and the Bomb: Vanunu, Israel and Nuclear Security', London: Pluto Press, p. 10; see also Michael I. Handel, 1973, 'Israel's Political Military Doctrine', Centre for International Affairs, Harvard University Occasional Papers in International Affairs, no. 30, p.66

Described as 'a wink, a smile and a pat on the back',[565] this posture is viewed as having been a successful deterrent in the Arab–Israeli conflict and thus a model for cyberspace.[566] Yet it has also shifted over time, with Israel's position on nuclear weapons became increasingly clear. Shmuel Bar argues it is more accurate to describe Israel as a 'non-declared nuclear power' today rather than maintaining nuclear ambiguity: a policy observed more in the breach than in the observance.[567] Yet despite having shifted somewhat, the fig leaf of deniability still works to Israel's advantage. Adversaries have little doubt about Israel's nuclear capabilities, and the Israeli government is not constrained in the same ways declared nuclear powers are. Given the overall perception of strategic ambiguity as contributing to deterrence success it is unsurprising this concept has also been applied to cyberspace. Israel often neither confirms nor denies cyber-attacks, which Cohen et al argue allows Israel to avoid taking responsibility and lessens the chance of reprisals.[568] And yet as with nuclear ambiguity, this cyberspace 'strategic ambiguity' is in fact not particularly ambiguous; Israel is increasingly choosing to let its role in cyber-attacks be known.

An example of this is Israel's participation in the Stuxnet attack, or more accurately, participation in the suite of cyber capabilities known as Olympic Games that was used for the Stuxnet attacks.[569] Despite the fact the Israeli government has never publicly admitted its participation, once the attacks became public, press reports from both Israel and the US not only linked Israel as a contributing nation, but named the unit responsible as the cyber unit within Intelligence Corps 8200.[570] And while press speculation is hardly conclusive, what happened next was illuminating. This was an attack known as Operation Flame (based on the same US National Security Agency (NSA) virus from which Olympic Games was derived) which wiped the hard drives at Iran's Oil Ministry and the National Iranian Oil Company.[571] One day after Operation Flame struck Iran, Israeli's Vice Premier and Minister of Strategic Affairs Moshe Ya'alon praised Israel's 'superior technology' and stated 'These achievements of ours open all kinds of possibilities for us'.[572]

Such statements from a senior Israeli minister in a public forum, while not a formal acknowledgment of responsibility, are fairly unambiguous and Israel views these behaviours as helping build credibility, both in the scope of its capabilities and its willingness to use them. Yaakov Katz, an Israeli reporter, argues it does not matter which state conducted Flame – the important thing is that Iran feels vulnerable.[573] But

[565] Yaakov Katz, 2012, 'Israel's Cyber Ambiguity', *The Jerusalem Post*

[566] Yoel Cohen, *Whistleblowers and the Bomb: Vanunu, Israel and Nuclear Secrecy*, p.8

[567] Bar, 'Israeli Strategic Deterrence Doctrine and Practice', p.342.

[568] Cohen, Freilich, and Siboni, 'Israel and Cyberspace: Unique Threat and Response', 314; Martin C. Libicki et al., *Cyberdeterrence and Cyberwar*, (Santa Monica, CA: RAND, 2009)

[569] Kaplan, *Dark Territory: The Secret History of Cyber War*, 208.

[570] Raska, 'Confronting Cybersecurity Challenges: Israel's Evolving Cyber Defence Strategy', 6; David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, 1st ed., (New York: Crown Publishers, 2012); Cohen, Freilich, and Siboni, 'Israel and Cyberspace: Unique Threat and Response', 314.

[571] 'Meet "Flame," The Massive Spy Malware Infiltrating Iranian Computers | WIRED', accessed 25 June 2021, https://www.wired.com/2012/05/flame/.

[572] Katz, 'Israel's Cyber Ambiguity'.

[573] Ibid

making Iran feel vulnerable carries risk; and despite these Israeli actions Iran has not been deterred from conducting cyber-attacks. Indeed, Fred Kaplan argues it was the Stuxnet and Flame attacks that spurred Iran to create a cyber war unit, and that the Shamoon attack four months later on against a US-Saudi oil company was a direct response.[574] This type of activity does not indicate deterrence has been successful. This is the case regardless of Israel's definition of deterrence success. As Bar has argued, successful deterrence can only be measured in retrospect by the duration between the round of hostilities during which an attempt was made to restore deterrence, and the next round of warfare.[575] If he is correct, then the relatively small gap between cyber-attacks and counter-attacks in 2012 indicates that strategic ambiguity had not achieved its desired end-state, and that this may be an example of Israeli deterrence in cyberspace causing escalation – rather than deterrence – despite the application of Israeli capabilities, increased credibility of responses, and unofficial communication of Israeli red lines surrounding critical infrastructure.

3.8 Risks of the US partnership

The whole Olympic Games program further highlights Israel's sometimes awkward international relationships, which may also bring the risk of unintended escalation. Indeed, Israel's relationship with the US is a significant issue here. The relationship, while helpful for building shared capabilities, credibility, and communicating deterrence intent and goals between partners is also viewed as being deeply problematic by Israel's adversaries, indicating that it is a contributing factor to escalation. The deterrence efforts of states do not occur in a vacuum and Israel is no exception: its deterrence approach for cyberspace is influenced by the international environment and its relationships with partners, and most particularly the US. Understanding the impact of this relationship is critical for this research given the significant differences in the US approach to deterrence[576] and the potential to be viewed by adversaries as a serious security threat.

While the US–Israel relationship has proved dynamic but durable[577], it is not a formal alliance but rather a strategic partnership, and as such does not come with binding commitments.[578] But despite the lack of a formal strategic alliance, Israel has worked to build a close relationship with the US on cybersecurity, expending significant effort towards creating strong ties with US cyber defence agencies in particular.[579] Consider that in 2016 Israel signed a joint declaration with the US to increase 'operative cyber defense cooperation'.[580] Further, Israel has close ties with the US National Security Agency,[581] and in 2016 signed

[574] Kaplan, *Dark Territory: The Secret History of Cyber War*, 213.
[575] Bar, 'Israeli Strategic Deterrence Doctrine and Practice', p. 346.
[576] The US approach is examined in detail in the next case study chapter, Chapter 4.
[577] Aharon Klieman, 'Doomed to Succeed: The US–Israel Relationship from Truman to Obama', *Israel Journal of Foreign Affairs* 10, no. 2 (3 May 2016): 305–6, https://doi.org/10.1080/23739770.2016.1197627.
[578] Frei, 'Israel's National Cybersecurity and Cyberdefense Posture', p. 18.
[579] Ibid.
[580] Barbara Opall-Rome, 'US-Israel Sign Cyber Defense Declaration', *Defense News International* 31, no. 23 (2016)
[581] Frei, 'Israel's National Cybersecurity and Cyberdefense Posture', p. 18.

a cyber defense declaration which included real-time operational knowledge sharing between each nation's Computer Emergency Response Teams (CERTs).[582] This agreement was an acknowledgment of a surprisingly close relationship. While the US and Israel have shared a Memorandum of Understanding on matters of homeland security since 2008,[583] the decision to announce the 2016 agreement demonstrates that Israel accepted the need for alliances, although as Cohen et al note Israel needs to deepen such relationships within the limits of operational security.[584] The Israeli Prime Minister's office stated at the time that the declaration 'highlighted the importance of an international integration of forces between the two countries to more effectively deal with joint cyber threats'.[585] Prime Minister Netanyahu has noted the importance of cooperation with Washington on matters pertaining to cybersecurity, stating in 2017 that 'we are better together'.[586] The relationship also extends to information sharing regarding governance, as evidenced by the then IDF Chief of Staff Gadi Eizenkot visiting NSA headquarters and Cyber Command in 2016 while considering the upgrading of Israeli force structure to better manage the lines between intelligence gathering and defense/offense.[587] Further, the working level is also included: in 2017 the US and Israel commenced a bilateral cyber working group, which aimed to 'defend critical infrastructure against attackers and track down perpetrators' and strengthen bilateral ties on cyber issues.[588] The sharing of capabilities and better communication between partner nations could be argued to help bolster each state's deterrence posture. Indeed, US official Thomas Bossert argued in 2016 that the agility Israel had in developing solutions will 'result in innovative cyber defenses that we can test here and take back to America.'[589]

But the relationship faces significant tests in the deterrence space, as despite each having a commitment to deterrence, the two define and enact deterrence very differently. These differences may cause tensions in the strategic partnership, as demonstrated by the Israeli approach on the attribution of cyber-attacks. While the US has worked to build coalitions of like-minded allies before attributing cyber-attacks such as NotPetya or Wannacry, Israel is not only willing to attribute responsibility for cyber-attacks on its own, and it has also demonstrated the willingness to respond to such attacks with kinetic force. For example, on May 4, 2019 Hamas allegedly conducted a cyber-attack on Israeli websites. In response the IDS conducted an air strike, destroying a building in the Gaza Strip. On May 5, the Israeli government released a statement that the strike was specifically aimed at defeating a cyber-attack in battle.[590] A

[582] Opall-Rome, 'US-Israel Sign Cyber Defense Declaration'; Adamsky, 'The Israeli Odyssey toward Its National Cyber Security Strategy', p. 124.
[583] Frei, 'Israel's National Cybersecurity and Cyberdefense Posture'.
[584] Cohen, Freilich, and Siboni, 'Israel and Cyberspace: Unique Threat and Response', p. 316–17.
[585] Opall-Rome, 'US-Israel Sign Cyber Defense Declaration'.
[586] 'US, Israel Set up Team to Combat Cybersecurity Threat', *The Times of Israel*, 2017
[587] 'Israel Spies Opportunity as U.S. Gives Cyber Command Major Upgrade', *Haaretz*, 2017
[588] 'US, Israel Set up Team to Combat Cybersecurity Threat'.
[589] Ibid.
[590] Judah Ari Gross, 'IDF Says It Thwarted a Hamas Cyber Attack during Weekend Battle', 5 May 2019, *The Times of Israel*

Shin Bet official stated 'Israel's ability to defend itself and thwart cyber-attacks means the Hamas terror group's efforts to carry out attacks in the cyber realm fail time and time again'.[591]

This kinetic response to an alleged cyber-attack appeared to set two new precedents for Israel. First, it demonstrated a seeming new ability and willingness to attribute a cyber-attack in real or close to real time.[592] Second, it demonstrated Israel's willingness to respond to a cyber-attack with 'disproportionate' kinetic force. Further, while the perceived threat to its interests was relatively low-level – the Hamas 'attack' involved defacing public websites – it demonstrated Israel is unwilling to allow further development of capabilities by its adversaries. This Israeli response appears to demonstrate Israel's long-established principle that deterrence is achieved and maintained through periodic episodes of deliberately disproportionate force;[593] but is a notable exception to their principle of often not publicly attributing attacks, or claiming direct responsibility for responses.[594] However it may be more accurate to argue that Israel is comfortable attributing attacks when the threat is sufficiently clear and a response is possible, thus continuing to enhance Israel's credibility.

Although this issue is examined further in Chapter 5, it is worth noting the concern this response caused in the US among policymakers – most specifically that the Israeli response was potentially an unwarranted escalation.[595] The differences in how the US and Israel define and manage attribution are confusing for practitioners within each state, let alone adversaries to understand, and when this confusion is coupled to Israel's continued drive for superiority in cyberspace it is understandable that adversaries may choose to respond by escalating both their attacks and capabilities.

3.9 Risks of seeking superiority

Israel's decision to significantly invest in cyber capabilities and repeated efforts to damage the cyber capabilities of its adversaries are both clear attempts at deterrence, and understandable in the context of Israel's broad deterrence approach, which relies on superior technology.[596] However this investment also carries the significant risk of causing adversaries to respond with similar drives, potentially causing a cyber arms race it cannot control. To put this in context, Israel's drive for superiority in cyberspace is comprehensive, spanning both civilian and military enterprises and includes considerable financial,

[591] Elias Groll, 'The Future Is Here, and It Features Hackers Getting Bombed', *Foreign Policy* (blog), accessed 8 August 2021, https://foreignpolicy.com/2019/05/06/the-future-is-here-and-it-features-hackers-getting-bombed/.
[592] Groll, 'The Future Is Here, and It Features Hackers Getting Bombed', *Foreign Policy*
[593] Bar, 'Israeli Strategic Deterrence Doctrine and Practice', p.329.
[594] Bar, p.351.
[595] 'Israel Responded to a Hamas Cyberattack with an Airstrike. That's Not Such a Big Deal. - *The Washington Post',* accessed 8 August 2021, https://www.washingtonpost.com/politics/2019/05/09/israel-responded-hamas-cyberattack-with-an-airstrike-thats-big-deal/; 'Did Israel Have the Right to Bomb Hamas' Cyber HQ?', Defense One, accessed 8 August 2021, https://www.defenseone.com/ideas/2019/05/did-israel-have-right-bomb-hamas-cyber-hq/156829/; Groll, 'The Future Is Here, and It Features Hackers Getting Bombed'.
[596] Eizenkot, 'Deterring Terror: How Israel Confronts the Next Generation of Threats', p.5.

military and governance effort put into building its cyber capabilities.[597] Indeed, Israeli companies are at the forefront of global technology; in terms of global private investment, private cybersecurity in Israel is second only to the US.[598] And the IDF has built, maintained and deployed sophisticated cyber capabilities, including conducting known attacks and the use of offensive cyber capabilities.[599]

But how sophisticated are these capabilities, and are they having the desired effect? Here Cohen et al argue Israel's efforts to improve capability were specifically designed to mitigate IDF concerns that its reliance in technology could leave it exposed during conflict rather than for explicit deterrence purposes.[600] Given the centrality of technological superiority to the IDF, this concern is unsurprising. Developing and maintaining a technological and human capital edge is seen as a key component of Israel's deterrent image;[601] the repeated use of force in different circumstances demonstrates Israeli military, technology, intelligence and social-robustness superiority.[602] This argument demonstrates a strong perceived link between Israel's possession and use of capabilities and the credibility of their deterrence approach.

This is partly due to the strong role the military has in deterrence in cyberspace. Militaries tend to perceive the acquisition and use of advanced capabilities as advantageous, and Israel is no exception. For example, Bar notes the strength of the military in Israel, the relative size of the defence budget and the absence of separation between the civilian Ministry of Defense and the IDF in the realm of acquisition gives rise to the popular saying that 'Israel is not a country with an army – the IDF is a military which has a country'.[603] This role extends to cyberspace, where it is difficult to overstate the role and centrality of the IDF in shaping deterrence policy and practices and its preference for pre-emptive strikes. This is further highlighted by the 2014 statements the IDF made regarding being surprised by adversaries' cyber capabilities, and the resulting need to focus on preventative strikes against cyber-attacks.[604]

> During Operation Protective Edge, we saw attacks on a greater scale and on a more sophisticated level. A significant amount of thought and investment stood behind the attacks we saw.[605]

Gil Baram argues that such activities, even cyber warfare, are preferred because it allows Israel to initiate operations against remote targets without risking lives, and gains Israel worldwide prestige – goals clearly linked to Israel's capability, credibility and communication efforts. But Netolicka argues Israel's statements and actions in cyberspace instead signalled offensive intent, and points to the problem of

[597] Netolicka and Mares, 'Arms Race "in Cyberspace" – A Case Study of Iran and Israel', p.410; Tabansky, 'Israel Defense Forces and National Cyber Defense', pp.57-58

[598] Adamsky, 'The Israeli Odyssey toward Its National Cyber Security Strategy', p.26.

[599] Frei, 'Israel's National Cybersecurity and Cyberdefense Posture', p.7.

[600] Cohen, Freilich, and Siboni, 'Israel and Cyberspace: Unique Threat and Response', p. 311.

[601] Bar, 'Israeli Strategic Deterrence Doctrine and Practice', p. 327.

[602] Ibid.

[603] Ibid

[604] Zahav, 'Middle East and Terrorism'.

[605] Ibid

mutual perceptions of threats and subsequent reactions being distorted.[606] Regardless of intent, however, the practical reality remains that Israel's adversaries will continue to view its development of capabilities as inherently threatening, and potentially leading to escalation.[607]

Taken as a whole, Israel's public policy measures since 2008 demonstrate a substantial effort towards increasing Israel's capability, credibility and communication efforts in cyberspace. The decision to not only adopt but publish multiple government resolutions, a whole of nation cybersecurity strategy, and explicit defense doctrine, as well as commenting publicly on cybersecurity matters points to a mature policy approach. Moreover, by basing that approach on existing Israeli deterrence principles – including willingness to respond to all attacks with kinetic force, treating cyberspace as a domain of warfare, building Israeli capability superiority, and maintaining strategic ambiguity when deemed appropriate – Israel has created a cohesion in their policies that is remarkable.

But does this constitute a deterrence approach? Gil Baram and Kevin Lim argue that Israel's progress in developing and using its military capabilities in response to cyber-attacks since 2015 is evidence that their doctrine has been successful and that the policies adopted to date comprise a deterrence strategy.[608] Adamsky argues Israel's approach to deterrence in cyberspace meets Israel's definition of cumulative deterrence, including the requirement for periodical execution of threats seen as essential for communicating resolve and capability.[609] But as for any other nation or domain, establishing deterrence credibility is complex and Israel judges its credibility has previously failed.[610] Indeed, Adamsky argues that the Israeli approach is much closer to coercion than deterrence, pointing out that Israeli operations resonate more with brute force;[611] however such use of force is characteristic of the Israeli view that deterrence is not an end state but a cumulative process that includes sporadic clashes to 'refresh the rules of the game'.[612] Doran Almog, meanwhile, sees this as a careful and deliberate choice, based on experience:

> Unlike classic deterrence as practiced during the Cold War, whose success hinged on a bipolar standoff that held in check any impulse to launch a nuclear first strike, cumulative deterrence is based on the simultaneous use of threats and military force over the course of an extended conflict.[613]

That said, such an approach to deterrence in cyberspace may be dangerous; reliance on pre-emptive strikes and visible punishments carries risk, particularly that of inadvertent escalation. As Bar notes, a

[606] Netolicka and Mares, 'Arms Race "in Cyberspace" – A Case Study of Iran and Israel', p.423

[607] Jarno Limnéll, 2016, 'The Cyber Arms Race Is Accelerating – What Are the Consequences?', *Journal of Cyber Policy,* 1:1, 55

[608] Lim, 'Israel and Iran Just Showed Us the Future of Cyberwar With Their Unusual Attacks'.

[609] Adamsky, 'From Israel with Deterrence: Strategic Culture, Intra-War Coercion and Brute Force', p.166.

[610] Bar, 'Israeli Strategic Deterrence Doctrine and Practice', 350.

[611] Adamsky, 'From Israel with Deterrence: Strategic Culture, Intra-War Coercion and Brute Force', p.171.

[612] Samaan, 'From War to Deterrence?', p.488.

[613] Doron Almog, 2004, 'Cumulative Deterrence and the War on Terrorism', *Parameters,* 3:4, 4-19

cyber-attack may succeed beyond the expectations of the perpetrator and result in escalation to the level of a full-scale response.[614] Thus while the policy and literature have so far indicated that Israel judges that it is largely meeting its own definition of deterrence success for cyberspace and this definition does meet the requirements of basic deterrence, the Israeli reliance on offensive measures in operationalisation and definition of success as cumulative, renders its actions closer to acts of war and thus at serious risk of creating an arms race, rather than deterrence. This chapter now moves to exploring whether this potential finding is supported by Israeli cybersecurity experts.

3.10 How effective is Israeli deterrence policy? Perceptions from Israeli policy experts

As outlined in Chapter 2, this thesis is framed around considering states' declared policy against expectations related to deterrence in order to generate comparable findings into whether states' cybersecurity approaches indeed met a definition of classic deterrence; consider how states' different approaches influenced their operationalisation of deterrence; and consider whether states judged their deterrence efforts a success. The inclusion of first-hand views from experts directly involved in creating, implementing, or assessing Israel's deterrence policies increases the likelihood that the findings generated from this research are accurate, and helps ensure the appropriate strategic context is taken into account. This section of the case study provides an overview of participant expertise and summarises their overall views on success before considering each deterrence requirement in turn.

The analysis then considers how the challenges of deterrence for cyberspace influenced Israel's operationalisation of each requirement, before considering how the expert participant views compared to the findings from the policy and literature. Table 3.1 provides a brief summary of the Israeli participant's background for context. As noted in Chapter 2, the interviews were structured to determine whether Israeli policy aligned or differed from the classic conception of deterrence requirements of capability, credibility and communication. This structure generated data on each of the three individual requirements, as well as on the perceived success of deterrence as a whole. The interviews also allowed participants significant scope to provide additional information, and used the snowball technique to probe further, particularly where the data appeared to contradict the policy, literature or both. The participants for this study were recruited from academia, think tanks, government, and former government backgrounds; however, categorising each participant on the basis of their employment proved complex as all crossed at least two of these categories, and most crossed three.[615]

[614] Bar, 'Israeli Strategic Deterrence Doctrine and Practice', p.348.

[615] Nine participants were interviewed; only one declined to be recorded. The interviews were conducted in participant's office space in Israel.

Table 3.1 Israeli participant expertise and perceptions of deterrence

Participant	Capability	Credibility	Communication	Overall
I1: Senior former military scientist and government cyber adviser	Yes	Yes	Yes	Yes, unequivocally
I2: Senior cyber researcher	Yes	Yes	Yes	Yes, but noted some concerns around use of deterrence as a political tool
I3: Senior former government expert in cybersecurity and warfare	Yes	Yes	Yes, with caveats on media messaging	Yes
I4: Cyber researcher	Yes	Yes	Yes	Yes, but noted questions about long-term efficacy as technology changes
I5: Former senior government cyber official	Yes	Yes	Yes	Yes, but need to note that cyber is a step change for humanity, there is some uncertainty as a result
I6: Former cyber intelligence professional	No	No	No	No, because of the lack of a definitive capability to deter all attacks
I7: Senior cyber researcher	Yes	Yes	Yes	Yes, but caveats around the fact the space is evolving and Israel needs to understand it better

3.11 Defining deterrence success: On Israel's terms

The participants were remarkably consistent on the importance and success of deterrence for Israel's security, and viewed the application of deterrence in cyberspace as a logical extension of this approach.

Participants repeatedly highlighted the role deterrence had played in Israel's survival since 1948 and noted deterrence in cyberspace was part of a calculated overarching deterrence strategy. In considering deterrence, Participant I1, a senior former military scientist and government cyber adviser, referred immediately to a picture of former Israeli President Ben-Gurion and stated:

> at the establishment of the Israeli state in 1948, in order to survive, he said we cannot compete with our neighbours here in numbers, in quantities, therefore we should compensate in quality… and one of the main elements was of course deterrence. For us war is bad news.[616]

Or as Participant I3, a senior expert in cybersecurity and warfare, characterised it '… [Deterrence] is not tiny. It is why Israel exists.'[617] Participants also broadly agreed with the Israeli approach to deterrence in cyberspace being delivered not only through threats, but also through punishment and pre-emptive action. This included a consistent view that there would always be times where a pre-emptive strike was necessary. Participant I4, a cyber researcher, defined this approach as 'The basic definition of deterrence, you want to prevent your adversary to do something. Not after he did something. You want to prevent an undeterrable action.'[618] Participant I6, a former cyber intelligence professional, echoed this view and pointed to the lessons from Israel's history as to why deterrence remained a core principle in cybersecurity policy:

> And when you get hit, it's too late. That's the problem. We are in a very tough neighbourhood. We have a lot of enemies that want to kill us. We can't lose. Because for us, it would only be once, one time. Not such as for our enemies, that have 22 countries and many, many millions of people.[619]

As with Israel's broader approach to deterrence, conflict was viewed as a necessary condition for creating successful deterrence in cyberspace. Participant I3 explained the importance of using force to reinforce deterrence:

> We have to make this as short as possible, because we don't have any strategic depth, not only in terms of territory, but we don't have the economic strategic depth to have long wars. We need to have decisive war in a very short time… so the goal here is to renew your deterrence.[620]

Thus, as suggested in previous sections of this chapter, the necessity of deterrence for Israel's survival is accepted by participants, as was the perception Israel faced serious threats to its interests in cyberspace. However, there were differing ideas about the nature and origins of those threats, with some participants focusing on Israel's 'traditional' enemies, and others also including newer threats. The threat posed by

[616] Participant I1 Quote 15, p.4
[617] Participant I3, Quote 22, p.4
[618] Participant I4, 8, p.2
[619] Participant I6, Quote 24, p.5
[620] Participant I3, Quote 6, p.1

Israel's historic enemies[621] noted earlier in this chapter was described by Participant I3 in the bluntest terms: 'Deterrence means you want to make sure the Arabs, it's very simple, we have one enemy here called the Arabs, the Arabs are not tempted to exercise their force against Israel.'[622] And Participant I4 noted 'We can say Iran of course, but I think the cyber threats are the same as the not-cyber threats.'[623] Indeed, the role Iran plays in threatening Israel's interests in cyberspace demonstrates the difficulty in distinguishing between state and non-state threats in cyberspace. Participant I3 noted, 'Iran is leading the capabilities and sharing some of these capabilities with Hezbollah and Hamas.'[624] Participant I2 described this issue as part of the problem of the cyber domain more broadly:

> Whether these actors are terrorists of state sponsored, or partly state sponsored, or just businessmen who want to get money, this is one of the challenges in the cyber domain – this is a dual-use problem.[625]

Several participants argued that this meant it was important to include non-state actors in their conceptions of deterrence, as non-state actors were viewed as posing a significant risk to Israel through cyber-attacks. Participant I7, a senior cyber researcher noted:

> I go around and talk, keep trying to cancel this false dichotomy between state-on-state actors. It's a very American thing, it's not true throughout history, it's not true today in most of the world. There's a whole range of interactions between states and other non-formal assets that states have. In that case it's relatively futile to continue to think about responses when you only constrain yourself to state-on-state work.[626]

This view seems to demonstrate a recognition that the issue of non-state actors merited serious attention. But participants offered differing views on the potential emergence of new threats, with some participants considering the threat landscape as changing due to the opportunities posed by cyber. Participant I3 stated, 'The Russians are active, actually very active, and China.'[627] Israel maintains a complex relationship with Russia, and participants were wary of its activities and intent. Participant I7 noted, 'There are a lot of attempts to prevent any confrontation.'[628] Participant I2 went further, stating

[621] All but one of the Israeli participants repeatedly referred to their adversaries as 'the Arabs'. This term includes both state and non-state actors, and Arabic countries such as Syria and Lebanon. However it also included Iran, in every interview, despite Iran not being an Arabic nation.

[622] Participant I3, Quote 4, p.1

[623] Participant I4, Quote 14, p.3

[624] Participant I3, Quote 23, p.4

[625] Participant I2, Quote 19, p.4

[626] Participant I7, Quote 28, p.5

[627] Participant I3, Quote 27 p.5

[628] Participant I7, Quote 12, p.2

> From what I understand Russia is the biggest threat… if we compare the interests of Israel and Russia we see some issues that the interests of both sides are not converging so it is possible that Russia is a challenge, and also China to some extent is a challenge.[629]

The notion of China as a potential threat to Israeli interests was also raised by Participant I6, who noted that this might require a review of deterrence approaches: 'China is something else. And, of course, what is good for Iran is not good enough for China.'[630] But Participant I7 noted the reason for China being considered a threat was due to Israel's enmeshment with the US. He considered that this was indicative of an issue of relationship management rather than direct threat. 'China is less of an issue, it's an issue for Americans because they are putting blunt pressure on allies, so that's the issue here.'[631] While neither China nor Russia are listed in Israel's public threats their repeated mention by participants supports the argument that Israel is aware of emerging threats against its interests in cyberspace from high-technology nations. And participants also noted that threats to Israel from cyber-attacks needed to be considered in the context of broader security threats. Participant I4 argued that cyberspace did not change the nature of the threats faced by Israel.

> Cyber technology enables countries or actors to do many things they used to do but in much larger scale. It's not a new thing, the cyber technology just changes the scales. It's not new, just looks different.[632]

And some participants argued the lack of deaths caused by cyber-attacks meant that for Israel, cyber is unlikely to be considered its most pressing threat. Participant I7 characterised it thus:

> In the general security priority, cyber shouldn't be one of the top priorities because it's quite clear that casualties aren't an issue here. In our strategic context at this stage the range of uses for cyber is limited or maybe different… they don't necessarily frighten us as much as conventional or simple casualties or dumb attacks.[633]

Despite some disagreement over the scope and seriousness of the threats posed by states such as Russia and China, participants therefore largely agreed that regardless of where cyber threats emanate from they are serious enough to require significant government attention, and such attention should be focused through Israel's existing deterrence approach. But how closely does that approach mirror a classic deterrence approach? I now turn to examining each of the key deterrence requirements in turn to answer this question and further explore how Israel's operationalisation of each element may be leading towards the risk of unintended escalation.

[629] Participant I2, Quote 24, p.5
[630] Participant I6, Quote 6, p.2
[631] Participant I7, Quote 13, p.3
[632] Participant I4, Quote 3, p.1
[633] Participant I7, Quote 14, p.3

3.12 Perceptions of capability: Superiority as necessity

As revealed in Israeli policies, the Israeli approach towards capability in general is that superiority is necessary for Israel's deterrence success – and thus survival. Cohen et al. argue this view developed in response to the severity and immediacy of the threats Israel faces through cyber-attacks.[634] However, this approach is not unique to cyberspace. Maintaining a capability edge is also part of a long-established Israeli defence and strategic policy tradition. This view extends to participants' views of capabilities in cyberspace: having superior capabilities was not only viewed as necessary, but their regular use formed an important part of Israel's credibility and communication of deterrent intent. Further, the concept of capabilities was described by participants as comprising not only cyber capabilities but the full range of available government levers.

Participant I5, a former senior government cyber official, expressed capability superiority in technological terms as part of Israel's broader approach to staying ahead of the curve: 'We need to be in front of everything, at least in our neighbourhood.'[635] This approach fits within Israel's broader conception that technological superiority is a necessary requirement for deterrence. But participants were careful to note that Israel could, and indeed should, use any capabilities it chose in response to cyber-attacks, including the use of kinetic force. Participant I1, a senior former military scientist and cyber adviser, argued this was absolutely necessary for deterrence: 'You can deter attacks, any type of attack if you are ready to retaliate heavily, but doesn't mean necessarily by cyber.'[636] Participant I1 further pointed to the example of economic measures for deterrence, which he considered had been successful:

> What happens here daily, they are launching rockets, we have other means than military to show them they will not gain too much, like the siege around Gaza bank, so we prevent them from getting money.[637]

As well as economic and military measures, participants noted the importance of having robust cyber capabilities for deterrence. Participant I3 considered this was obvious:

> Of course cyber, you should use cyber, as part of your ability to deter your enemy… we have cyber capabilities, so these guys should not be surprised that they are hit.[638]

However, he also reiterated that having such capabilities should not constrain their government to only responding to cyber-attacks in kind.

[634] Cohen, Freilich, and Siboni, 'Israel and Cyberspace: Unique Threat and Response', p. 311.
[635] Participant I5, Quote 38C, p.5
[636] Participant I1, Quote 26, p.5
[637] Participant I1, Quote 12, p.3
[638] Participant I3, Quote 9, p.2

> Of course you need cyber activity for deterrence. But why do you think you should deter the Iranians of hitting you with cyber only by the use of cyber? It doesn't make any difference.[639]

Thus participants seemed to view capabilities as interchangeable tools which offered a great deal of flexibility in their responses. However, participants differed in their reasoning for maintaining a diverse suite of capabilities for deterrence. Participant I2 considered this was a question of effectiveness: 'Why actors should limit themselves to retaliate in the cyber domain when they can more effectively retaliate in other domains?'[640] Participant I7, a senior cyber researcher, agreed, noting it was simply often a more cost effective use of capabilities than attempting to use cyber means: 'If you are doing all sorts of war gaming it's much more cost effective to cause pain with more conventional means.'[641] But Participant I3 conceptualised the use of kinetic means as a necessary response to the perceived threat:

> In the Middle East, this is a mixture of cyber and kinetics. The language in the Middle East is kinetic. Why should cyber-attacks be responded to only in cyber? Why don't you blow the whole place up and that's it?[642]

And Participant I4, a cyber warfare researcher, similarly characterised kinetic force in response to cyber-attacks as a deliberate method to prevent escalation:

> We also use usually military force and we bomb certain targets, trying to do the minimum because we don't want to deteriorate, to be in a war before we can understand.[643]

The use of kinetic force in response to cyber-attacks was unique to Israel at the time of writing, and the public narrative around the 2019 demonstration of Israeli capabilities against Hamas, the first public kinetic response to a cyber-attack in close to real time, was that it had potentially established new precedents for attribution and response.[644] Even so, participants expressed scepticism about the reasoning behind this public narrative, and the cyber threat posed by Hamas in this sphere. Participant I1 argued the threat from Hamas was low-level: 'The only thing they (Hamas) succeeded in doing was in defacing certain unprotected sites, no damage at all.'[645] Participant I2 agreed the threat was low-level: 'My guess is that Hamas cyber capability is not very sophisticated and that this was not necessarily the reason they specifically wanted to deter Hamas cyber capabilities.'[646] Participant 3I was frustrated with the attention this event generated, viewing it as no different from pre-emptive strikes in other spheres:

[639] Participant I3, Quote 12, p.3
[640] Participant I2, Quote 30, p.6
[641] Participant I7, Quote 7, p.2
[642] Participant I3, Quote 33, p.6
[643] Participant
[644] Gross, 'IDF Says It Thwarted a Hamas Cyber Attack during Weekend Battle'; Groll, 'The Future Is Here, and It Features Hackers Getting Bombed'.
[645] Participant I1, Quote 14, p.3
[646] Participant I2, Quote 28, p.6

> In the case of the clash in Gaza we destroyed the cyber unit of Hamas. So I got so many calls, and interviews, what happened? Nothing happened. So you know if you destroy a radio station what's the difference? If you destroy an electronic disruption unit it's ok, but if you do it in cyber… cyber is a hype.[647]

These views demonstrate that although the official narrative reflected Israel's policy of deterring cyber-attacks, the execution of such policy may in fact have been influenced by other concerns. This apparent disconnect between official narrative and the views of practitioners may indicate an area of potential risk for policymakers. If Israel considers such activities as merely the logical extension of its policies in other spaces, but its adversaries accept the narrative of new precedents, this could indicate potential for unintentional escalation. And it is worth considering the alternative argument from Participant I6 here, a former cyber intelligence and warfare professional, who argued:

> You can't have deterrence without a show of force from time to time. And if you show your force in the cyber realm the other side know what you can do and he can act against you. But also if you show you're strong, if you show your power, the other side can catch your tool, reverse engineer it and send your tool against you, or someone else. So in the cyber realm today I can't say that any nation, even super power such as the United States, have strategic deterrence in cyber.[648]

This argument from Participant I6 was based on his definitions of capabilities for deterring in cyberspace solely as technical cyber capabilities. Hence his point that the viable cyber defence is an electromagnetic pulse (EMP). However, he did later concede the need to continue building capabilities and fighting, because he saw no other alternative. 'We need to be ahead, by far, we need to be ahead, technology and everything against our enemies.'[649] Overall, participants' broad acceptance of the necessity of superior capabilities supports the policies emphasis on developing and using such capabilities. Such acceptance and support may also be attributed to the Israeli acceptance of cyber as an integrated domain of warfare. Participant I3 expressed the view that it was not possible to separate deterrence in one domain from all others:

> Cyber is another domain of force deployment. Can you deter with air force? There is no meaning. You deter with everything you have. It's integrated. Can you deter with infantry soldiers? Cyber is part of everything, and you generate your deterrence.[650]

Participant I5 agreed, and pointed out that the modality of an attack was, in his view, largely irrelevant: 'It doesn't change just how I attack or how I use the different vehicles to attack or to do national security or communication.' [651] Participant I2, a senior cyber researcher, sounded the only note of caution in Israel's construction of cyber as a domain of warfare:

[647] Participant I3, Quote 13, p.3
[648] Participant I6, Quote 7, p.2
[649] Participant I6 Quote 24, p.5
[650] Participant I3, Quote 9, p.2
[651] Participant I5, Quote 29C, Interview 5, p.7

> It [the cyber domain] is to some extent socially constructed, because if military decides it is a domain, then it is a domain. They establish a cyber command, so it becomes a cyber domain. It can be a mistake, it can be inaccurate, but it becomes a domain by the military saying it's a domain.[652]

Participants viewed Israel's overall approach to building capabilities in cyberspace as consistent with how it treats capabilities in broader strategy: having more capabilities of advanced technology is a necessity due to the threats it faces. While they agreed that success was a nuanced concept, participants noted Israel's range of capabilities provided sufficient grounds to be optimistic about their deterrent value. Participant I7 judged, that 'Until now it was pretty good, because we haven't seen any damage. In looking forward I think it will be better than others.'[653] But there was also a repeated understanding that despite using that range of capabilities, Israel would never be able to prevent every attack. Participant I3 argued:

> Whatever you do, you are never able to defend everything, so build to your capability to defend. To make sure the event does not happen. Build your capability to manage when it happens. And now build your capability to recover.[654]

Participants also agreed that gaining and maintaining superior capabilities was essential for deterrence in the cyber domain, as was regularly using those capabilities; they saw a large role for pre-emptive strikes to prevent others from gaining capabilities and did not consider that like-for-like retaliation was necessarily a useful approach. However, the development and use of such capabilities necessarily requires the IDF to play a significant role, and participants noted some concerns regarding its role in delivering deterrence. Participant I7 noted a concern related to the military's weight in defining what success looked like:

> You have the whole issue of the military here having a disproportionate weight in the shaping of policy and so on. So they [the military] often define the success, for different reasons.[655]

These views show that despite the carefully constructed public policy approach delineating the military's role in deterrence, there is not complete acceptance that the military is always useful in achieving deterrence outcomes. Further, Participant I2 also identified potential risks arising from the persistent use of military capabilities to achieve deterrence: 'Once you retaliate, use force, you signal to the opponent that deterrence didn't work, so it is not always helpful in establishing deterrence posture.'[656] He continued:

[652] Participant I2, Quote 35, p.7

[653] Participant I7, Quote 56, p.10

[654] Participant I3, Quote 45, p.9

[655] Participant I7, Quote 3, p.1

[656] Participant I2, Quote 4, p.1

> The identity of deterrence helps justify specific measures. Some of them are related to deterrence like the use of force in order to enhance a deterrent posture but some of them are poorly connected to deterrence.[657]

But Participant I5 saw the military as a much more essential part of delivering deterrence outcomes: 'Deterrence is not just from deterrence by denial, but also from deterrence by punishment, which is very clear this is the role of our security forces.'[658] Thus while building and maintaining superior capabilities in order to deliver deterrence in cyberspace is a recognised policy goal supported by significant military effort, this research shows the reliance on offensive measures and military capabilities is recognised as a potential risk for perceptions of Israeli deterrence success. While recognising the importance of having superior capabilities, participants were divided almost equally between accepting the regular use of capabilities as a necessity for deterring cyber-attacks and viewing such use of force as potentially risking escalation. This division plays directly into Israel's conception of its deterrence credibility, covered in the next section of this case study.

3.13 Perceptions of credibility: The regular use of overwhelming force

Perhaps even more than capability, participants considered credibility to be critical for Israel's deterrence, and thus its survival. This required the regular use of overwhelming force and ensuring public statements, such as attributing responsibility for attacks, and swiftly followed by visible punishments. Participant I3 was blunt in his assessment: 'Credibility is gained by your actions, period.'[659] Participant I5 agreed that credibility depended on taking actions: 'So our deterrence, we are trying to build it, not on what we say, but on what we do, meaning our behaviour.'[660] Participant I7 reiterated that credibility required the appropriate response to attacks, and that this should not be limited to retaliations in kind: 'If there's tangible damage, then you need a whole range of tangible options to respond.'[661] Participant I1 viewed the policy approach of responding to cyber-attacks – by any means it deems appropriate – as essential for establishing credible deterrence: 'If the other side will be assured that by launching a cyber-attack against me, my retaliation will only be cyberspace, they may not be afraid and do it.'[662]

Thus, while Israel maintains significant offensive cyber measures and capabilities, the decision to not restrict itself to cyber responses for cyber-attacks is directly linked to a perception of how to create credibility, particularly where responses were judged to require overwhelming force. Israel views the concept of like-for-like responses as potentially damaging credibility. This commitment to credibility through any response deemed appropriate by Israel could result in unintended consequences, particularly if states conducting attacks against them are expecting a cyber response.

[657] Participant I2, Quote 6, p.2
[658] Participant I5, Quote 9, p.2
[659] Participant I3, Quote 33, p.6
[660] Participant I5, Quote 19, p.4
[661] Participant I7, Quote 25, p.4
[662] Participant I1, Quote 27, p.5.

Several participants also defined credibility in terms of domestic necessity. Participant I2 sounded a note of caution on this score: 'Deterrence has a lot of power in justifying political moves. Because it seems as if it is a middle ground between force and the use of force in Israeli culture.'[663] Indeed, in considering the 2019 IDF missile strikes as a response to Hamas cyber-attacks, Participant I2 noted that the Israeli government also had to consider the domestic optics of such actions:

> If Israel is attacking Hamas headquarters and Hamas activists, there is a limited number of targets. So if one of the targets that can be more justifiably attacked is the cyber headquarters of Hamas.[664]

Participant I7 noted this as well:

> There is a new option that you can say I did cyber this and cyber that, it serves your domestic purposes and the other guy can easily deny or something like this, because nothing happens that you can see.[665]

This may partially explain why Israel has worked hard to establish the narrative that the activities they take to build deterrence are justified. This narrative was also perceived by Participant I7 as being justified for the 2019 response, though not on cyber deterrence grounds:

> So the very level of intelligence collection and analysis that leads to selecting targets, and then they also need to justify it internally to their own oversight. But say if these people who are affiliated with part of the Hamas organisation it's a good enough reason.[666]

This picture of credibility is more nuanced than that offered by policies alone. Participants pointed to this when considering how a credible deterrent should be constructed for cyberspace. Participant I3 noted this was partly due to the complexity of the threat space and the need to carefully choose what information becomes public in order to best maintain credibility:

> You can decide what you want to gain, and from that you will derive what you want to be in the public [eye]. When you say how to build credibility, there is no single answer. There is no, ok, you have to put it to be public or not public, it's a mixture of. We know the public, we don't like things to be complex. We like simple.'[667]

And Participant I1 explained credibility in line with the classical view of deterrence credibility – as existing as a perception in the minds of an adversary, but then described this credibility as cumulative rather than static:

[663] Participant I2, Quote 7, p.2
[664] Participant I2, Quote 25, p.5
[665] Participant I7, Quote 23, p.4
[666] Participant I7, Quote 22, p.4
[667] Participant I3, Quote 40, p.8

> If every war will end with the situation in which everyone will be convinced that we won and they lost, then after one round, two rounds, three or even five, they will lose hope of getting back what they lost before by force and they will come to negotiate with us for peace. This is what is called cumulative deterrence.[668]

This continued reference to cumulative deterrence reminds us that Israel's definition of successful credibility, similar to its definition of successful deterrence more broadly, is not considered to have failed if attacks occur. Rather such attacks are viewed as a signal that deterrence has reduced in credibility and needs to be refreshed, a cycle that while accepted in Israel may not be accepted or understood by adversaries. The complexity of establishing credibility is further demonstrated through an examination of how Israel has approached the problem of attribution of attacks in cyberspace – that is, identifying the actors responsible. Adamsky argues that Israel's approach is 'perpetrator-indifferent', which allows Israel to focus on protecting assets regardless of the identity of the attacker.[669] Yet this is contradicted by Israeli practice, which has certainly not only attributed attacks but responded to such attacks. It is therefore perhaps more accurate to characterise the Israeli approach to attribution as nuanced and dependant on circumstances, particularly regarding the decision to attribute publicly, based on the repeated arguments by participants that the careful management of attribution was critical for maintaining credibility. Participants noted the arguments over whether states could attribute, but dismissed any suggestion that technical barriers were insurmountable. Participant I5 noted that while technical attribution was complex, it was nonetheless possible:

> First, it's a real work to attribute. That's why you need again the layers because you cannot go to each and every attack and try to attribute. But those that are very interesting to you, you may attribute. Technically it can be done.[670]

Participant I1 considered that while technical issues might cause initial confusion, such issues were readily surmountable: 'The technical nature of a cyber-attack is preventing you most of the time from knowing where it came from originally. But then you can say it.'[671] And Participant I4 highlighted there were considerations apart from the technical issues that impact whether a state chooses to attribute:

> There is a variance in the way that countries or victims attribute or not the attacks. It's not just do they know or not, it's what they decide. It's not just technical, it's as much political and geopolitical.[672]

[668] Participant I1, Quote 20, p.4
[669] Adamsky, 'The Israeli Odyssey toward Its National Cyber Security Strategy', p. 1.
[670] Participant I5, Quote 26, p.5
[671] Participant I1, Quote 37, p.7
[672] Participant I4, Quote 6, p.2

The point of attribution being a political rather than a technical problem, was further raised by Participant I1; he argued this was because it was better to not attribute publicly where there was any uncertainty over the best response, or indeed, whether a response was politically possible:

> If you didn't want to do it, you better not say before. It's a legitimate decision not to retaliate with bombing targets, but don't say that you do it or threaten you are going to do it and then don't do it, this is unhealthy anyway.[673]

The political complexity of attribution was again raised by Participant I2, who noted states might know who was responsible for an attack but choose not to publicly attribute, because to do so without a corresponding response damaged a state's credibility:

> Sometimes it is political, because sometimes you know who did it, and you don't want, for different reasons. You don't want to attribute that attack because for example you need to retaliate.[674]

Participants agreed that timely attribution linked to a swift visible response was critical in the Israeli view of credibility. Participant I7 characterised this as 'The aggressor should be disillusioned as much as possible that they will have the benefit of months or years before some punishment.'[675] Participants also agreed that Israel was capable of attributing cyber-attacks against it without any assistance from partners or international bodies. Participant I3 argued:

> We imagine we need to attribute and get with a proof to the United Nations, to whatever tribunal, before we retaliate. So why? Why do we need to do that? You want to retaliate, retaliate. You don't need to go to any tribunal.[676]

The question of needing to go to a tribunal, and thus needing evidence, is neatly side-stepped by Israel's preference for 'strategic ambiguity' when they wish to respond to an attack without necessarily sharing sources or waiting for a coalition approach to attribution. Indeed, participants further considered that in some cases strategic ambiguity was just as effective in creating credibility as certainty. Participant I5 explained this as the need to maintain a level of ambiguity around acceptable behaviours in cyberspace:

> Generally in our tough neighbourhood we try not to put the red bar, because we live in a neighbourhood where everybody try to just say "oh I am just exactly on the red bar,"[677] it's very complicated and dangerous in the Middle East.[678]

[673] Participant I1, Quote 29, p.6
[674] Participant I2, Quote 41, p.8
[675] Participant I7, Quote 54, p.10
[676] Participant I3, Quote 30, p.6
[677] The mention of a red bar here refers to the concept of red lines, the crossing of which prompts a particular reaction from a state.
[678] Participant I5, Quote 18, p.5

And Participant I1 observed that this ambiguity was useful for Israel as the offensive actor, citing the example of the ambiguity surrounding the Stuxnet event when it first occurred: 'But once they are convinced it is us or the US, then we don't have to take the blame on us. For deterrence, it's enough.'[679] This approach is not unique to cyberspace; as noted previously in this chapter it mirrors Israel's carefully ambiguous approach to nuclear weapons. Participant I3 characterised this as 'It's better to be silent and be asked to speak, than to speak and be asked to be silent.'[680] Continuing this theme, Participant I1 pointed to strategic ambiguity in the nuclear sphere as an example of the success of ambiguous policies. He argued,

> Israel never declared nor denied that it has a nuclear capability. And it doesn't have to do it because all our enemies are fully convinced we have it. If we have it, we have it for deterrence ok? And deterrence is already achieved.[681]

Participant I1 then described Stuxnet as an example where a deterrence message was communicated to Iran indirectly:

> States use covert action but if you speak about deterrence at least secretly, the other side should know that you did it. Take for example the attack exposed in 2010 on the Iranian centrifuges (Stuxnet) and Iranian enrichment facility. At the beginning Iran accused Israel. Then they say the USA. Then they say Israel and the USA. You don't know, but you don't have to know.[682]

But this willingness to 'go it alone' and act without either sharing attribution information, or claiming responses publicly, poses potential issues for Israel's close relationship with the US, which prefers a coalition approach towards public attribution for cyber-attacks. Participant I1 viewed the idea of attributing by coalition as problematic, because gaining consensus on such events was time consuming:

> Cyber-attacks can easily be denied. They can be denied by the attackers because it is very rare to have some proof that someone attacked you and it can be denied also by the victims. So many times attacks like this are launched, but sometimes the attacker doesn't take responsibility, sometimes no one mentions it, sometimes the victim says ok, we had this problem but we're still checking to see if it was attack, cyber-attack, or technical malfunction or whatever. So there's a huge variety of different responses by the attacker as well as the victim.[683]

And Participant I3 considered that Iran had not been deterred from cyber-attacks at all. Importantly for this research however he did not consider that this was necessarily a failure of deterrence, arguing that as such attacks did not meet the definition of warfare, they were acceptable:

[679] Participant I1, Quote 40, p.8

[680] Participant I3 Quote 33 p. 6

[681] Participant I1, Quote 38, p.7

[682] Participant I1, Quote 38, p.7

[683] Participant I1, Quote 34, p.7

> Iran is always active in Israel, so we are probably not deterring Iran… Iran is doing a lot of activity in Israel in cyber. I would assume, I don't know, that Israel is not sitting there, doing something in other places. This is under the threshold of large activity that will break the peace. So this is probably mutual deterrence under a certain level of activities.[684]

Thus these attacks, while ongoing, were not viewed as a failure of credibility. This point is important for understanding Israel's deterrence approach, because the creation of credibility was viewed by all participants as crucial for deterrence in cyberspace; and despite the noted complexities regarding attribution, only one participant considered that Israel had not created sufficient credibility for deterrence in cyberspace. Participant I6 argued:

> Deter is something you can't do for long term. You have to change the plan all the time because the conditions change but you have to do strategic plan to deter… you need all the time new way of thinking and new ideas.[685]

Thus Participant I6 argued that credibility had not been created because Israel had not sufficiently tailored its deterrence enough to each threat. This outlying view presents a contrast to all other participants who judged Israel's approach was sufficiently tailored to be credible for threats it faced between 2008 and 2018. However, there is an important caveat here with respect to the credibility of the Israeli deterrent. Unlike the views on capabilities, which were judged by participants as being largely suitable and fit for purpose, participants raised concerns as to whether Israel's approach would remain credible in future, particularly against emerging, high-capability threats. This theme continues in a consideration of how effectively Israel communicates its deterrent intent and posture.

3.14 Perceptions on communication

The participant interviews were particularly illuminating regarding Israel's views on not only the importance of communicating deterrence intent clearly, but the associated assumption that the use of force was absolutely necessary, including overwhelming force as a regular and planned part of deterrence to ensure adversaries understand Israel's likely responses to attacks on its interests. Once again, the issue of needing to communicate deterrence messages was at times complicated by the need to manage internal domestic messaging. Participant I4 highlighted that in Israel any consideration of deterrence messaging must also take into account that communication is often aimed at a domestic audience as much as any external audience: 'I think you do need to take into consideration the strategic aspects but also the domestic, the national social situation, inside the country.'[686] Participant I3 characterised this as:

[684] Participant I3, Quote 42, p.8
[685] Participant I6, Quote 80, p.17
[686] Participant I4, Quote 14, p.3

> People think that you should be courageous in front of your enemies, which is completely false. Your courageousness is measured by how you deal internally. In Israel, the courage is in front of Jews, not the Arabs.[687]

Additionally, Participant I4 noted such domestic communication for deterrence measures was important for building consensus, particularly for potential future deterrence operations:

> The Israeli society is really divided. So I think what we hear about is trying to influence citizens opinions I think, and this is my own opinion, really important or big threat which the country is not ready to deal with yet.[688]

Another indication that those attempting to assess communication efforts must use caution was the view indicated by some participants that Israel's public policies on deterrence may not be a complete, or accurate, picture of their policy. Indeed, two participants also viewed Israel's public cybersecurity strategy as less useful in guiding strategy than the public narrative surrounding these documents otherwise indicates. Despite the fact such strategy had never been publicly released before, participants were dismissive about their usefulness for deterrence, characterising them instead as tools for communication. Participant I7 argued that 'Most of the value [of strategy documents] is internal to show that they are doing things and internationally, it's also an aspect they want to promote.'[689] He further argued this carries risk as relying on public policy for communication may lead both adversaries and allies to misconstrue Israeli intent. He noted:

> we don't do public documents unfortunately for many systemic reasons and some cultural reasons… there's very little respect for formal documents from the organisation that should produce these documents, let's say.[690]

Participant I5 agreed such reliance on such documents as indication of Israeli strategy was dangerous, as strategy in Israel is a practice not constrained by written policies.

> Most of it is not written, most of it is not public, in Israel we do not write. You find much less than there really inside. What you read… is not really what's happening.[691]

Participant I6 further cautioned against relying on government resolutions as absolute declarations of policy, noting not all such decisions are implemented: 'Between 70–80% of the decisions will die in the natural way.'[692] But Participant, I5 a senior former government cyber official who had direct input into these policies seemingly contradicted this when he argued:

[687] Participant I3, Quote 36, p.7
[688] Participant I4, Quote 36, p.7
[689] Participant I7, Quote 43, p.8
[690] Participant I7, Quote 40, p.7
[691] Participant I5, Quote 29, p.6
[692] Participant I6, Quote 28, p.6

> The role of the government resolution[693] was very important first because we changed the way we defend our nation in the cyber domain than in other domains. So we needed it to be formal. We needed it to be on the table, and the establishment of a new organisation cannot happen without a governmental resolution without the political authority of the Prime Minister.[694]

These views indicate high-level awareness of the importance of such strategies for communicating deterrence aims and goals – if not for shaping practice, then for guiding public expectations of that practice. And that practice is largely judged a success, despite ongoing cyber-attacks. Israel's judgment of its efforts to communicate its deterrence posture as effective reveals both the complexity of assessing success.

Consider the level of knowledge of an adversary that Israel requires regarding both historical enemies and emerging threats. Participants revealed a consistent view that in responding to historical threats, the open use of force was an absolute requirement to communicate deterrent intent. Participant I6 argued Israel's use of such force was essential. 'You can't have deterrence without a show of force from time to time.'[695] Participant I1 agreed that kinetic punishment is needed to maintain deterrence, as has worked in other domains: 'It worked with Egypt, with Syria, with Jordan.'[696] Thus this approach to attacks in cyberspace is consistent with how Israel has communicated its deterrence posture in other domains. As Participant I3 argues 'If you want to shoot, shoot. Talking will get you nowhere.'[697] But while this use of force was accepted by all participants as current Israeli practice and unlikely to change, Participant I2 sounded a note of caution as to whether such a response was always helpful in establishing or communicating deterrence intent. He argued there was a risk that such use of force could be misunderstood:

> The use of force is not always helpful to establish a deterrence posture. It depends on how the opponents, the challenger, interprets the use of force… it can also be interpreted as a deterrence failure.[698]

And participants noted that evaluating success or failure of a deterrent message was complicated by it not always being immediately obvious to whom a message was aimed. It can be difficult to differentiate between an activity, its effects, and the activity's intended audience – which may be different to the primary target. An example of this complexity is evident through the following quote from Participant I1:

> … the main goal of this special forces penetration into Gaza was not to hit the bases and terrorist forces. It was to deliver a message to Egypt – we Israel, we are very strong. We can do whatever we want. We can enter into Egypt, we come with a lot of force, we do whatever we want. Then

[693] This is a reference to Resolution 2444; Netanyahu, 'Advancing the National Preparedness for Cyber Security: Government Resolution No. 2444'.
[694] Participant I5, Quote 14, p.3
[695] Participant I6, Quote 7, p.2
[696] Participant I1, Quote 22, p.5
[697] Participant I3, Quote 33, p.6
[698] Participant I2, Quote 3, p.1

> we come back because we don't like you, something like this, in order to deter Egypt from having thoughts if attacking us.[699]

But this uncertainty around the deterrent message is problematic if it needs to be appropriately targeted. Participant I6 argued that for communication to be effective, it had to be tailored and targeted to particular threat actors:

> You need to understand what effect the other side, you need to know his culture, and his condition, and what hurt him all the time, and you need to try and watch and predict it, a long time before it happened.[700]

Participant I6 further argued such tailoring was complex and required a high level of knowledge about adversaries:

> The worst thing, what you can do against a country such as maybe Malaysia, you can't do against North Korea because they think different. Because the leadership is different way of thinking, they don't work the same. Someone that kills his own persons by anti-aircraft gun is, he make his own population die from hunger, this is different. You need to understand what made him hurt. What hurt him. It's a problem. [sic][701]

Participant I5 also pointed out that visible responses should further depend on what Israel wanted to deter:

> You want to deter a specific attack on your electrical grid, or your election campaign? Do you want to shame, do you want to explain why you are now attacking, this is the different… it is a spectrum.[702]

This view of Israel's communication efforts as requiring significant nuance was acknowledged by participants as necessary to manage the range of threats Israel faced. Further, at times Israel's public deterrence narrative is designed to meet internal political needs, rather than the designated threat. Participant I2 considered this was potentially a problem, arguing that the public narrative around deterrence and its centrality to the domestic audience can at times do nothing for, or potentially damage, its intended deterrence outcomes:

> In Israel especially, it's part of the public discourse, there's a very prominent public discourse on deterrence and politicians from both sides of the political continuum talk about deterrence and the need to deter and I think it's a very fundamental aspect in the social element, it's a fundamental part of the story.[703]

[699] Participant I1, Quote 32, p.6
[700] Participant I6, Quote 81, p.17
[701] Participant I6, Quote 81, p.17
[702] Participant I5, Quote 27, p.6
[703] Participant I2, Quote 2, p.1

And Participant I6 agreed communicating policies internally was important, pointing to the problem of cyber in Israel not being necessarily a well-understood problem:

> And when you ask people about cyber, what is cyber, everyone will give you another answer. And most people will talk about computers, networks, systems, technology – I say it's not true. First of all, its human behaviour. The human factor is the most important thing in the cyber realm because the human build [sic] this environment and the human affect by their environment.[704]

While participants viewed Israel's efforts to communicate its deterrent intent in mostly positive terms, there were several caveats noted. Participant I1 cautioned against attempting to judge the effectiveness of a communication message, noting success was not always visible: 'Relevant very much to deterrence, if it's not zero-one, is that sometimes you act against, party one acts against party two in order to deter party three.'[705] He considered that this multi-party deterrence activity might not translate into visible outcomes. Additionally, Participant I1 noted the intent of certain actions might become confused or misconstrued by the media. He returned to the example of the 2019 IDF air-strike on an alleged Hamas cyber facility, observing:

> One of the targets that was chosen was the cyber…actually it was not. It was the local headquarters of Hamas in the sector, in this area, which was in the same building as the cyber unit or something like this of the Hamas, and it went out of proportion.[706]

This narrative of the kinetic act in response to a cyber-attack being a convenience, rather than a targeted deterrence message to Hamas, is quite different to the official version of events[707] discussed earlier in this chapter. But Participant I5 speculated that such differences merely reflect the fact that the domain is relatively new and constantly evolving:

> We are not yet really understanding exactly what cyber warfare is, and how it is going to look like, and how to combine cyber and physical domain together and what is legitimate and what is not acceptable. I think we are in the process of learning.[708]

This relative newness was also considered a problem for translating the communication requirement. Participant I2 also argued the lack of clear red-lines was a potential problem for the communication of deterrent threats: 'In the other domains there are threats, public threats, of what we do in the case of attack, and (we) don't have it in the cyber domain.'[709] Further, the problem of emerging threat actors was again raised as a problem for Israel's cybersecurity approach in cyberspace. Indeed for both the credibility

[704] Participant I6, Quote 72, p.15

[705] Participant I1, Quote 31, p.6

[706] Participant I1, Quote 13, p.3

[707] Zak Doffman, 'Israel Responds To Cyber Attack With Air Strike On Cyber Attackers In World First', Forbes, accessed 25 June 2021, https://www.forbes.com/sites/zakdoffman/2019/05/06/israeli-military-strikes-and-destroys-hamas-cyber-hq-in-world-first/.

[708] Participant I5, Quote 35, p.7

[709] Participant I2, Quote 10, p.3

and communication requirements – far more than capability – participants expressed concerns that Israel's approach might not be sufficient to meet emerging threats in future, and that this was potentially a serious problem. Participant I3 remarked that:

> People have this dream or vision that somewhere down the line we will be sitting in our office and running wars with buttons…I think this is stupid. What I mean by that is in the end our kids die because of that. You think you can do something, which you cannot do, and you pay costs. And the costs are not only money.[710]

And despite the Israeli narrative regarding its advances in cyber warfare[711] Participant I5 argued

> we are not really understanding exactly what cyber warfare is, and how it is going to look like, and how to combine cyber and physical domains together and what is legitimate and what is not acceptable.[712]

This view seems to contradict the official projection of Israeli cybersecurity policy as a settled and coherent policy approach which other states are invited to learn from.[713] Overall, while participants agreed communication was a key requirement for deterrence, the concerns expressed about Israel's communication measures – particularly the use of force as a method of communicating intent and the effectiveness against emerging threats – seem to indicate that the Israeli communication approach is perhaps not as cohesive as advertised. Given the caveats and areas of uncertainty identified by participants for each deterrence requirement, it is worth now considering whether participants considered Israel's approach as being successful overall – and whether it is likely to be considered successful in future.

3.15 Is it deterrence, and is it successful?

The question of how successful participants judged Israel's approach to be overall produced mixed results. Overall, participants agreed there was evidence of a significant Israeli government effort towards creating and maintaining all three elements required for deterrence theory and agreed these requirements were the bare minimum for establishing deterrence. However participants also noted complexity in attempting to assess Israel's deterrence for cyberspace, arguing that it was necessary to consider Israel's approach as part of a broad deterrence strategy, rather than one confined to cyberspace. Participant I3 argued that any discussion of deterrence in the Israeli context must begin from the understanding that deterrence cannot be considered in isolation but is rather part of a whole of nation defence strategy:

> When I look at deterrence, I look at the holistic issue ok?' The attempt to isolate the cyber issue from the rest of the force deployment issue is first of all doomed to fail. Now the question comes,

[710] Participant I3, Quote 21, p.4
[711] Lim, 'Israel and Iran Just Showed Us the Future of Cyberwar With Their Unusual Attacks'.
[712] Participant I5 Quote 34, p.7
[713] 'Israel National Cyber Security: In Brief', September 2017, State of Israel, p.18

> can you deter the enemy, the rival, to deploy cyber against you? I think this question has no meaning. Because deterrence, you cannot try to break it down into little bits and pieces. Ok, I've managed to deter my enemy, say Iran. I managed to deter Iran to do a little bit on cyber but I did not manage to deter Iran (from) hitting the tankers in the Gulf.[714]

There is a narrative throughout the Israeli case that any attempt to separate cyber as a domain creates a false dichotomy that is unhelpful for discussions of deterrence efficacy. Israel thinks it can evaluate its deterrence in cyberspace as part of holistic approach to deterrence; however, both adversaries and allies think they can separate what happens in cyberspace. There is a risk here that a state such as Iran behaves in cyberspace in a way it considers acceptable and confined to the cyber realm, which Israel then perceives as a major threat and responds kinetically. The resulting potential for unintentional escalation and retaliation is therefore serious. Further, the question of whether Israel's deterrence could be evaluated was questioned by participants, who acknowledged the complexity of studying deterrence efficacy but attributed this difficulty to contrasting reasons. Participant I4 argued this was partly due to the emergent nature of studying deterrence in cyberspace, stating: 'I don't think it [deterrence] doesn't work. I don't think it's a concept we should not use. But I just think we don't know exactly how it applies today.'[715] In contrast, Participant I2 argued the difficulty was due to the complexity of studying deterrence more broadly in the field (as acknowledged in Chapter 1).

> In general, it is difficult to study deterrence. And this is not only a problem for cyber deterrence. There is a poor, very poor, in international security, a very poor causal connection between the issuing of a deterrence threat and deterrence success.[716]

However Participant I2 did not consider this complexity was necessarily an indication of deterrence not working.

> I think deterrence can work, but it can be difficult to predict… it's difficult to predict the conditions under which it can work and it's very difficult to study, to establish the causality of deterrence success. But this is human activity and can be deterred because it is human.[717]

Additionally, there were disagreements over whether some actions even should be defined as deterrence. Participant I2 used the example of Stuxnet:

> Stuxnet itself was not… I mean, it can be interpreted by itself as a kind of deterrence but Stuxnet itself was not… it was a way to deal with the Iranian nuclear program but it was not a deterrence practice, it was a preventative, or pre-emptive attack, not deterrence.[718]

[714] Participant I3 Quote 10, p.2
[715] Participant I4 Quote 11, p.3
[716] Participant I2, Quote 46, p.9
[717] Participant I2, Quote 38, p.7
[718] Participant I2 Quote 16, p.3

Participant I6, taking an operational view, considered that deterrence in cyberspace was not possible due to the lack of an overwhelming capability:

> You can also say that there is no way to deter maybe some enemies, maybe you can deter other enemies, in some ways it will be for short term or long term but you can say. I truly believe that in the cyber world you can't find a real solution except EMP.[719] EMP will shut down all the electricity that don't defend against it. If you are defendable against it you have to find [the] other thing. When I understand that every general military equipment needs to be secure against EMP, it can't be. And so you can't deter.[720]

But Participant I7 was more sanguine, pointing out deterrence success was more accurately characterised as a range.

> First of all it's difficult to say when you succeed… no-one expects a one hundred percent success in deterring terrorism, but how much is a question of strategy. That's the range of success. The success isn't in preventing a major operation.[721]

The extension of the Israeli definition of deterrence to cyberspace as cumulative is a conception that has significantly impacted assessments of deterrence success: successful deterrence for cyberspace is defined as being prevention of the worst attacks while maintaining the ongoing survival of the Israeli state. By this measure, Israel's deterrence in cyberspace can be considered a success as long as Israel's interests in cyberspace remain operational and protected despite regular attacks. Yet by almost any other definition of deterrence as attempting to influence adversaries away from conducting cyber-attacks against Israel, the approach would seem to have failed. And there is internal disagreement over definitions of deterrence, and whether certain measures are actually deterrence or defence measures. According to Participant I2:

> So definitely it's very hard to deter these kinds of actors and I agree that some of the ways to address these challenges is by improving defence, not deterrence. I agree there's a lot of challenges in deterring, in cyber deterrence practice.[722]

There were also significant differences in responses regarding the seriousness and extent of the cyber threat. For example, Participant I3 argued 'There is nothing special in cyber.'[723] However, this stands in contrast to Israeli policy, which has specific policies designating cyber threats as serious enough to require their own significant policy effort. And Participant I7 saw such arguments as largely moot:

> If you start asking people who are not in the academic research on deter, they will say the same thing. It doesn't matter. Cyber or not cyber, it's the same. You had this attention to the topic almost twenty years ago with the terrorists, and people say you cannot deter because it is

[719] EMP: Electromagnetic pulse
[720] Participant I6, Quote 69, p.13
[721] Participant I7 Quote 4, p.1
[722] Participant I2 Quote 20, p.4
[723] Participant I3, Quote 47, p.9

> terrorists, and it turns out you can partly deter and mostly disrupt the process of them executing their strategy.[724]

3.16 Preliminary findings

Despite the acknowledged difficulties of studying deterrence and its applicability to cyberspace, all participants in this research agreed such research was important, not just for Israel, but for the development of strategic theory more broadly. This chapter presents the preliminary finding that the Israeli approach to deterrence in cybersecurity is fundamentally the same as its broad deterrence approach, contains the requirements of classic deterrence, and is claimed by the government as a success. At the same time, the resulting reliance on refreshing deterrence through the regular use of pre-emptive overwhelming force may be misunderstood by its interlocutors and could result in unintended escalation.

Nonetheless, Israel does not consider its deterrence polices for cyberspace as perfect. Participants in this case study noted several areas where it could improve, particularly regarding its communication of deterrence intent both domestically and to adversaries. And Israel's over-reliance on deterrence strategy has resulted in strategic miscalculation in the past, such as during the conflict with Hezbollah in 2006;[725] and as Amir Lupovici has pointed out, the practices of deterrence can eventually lead to the violence such policies aim to prevent.[726] Thus there is a risk that could also occur in cyberspace. Further, Israel's claimed success in deterring cyber-attacks could be attributed to many other factors, such as that Israel is seeking to deter an enemy that is operating from a relatively low technological base. It is difficult, then, to determine how much Israel's success is due to strong deterrence, and how much is due to the relatively low ability of its main threat actors. But there is a compelling counter-argument that the low technological ability could also be described as a success, in that Israel has not allowed its adversaries to develop a better capability.

Israel's commitment to military defence and protection of Israeli interests is certainly significant. Its commitment to deterrence has remained robust despite the challenges of applying deterrence theory in cyberspace. And while there are arguments over Israel's ability to adapt strategic policy to meet changing strategic circumstances, particularly in the cyber era, the case study agrees with Henriksen's assessment that Israel is aware of the breadth of threats it faces in cyberspace.[727] While Israel's strong focus on the historic 'Arab' threat[728] has been argued as leaving Israel potentially exposed to higher order threats – with the attempt to deter becoming a trap tying the deferrer and the putative challenger together[729] – the

[724] Participant I7, Quote 1, p.1
[725] Henriksen, 'Deterrence by Default? Israel's Military Strategy in the 2006 War against Hizballah', p.95.
[726] Lupovici, 'Toward a Securitization Theory of Deterrence', p.182.
[727] Henriksen, 'Deterrence by Default? Israel's Military Strategy in the 2006 War against Hizballah', p.115.
[728] While it is beyond the scope of this research to address the systemic issues in the region, it is worth noting this conception of the threat to Israel is contended by many states and seen as deeply offensive by the Palestinian people. An overview of the complexities of the security challenge is presented in Michael Broning, 2011, *The Politics of Change in Palestine: State-Building and Non-Violent Resistance*, London: Pluto Press. For a Palestine-centred view, see Ali Abunimah, 2014. *The Battle for Justice in Palestine,* Chicago, United States: Haymarket Books
[729] Lupovici, 'Toward a Securitization Theory of Deterrence', p.183.

case study revealed that both participants and strategists were well aware of higher order cyber threats posed by emerging actors.

3.17 Conclusion

This chapter has explored how and why Israel chose to apply and maintain a commitment to deterrence as part of its cybersecurity policies throughout 2008–18. It considered how successful strategists and cyber experts judged that approach and argued that the definition of deterrence as cumulative gave Israel the ability to claim success, regardless of the number or scale of cyber-attacks occurring. The chapter considered the concerns raised by experts that Israel's reliance on the use of force, particularly pre-emptive force, to bolster Israeli credibility and communicate 'deterrence' messages was instead potentially contributing to unintended escalation. Despite meeting its own definition of deterrence as a cumulative process, its methods of operationalisation of deterrence for cyberspace, including the use of overwhelming force and treatment of the cyber domain as part of integrated domain of warfare, had led Israeli cyber experts to place substantial caveats on Israel's 'success'. These caveats include concern over the value of evaluating success at the conceptual level and concerns that Israel's use of force in response to cyber-attacks might be triggering arms races with adversaries. The case study indicates that while Israel's policy and government narrative is of successful deterrence in cyberspace, the perception of its own experts is more nuanced. While Israel's approach in cyberspace has to date helped it create a robust cybersecurity framework built on the definitions of deterrence that have served Israel well throughout its history, several experts argued the challenges posed by cyberspace may well mean that Israel needs to reconsider this strategy in order to successfully deter emerging threats.

This case study also demonstrates that even in a state with an approach as seemingly cohesive as Israel's there is dissent over whether its approach can be considered success, whether it has done enough, and whether it will be sufficient to deter emerging future threats. This case study revealed significant concern that although Israel has been successful in mitigating the negative impacts of cyber to date, the potential for damage in future is great.[730] The next chapter will consider as a separate case study the very different approach taken to deterring cyber-attacks by the US, before findings from both case studies are analysed against each other and the classic deterrence requirements in Chapter 5.

[730] Cohen, Freilich, and Siboni, 'Israel and Cyberspace: Unique Threat and Response', p.316.

Chapter 4 US deterrence in cyberspace: The risks of 'failure'

4.1 Introduction

The US presents a mass of contradictions in its approach to deterrence for cyberspace. It is the nation responsible for the creation of the internet; a leader in the theoretical development of deterrence; and the subject of serious cyber-attacks throughout the period studied. No other nation would seem to have as high a stake in creating effective cybersecurity. Yet despite deterrence of cyber-attacks being a publicly acknowledged goal since 2010[731] and reiterating this goal repeatedly in major strategic documents (including DoD strategies[732] and the 2018 National Cyber Strategy,)[733] the US has not managed at any point to create or maintain a deterrence approach it considered successful. Further, since 2018 the US has instead adopted the approach of 'persistent engagement' which aims to have 'deterrent effects' through ongoing engagement and pre-emptive activity with adversaries in cyberspace;[734] a step that represents a significant shift away from classic deterrence theory. This chapter explores why the US partially adopted and then pivoted away from deterrence theory and presents an initial assessment on both the potential risks of this inconsistent approach and those associated with attempting to achieve 'deterrent effects' through persistent engagement. In particular it explores how and why US policy did not manage to create a balanced approach to creating the minimum agreed deterrence requirements of capabilities, credibility, and communicating deterrent intent for cyberspace. The chapter presents the finding that US reliance on developing superior capabilities – while understandable given the influence of capability superiority during the Cold War – was not sufficient to create a deterrence strategy. This lack of strategy meant the 2018 pivot is based on a perception of deterrence failure that is incorrect: the US ability to deter cyber-attacks may be due to the incomplete implementation of deterrence theory, rather than a failure of the theory itself.

The chapter begins by identifying the underlying context for the US approach to deterrence in cyberspace in 2008 and considering how this context created the conditions for unreasonable expectations of deterrence for cyberspace. Through examining primary and secondary sources, I argue the Cold War experience produced a reliance on capability superiority that created an incomplete construction of deterrence in US cybersecurity policy, including a definition of zero-sum success that did not allow for ongoing cyber-attacks. The chapter then investigates how effective these policies were perceived to be in creating deterrence via a series of expert interviews, including consideration of why deterrence as a theory

[731] United States of America, May 2010, 'National Security Strategy' (President of the United States of America), p.27

[732] Ash Carter, April 2015, 'The DoD Cyber Strategy', US Department of Defense; 'Department of Defense Strategy for Operating in Cyberspace', n.d., p.19.

[733] 'National Cyber Strategy of the United States of America', September 2018, The White House, US

[734] Ibid.

was perceived to have failed in cyberspace.[735] This chapter presents the initial finding that the struggle to operationalise the requirements of classic deterrence and resulting incomplete policy approach created the conditions for deterrence to be perceived as a failed strategy.[736] Finally, the chapter makes the case that the US policy shift away from classic deterrence to reliance on offensive superiority, entanglement and persistent engagement could be contributing to a cyber arms race and therefore increasing the potential for unintentional escalation from conflict in cyberspace into kinetic warfare.[737]

4.2 Defining US deterrence: The Cold War legacy of 'success'

Much of the literature on deterrence, including the basic deterrence requirements examined in this thesis, originates in the US. The US is a global leader on the theory of deterrence which, as discussed in Chapter 1, existed well before the Cold War and as a minimum requires a state to have capabilities, be able to credibly threaten their use, and communicate deterrent intent and consequences for breaching deterrence.[738] However the Cold War and the advent of nuclear weapons led deterrence theory to become considered largely in the ambit of nuclear theory.[739] The application of deterrence theory to nuclear weapons occurred relatively quickly, largely through the seminal work of Bernard Brodie and Thomas Schelling.[740] Schelling noted that with the advent of nuclear weapons, deterrence came to rest on the 'threat of pain and extinction, not just on the threat of military defeat'.[741] Military strategy was no longer the science of military victories, but also the 'art of coercion, intimidation and deterrence'.[742]

Nuclear deterrence quickly became a central concept for US security policy[743], and was widely perceived as successful in preventing nuclear conflict.[744] This had a deep and lasting impact on the US security community, including in the political, policy and academic spaces. The significance of these impacts was two-fold: first, the lasting definition of deterrence success as a zero-sum proposition where the existence of weapons of overwhelming force deterred all attacks;[745] and second, a perception emerged that with enough military force, a country may not need to bargain.[746] These impacts laid the foundations for an

[735] Aaron F. Brantly, 2020, 'Entanglement in Cyberspace: Minding the Deterrence Gap', *Democracy and Security,* 16:3, 210
[736] Richard Andres, 2017, 'Cyber Gray Space Deterrence', *PRISM,* 7:2, 91
[737] Alexander Klimburg, 2020, 'Mixed Signals: A Flawed Approach to Cyber Deterrence', *Survival,* 62:1, 114
[738] Christoph Bertram and International Institute for Strategic Studies, 1980, *Strategic Deterrence in a Changing Environment*, vol. 6, Farnborough: Gower Pub. Co; Colin S. Gray, 1993, *Weapons Don't Make War: Policy, Strategy, and Military Technology*, Lawrence, Kansas: University Press of Kansas; George H. Quester, 1986, *The Future of Nuclear Deterrence*, Lexington, Mass: Lexington Books; Keith B. Payne, 2001, *The Fallacies of Cold War Deterrence and a New Direction*, Lexington: University Press of Kentucky
[739] Bernard Brodie, 1946, *The Absolute Weapon: Atomic Power and World Order*, Harcourt
[740] Ibid, see also Thomas C Schelling, *Arms and Influence,* 1991:Yale University Press (reprint) Ch. 1, 2
[741] Schelling, p.21
[742] Schelling, p.34; for more on nuclear theory see Chapter 1: Literature
[743] Christoph Bertram and International Institute for Strategic Studies, 1980, *Strategic Deterrence in a Changing Environment*, vol. 6, Farnborough: Gower Pub. Co, pp.5–43; see also Raymond -Ojserkis, 2003, *Beginnings of the Cold War Arms Race: The Truman Administration and the U.S. Arms Build-Up*, Westport, Conn: Praeger, Introduction
[744] Jim Chen, Does Conventional Deterrence Work in the Cyber Domain, p.106
[745] Patrick Cirenza, 2015, *An Evaluation of the Analogy Between Nuclear and Cyber Deterrence*, Stanford University, p.ii
[746] Schelling, Arms and Influence, p.1

enduring US belief in the deterrent power of capabilities, and in the ability of deterrence to deter all attacks. But as noted in Chapter 1, nuclear deterrence is a highly specialised and specific subset of deterrence.[747] While useful in deterring nuclear attacks during the Cold War, nuclear deterrence should not be used as a shorthand for deterrence.[748] Yet throughout the US literature there is an overarching theme that the perceived success of nuclear deterrence deeply influenced US strategic theory, academic literature, and public policy pertaining to cyberspace.[749] This included research into how the scale, scope and reach of the nuclear arms race came to be.[750]

4.3 Constructing deterrence for cyberspace: The problem of 'cyber deterrence'

From the earliest days of its attempts to apply deterrence to cyberspace, the US has struggled with the fundamental issue of how to define and operationalise it. A good example here is William J. Lynn's 2010 argument that deterrence will 'necessarily be based more on denying any benefit to attackers that on imposing costs through retaliation' due to what he argued were the fundamental differences in the cyber domain.[751] By 2016 Martin Libicki was arguing for a more pragmatic definition of deterrence, explaining it as a state of mind one hopes to induce in foes that persuades them not to attack. Deterrence policies were then a set of rules in the sense that if a state declared a particular behaviour is unacceptable, and such a behaviour is observed, it would be countered with punishment.[752] Libicki argued the purpose of a deterrence posture was to reduce both the likelihood of future attacks and the money that would otherwise have to be spent on defence in the absence of deterrence[753]. However, Libicki's principles-based approach for cyberspace was not widely accepted. The influence of the nuclear era meant that deterrence had come to be understood by the means in which it is carried out, hence the term 'nuclear deterrence' being separated conceptually from 'conventional deterrence'.[754] In an attempt to explain this Robert Jervis argued the US approach suffered from framing of deterrence around the mechanism by which a threat is delivered, as this approach could not work for deterrence in cyberspace. [755]

As noted in Chapter 1, there is a distinction made in the US literature between 'deterrence in cyberspace' (the extension of deterrence theory in an attempt to deter cyber-attacks) and 'cyber deterrence' (the use of

[747] Timothy M. Goines, Winter 2017, Overcoming the Cyber Weapons Paradox, Strategic Studies Quarterly, p.89

[748] Colin S. Gray, 1993, *Weapons Don't Make War: Policy, Strategy, and Military Technology*, Lawrence, Kansas: University Press of Kansas, p.9

[749] Will Goodman, 2010, Cyber Deterrence: Tougher in Theory than in Practice? Strategic Studies Quarterly, Fall 2010, p.103

[750] Raymond P. Ojserkis, 2003, *Beginnings of the Cold War Arms Race: The Truman Administration and the U.S. Arms Build-Up*, Westport, Conn: Praeger, p.153

[751] William J Lynn Defending the new Domain p.100

[752] Martin C. Libicki, 2016, *Cyberspace in Peace and War*, Annapolis, pp.222-224

[753] Ibid

[754] Alexander L. George and Richard Smoke, 1974, *Deterrence in American Foreign Policy: Theory and Practice,* New York: Columbia University Press, p.60

[755] Robert Jervis, 2016, 'Some Thoughts on Deterrence in the Cyber Era', *Journal of Information Warfare*, 15:2, p,66

cyber weapons and capabilities in an attempt to deter all types of unwanted behaviours).[756] Given the relative newness of applying deterrence theory to cyberspace[757] and the different views outlined in the literature, it follows that key US policy documents reveal similar inconsistencies. The first definition of deterrence for cyberspace is in the 2005 National Military Strategy for Cyberspace explains:

> DoD will execute the full range of military operations in and through cyberspace to defeat, dissuade and deter threats against US interests.

The emphasis on using all available military means in cyberspace to deter unspecified threats creates a definition of military cyber means to deter threats, which could come from any domain. In 2011 the US DoD released its first public cyber strategy, which mentioned deterrence, but only in the context of needing to work with international partners and prevent insider activity:

> To deter and mitigate insider threats, DoD will strengthen its workforce communications, workforce accountability, internal monitoring, and information management capabilities… The development of international shared situational awareness and warning capabilities will enable collective self-defense and collective deterrence.[758]

But the actual term 'cyber deterrence' does not appear in US policy until 2015 in the 2015 DoD Cyber Strategy which stipulates:

> The Department of Defense must contribute to the development and implementation of a comprehensive cyber deterrence strategy to deter key state and non-state cyber actors from conducting cyber-attacks against US interests.[759]

This definition frames the US military view of cyber deterrence as having the purpose of deterring cyber-attacks, rather than using cyber means to deter broader threats:

> As DoD builds its Cyber Mission Force and overall capabilities, DoD assumes that the deterrence of cyber-attacks on U.S. interests will not be achieved through the articulation of cyber policies alone, but through the totality of U.S. actions, including declaratory policy, substantial indications and warning capabilities, defensive posture, effective response procedures, and the overall resiliency of U.S. networks and systems.[760]

This policy indicates the US intended to treat cyber deterrence as part of a holistic, whole-of-government deterrence effort – and yet this never materialised. Rather, by 2018, the US released both a DoD strategy

[756] Jun Osawa, 2017, 'The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?', *Asia-Pacific Review*, 24:2, 124; see also Stevens 148; Ewan Lawson, 2017, 'Deterrence in Cyberspace: A Silver Bullet or a Sacred Cow?', *Philosophy & Technology*, 31:3, 432

[757] Tim Stevens, 2012, 'A Cyberwar of Ideas? Deterrence and Norms in Cyberspace', *Contemporary Security Policy*, 33:1, p.151

[758] 'Department of Defense: Strategy for Operating in Cyberspace', July 2011, US Department of Defense

[759] Ash Carter, April 2015, 'The DoD Cyber Strategy', US Department of Defense

[760] Ibid

and a National Cyber Strategy, neither of which defined cyber deterrence. The DoD instead referred to the need to 'compete and deter in cyberspace', defined as:

> The US seeks to use all instruments of national power to deter adversaries from conducting malicious cyberspace activity that would threaten US national interests, our allied, or our partners.[761]

This was reiterated in the 2018 National Cyber Strategy, with the additional caveat that the US would include the following instruments of national power:

> diplomatic, information, military (both kinetic and cyber), financial, intelligence, public attribution, and law enforcement capabilities.[762]

Thus by 2018, as Evan Lawson has argued, the US had seemingly defined cyber deterrence as the efforts it takes to deter malicious actors in cyberspace by whatever method is appropriate.[763] But these public definitions have not created agreed and widespread understanding of exactly what was meant by the term. Here, Jervis has a strong case that framing deterrence as 'cyber deterrence' is not helpful, as cyber is merely an instrument that can be used to support national policies, including deterrence and coercion.[764] Jervis bases this argument on the logic that changes in technology do not change the first principles of conflict and deterrence,[765] an argument which is supported by Colin Gray.[766] If the meaning of a country's weapons is determined more by its policy than the technical characteristics of its weapons,[767] then defining deterrence through the lens of cyber capabilities is problematic.

As well as the problem that deterrence in cyberspace is not well understood, US security policy has also wrestled with defining deterrence aims and expectations in cyberspace. These have swung between descriptions of denial and punishment. For example, in its earliest cybersecurity policies the US noted the need to secure cyberspace and punish those who attacked US interests. The first hint of this occurred in the 2003 National Strategy to Secure Cyberspace, which was the first formal US mention of deterrence as part of its cyberspace strategy.[768] The Strategy stated that when the nation was attacked through cyberspace, 'the US response need not be limited to criminal prosecution. The US reserves the right to respond in an appropriate manner.'[769] This theme was also evident in the 2006 National Infrastructure Protection Plan, which noted that the US deterrence posture in cyberspace was an attempt to 'cause the

[761] 'Department of Defense: Cyber Strategy 2018', September 2018, US Department of Defense

[762] 'National Cyber Strategy of the United States of America', September 2018, The White House, US, p.21

[763] Ewan Lawson, 2017, 'Deterrence in Cyberspace: A Silver Bullet or a Sacred Cow?', *Philosophy & Technology*, 31:3, 432

[764] Robert Jervis, 2016, Some Thoughts on Deterrence in the Cyber Era, *Journal of Information Warfare*, 15:2, p.66

[765] Ibid

[766] Gray, *Weapons Don't Make War: Policy, Strategy, and Military Technology*., p.9

[767] Ibid

[768] President George W. Bush, February 2003, 'The National Strategy to Secure Cyberspace', The White House, US

[769] Jason Healey, 2019, 'The Implications of Persistent (and Permanent) Engagement in Cyberspace', *Journal of Cybersecurity*, 5:1, 4

potential attacker to perceive that the risk of failure is greater than that which they find acceptable'.[770] In the first case, the emphasis was on punishing attacks; in the second, the aim appears to convince an adversary not to attack at all. And, somewhat confusingly, the 2006 National Military Strategy for Cyberspace Operations identified the need to 'defeat, dissuade and deter', which implies roles for deterrence by denial and punishment.[771] Meanwhile, the 2010 National Security Strategy argued that the task of deterrence fell within the context of military force and defence commitments:[772]

> Military force, at times, may be necessary to defend our country and allies or to preserve broader peace and security, including by protecting civilians facing a grave humanitarian crisis. We will draw on diplomacy, development, and international norms and institutions to help resolve disagreements, prevent conflict, and maintain peace, mitigating where possible the need for the use of force. This means credibly underwriting US defense commitments with tailored approaches to deterrence and ensuring the US military continues to have the necessary capabilities across all domains – land, air, sea, space, and cyber.[773]

The focus on securing cyberspace through deterrence meant the military had a significant early role in developing the US approach. While the 2010 National Security Strategy noted the need for credibility and communication, it placed the emphasis on creating deterrence through developing, maintaining and using a suite of superior capabilities. This theme continued in the 2015 National Security Strategy, which also noted the need to prepare for failure. Under the heading 'Strengthen Our National Defense', the document noted 'Our military will remain ready to deter and defeat threats to the homeland, including against missile, cyber, and terrorist attacks, while mitigating the effects of potential attacks.'[774]

But despite demonstrating evidence for a significant commitment to building, maintaining and using capabilities to deter cyber-attacks, none of these US policies contained a similar level of commitment to the importance of creating credibility or communication of US deterrent intent. This helps explain why debate remains about whether these are sufficient to comprise a cyber deterrence strategy. On this point Jun Osawa has argued that the US has established a cyber deterrence strategy by process of trial and error, pointing to these policies and the associated official commentary about them as evidence of this.[775] But Alex Wilner also makes a strong case that a set of ad hoc policies do not add up to a coherent deterrence

[770] 'National Infrastructure Protection Plan: 2006', 2006, US Department of Homeland Security

[771] 'The National Military Strategy For Cyberspace Operations', December 2006, United States, Department of Defense

[772] President Barack Obama, May 2010, 'National Security Strategy', President of the United States of America, p.22

[773] Ibid.

[774] Ibid p.7

[775] Jun Osawa, 2017, 'The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?', *Asia-Pacific Review*, 24:2, 114

strategy. With cyber deterrence theory still in its messy infancy officials had not yet managed to convert what theory exists into policies,[776] and hence he argues it is more instructive to examine US practice.[777]

US authors differ further on the reasons why credibility and communication were lacking in the US approach. Richard Andres has argued that the US cyber deterrent lacks credibility because of its puzzling unwillingness to respond to cyber-attacks – inferring that if the US responded, credibility could be increased and deterrence may be more effective.[778] Tim Stevens similarly has observed that while the US has developed a body of cyber deterrence theory, this has largely failed to translate into concrete policy and strategy due to the complexities of translating the procedures and techniques of Cold War deterrence to the cyber domain, rather than the failure of the theory itself.[779] In contrast, Osawa's view that US cyber deterrence is effective but could be more so with better capabilities[780] is indicative of a common view among military strategists that more capabilities translates to more deterrence. This is a view that is hardly unique to the modern US military – after all, the same principle was highlighted by Sun Tsu.[781] But it is nonetheless contradicted by the US 2018 Cyber Command Strategy, which argues that bureaucracy is the critical barrier to implementing deterrence responses:

> We should not wait until an adversary is in our networks or on our systems to act with unified responses across agencies regardless of sector or geography. We cede our freedom of action with lengthy approval processes that delay US responses or set a very high threshold for responding to malicious cyber activities… the DoD is building the operational expertise and capacity to meet growing cyberspace threats and stop cyber aggression before it reaches our networks and systems. We need a policy framework that supports and enables these efforts.[782]

This statement seems to indicate that rather than more capabilities, the US military is arguing better governance is required to achieve deterrence, or at least a more holistic government approach. Yet the early US strategy had already clearly indicated the need for such a posture. Statements such as these indicate that US practice has been inconsistent. Another example here is the Cyber Deterrence Initiative (CDI). Originally outlined in the 2018 National Cyber Strategy, the CDI aimed to create a broad coalition of like-minded nations to join a US-led 'deterrence initiative' that includes collective response to malicious cyber activities by China, Russia, Iran and North Korea. And yet it has not been publicly mentioned by

[776] Alex S. Wilner, US cyber deterrence: Practice guiding theory, p.246; see also David J. Lonsdale, Warfighting for Cyber Deterrence: A Strategic and Moral Imperative (2017) p.421

[777] Ibid.; see also David J. Lonsdale, 2018, 'Warfighting for Cyber Deterrence: A Strategic and Moral Imperative', *Philosophy & Technology,* 31:3, 421, https://doi.org/10.1007/s13347-017-0252-8

[778] Richard Andres, 2017, 'Cyber Gray Space Deterrence', *PRISM,* 7:2, Cyber Gray Space Deterrence, p.92

[779] Tim Stevens, 2012, A Cyberwar of Ideas? Deterrence and Norms in Cyberspace, *Contemporary Security Policy*, 33:1, p.148

[780] Jun Osawa, 2017, 'The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?', *Asia-Pacific Review*, 24:2, 114

[781] General Tao Hanzhang, *Sun Tzu's The Art of War*, 31.

[782] Gen. Paul M. Nakasone, April 2018, 'Command Vision for US Cyber Command: Achieve and Maintain Cyberspace Superiority', United States Cyber Command, p.5

the US government since.[783] In 2019 Senator John McCain queried what progress had been made on this initiative, noting that nothing had officially been delivered.[784] And while this relates to an intelligence-sharing partnership between a coalition of like-minded partners – and thus may only exist in a classified form[785] – it cannot be considered part of a deterrence strategy since an approach that is entirely classified does not contribute to communicating deterrent intent or acceptable behaviour in cyberspace. Further, although those states who are party to the initiative may agree on certain norms or preferred responses to cyber-attacks – or even shared definitions of what comprises a cyber-attack – the fact remains that states and non-states outside that initiative are not able to participate or necessarily understand those responses.

The dissonance created by labelling an initiative as deterrence despite by definition not contributing to deterrence aims is thus further evidence of the incoherent US approach. Why has the US approach been so incomplete? And is this due to incomplete policy based on conflicting theory, or does it represent the need to revise deterrence theory applicability entirely? To answer these questions, this case study now turns to considering how poor definitions and inconsistent goals extended to the conceptualisation of the threat posed to US interests through cyberspace, which in turn made creating appropriate deterrence policy difficult.

4.4 Implications of a slowly evolving threat picture

The problem of poor definitions is first explored through US difficulty in publicly identifying and responding to cyber threats. While US policy recognised the potential harm from cyber threats, it took a substantial period of time to articulate these clearly. Once it did so, it then struggled to articulate appropriate responses to cyber-attacks, and determine at what point they would be enacted. In 2006, the then newly-appointed Secretary of Defense Robert Gates noted the increasing number of cyber-attacks and asked the Pentagon for a legal opinion regarding at what point a cyber-attack constituted an act of war under international law. Almost two years later he received a response, which was both vague and evasive.[786] The response stated that a cyber-attack might rise to a level that called for a military response and could be deemed an act of armed aggression under certain circumstances – but what those circumstances were, where the line should be drawn, even the criteria for drawing that line – were described as matters for policymakers, not lawyers to address.[787]

[783] 'National Cyber Strategy of the United States of America', September 2018, The White House, US, p.21; see also Josh Gold, n.d., 'The Five Eyes and Offensive Cyber Capabilities: Building a "Cyber Deterrence Initiative"', p.30; see also Brad D. Williams, 'US Urges "Like-Minded" Countries To Collaborate On Cyber Deterrence', *Breaking Defense* [blog], 24 April 2019, https://breakingdefense.sites.breakingmedia.com/2019/04/us-urging-likeminded-countries-to-collaborate-on-cyber-deterrence/

[784] John S McCain, 'National Defense Authorization Act', Fiscal Year 2019, Conference Report to Accompany H.R. 5515

[785] Josh Gold, n.d., 'The Five Eyes and Offensive Cyber Capabilities: Building a "Cyber Deterrence Initiative"', p.30

[786] Gordon Goldstein, 18 March 2016, 'Cyber war – bigger than ever – is here to stay', *The Washington Post*

[787] Kaplan p.214

To some extent, the problem in articulating such circumstances may, as Tim Stevens argues, be in part due to the constantly evolving nature of the threat;[788] a threat Osawa characterised in 2020 as an 'increasing issue with potentially severe consequences'.[789] And Alexander Klimburg agrees the overall level of destructive cyber-attacks is rising.[790] It is important to consider where these threat assessments are arising from, since the threat might also be inflated in some circumstances.[791] Lucas Kello also argues that the cyber threat is inflated, and that such inflation is not just popular but official myth.[792]

But what reason would strategists have to inflate perceived threats? As Bruce Schneider has observed this is at least partly due to an ongoing power struggle in the US government over who is in charge of cybersecurity and how much control the government will have over civilian networks.[793] Schneider goes further, asserting that by 'beating the drums of war', the military is leading policy development for its own benefit.[794] The extent of this risk is a critical question for states wishing to construct cybersecurity strategy given that a state cannot effectively deter threats if it has not agreed on their scale or severity.

That said, of course, the US policy position on the threat is mixed and has shifted over time from being initially vague to increasingly specific. For example, in 2009 President Barack Obama defined the cyber threat as 'a key security risk, particularly to economic prosperity':

> America's economic prosperity in the 21st century will depend on cybersecurity. And this is also a matter of public safety and national security. We count on computer networks to deliver our oil and gas, our power and our water. We rely on them for public transportation and air traffic control. Yet we know that cyber intruders have probed our electrical grid and that in other countries cyber-attacks have plunged entire cities into darkness.[795]

Yet despite this description of potential vulnerabilities, it was not specific to American circumstances, nor did it provide a strategy for securing US interests in cyberspace. To some extent the 2010 US National Intelligence Annual Threat Assessment provided some clarity on threat vectors, assessing the US as being 'severely threatened' by cyber-attacks from a range of sources. These included nation-states, terrorist networks, organised criminal groups, individuals, and other cyber actors with varying combinations of

[788] Tim Steven, 2012, 'A Cyberwar of Ideas? Deterrence and Norms in Cyberspace', *Contemporary Security Policy*, 33:1, 151
[789] Jun Osawa, 2017, 'The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?', *Asia-Pacific Review*, 24:2, 125
[790] Alexander Klimburg, Mixed Signals, p. 115, see also Richard Andres Cyber Gray Space Deterrence p. 91
[791] Joseph S. Nye, 2019, 'Deterrence in Cyberspace', *The ASPI Strategist* [blog], 1
[792] Lucas Kello, The Virtual Weapon and International Order, p.32
[793] Ibid
[794] Ibid
[795] US President Barack Obama, 29 May 2009, 'Remarks by the President on Securing Our Nations Cyber Infrastructure', The White House, US, from https://obamawhitehoU.S.e.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure

access, technical sophistication and intent.[796] This specifically highlighted the lack of threat awareness as a problem:

> The United States confronts a dangerous combination of known and unknown vulnerabilities, strong and rapidly expanding adversary capabilities, and a lack of comprehensive threat awareness. Malicious cyber activity is occurring on an unprecedented scale with extraordinary sophistication. While both the threats and technologies associated with cyberspace are dynamic, the existing balance in network technology favors malicious actors, and is likely to continue to do so for the foreseeable future. Sensitive information is stolen daily from both government and private sector networks, undermining confidence in our information systems, and in the very information these systems were intended to convey. We often find persistent, unauthorized, and at times, unattributable presences on exploited networks, the hallmark of an unknown adversary intending to do far more than merely demonstrate skill or mock a vulnerability. We cannot be certain that our cyberspace infrastructure will remain available and reliable during a time of crisis. Within this dynamic environment, we are confronting threats that are both more targeted and more serious. New cyber security approaches must continually be developed, tested, and implemented to respond to new threat technologies and strategies.[797]

This appears to indicate that while the US viewed threats in 2010 as serious, they were still not well understood – or, if they were well understood it was not considered necessary to express this understanding in policy. No individual threat actors were named, and the document's conception of the threat is broad, listing potential harms and vulnerabilities rather than specific threats. In 2017 the diversity of threats was reiterated by the then US Director of National Intelligence James Clapper, who observed that 'the breadth of cyber threats posed to US national and economic security has become increasingly diverse, sophisticated and serious, leading to physical, security, economic and psychological consequences.'[798]

By 2018, however, US threat assessments had become far more specific. The Worldwide Threat Assessment published by the US Director of National Intelligence is instructive on this score:

> Adversaries and Malign Actors Poised for Aggression: Russia, China, Iran, and North Korea will pose the greatest cyber threats to the United States during the next year. These states are using cyber operations as a low-cost tool of statecraft, and we assess that they will work to use cyber operations to achieve strategic objectives unless they face clear repercussions for their cyber operations. Non-state actors will continue to use cyber operations for financial crime and to enable propaganda and messaging.[799]

[796] Dennis C. Blair, Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence, 2 February 2010, from https://www.dni.gov/files/documents/Newsroom/Testimonies/20100202_testimony.pdf

[797] Ibid

[798] The Hon. James R. Clapper, 5 January 2017, Joint Statement for the Record to the Senate Armed Services Committee on Foreign Threats to the United States

[799] Daniel R. Coates, 6 March 2018, (DNI) Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community

This assessment represents the first time the US specifically identified named states as the major threat actors, as well as the types of threats they were assessed as posing. This indicates a degree of learning on the part of the US given that the threat became better understood over time. This theme of explicit naming of threat actors continued in the 2018 National Cyber Strategy, with President Donald Trump's administration articulating the increasing seriousness of the threat as part of a new era of cyber competition:

> Russia, Iran and North Korea conducted reckless cyber-attacks that harmed American and international businesses and our allies and partners without paying costs likely to deter future aggression. China engaged in cyber-enabled economic espionage and trillions of dollars of intellectual property. Non-state actors – including terrorist and criminals – exploited cyberspace to profit, recruit, propagandize and attack the United States and its allies and partners, with their actions often shielded by hostile states…New threats and a new era of strategic competition demand a new cyber strategy that responds to new realities, reduces vulnerabilities, deters adversaries, and safeguards opportunities for the American people to thrive.[800]

The push for a new cyber strategy seems to imply the existing strategy was not sufficient to manage the severity of the threat. US Cyber Command subsequently reinforced this, arguing 'Cyberspace threats are growing. They transcend geographic boundaries.'[801] The problem with this definition of threats and the centring of the military in deterring them is that the threats are poorly defined, resulting in the military having an unclear remit. This is problematic because there is disagreement about whether this view of the threat posed by cyber-attacks is accurate. As Brandon Valeriano and Ryan Maness note, the danger posed by cyber often arises out of self-interest in the need to perpetuate a national security state.[802] And while achieving consensus on the type and level of threat posed by cyber-attacks is a complex task, a state cannot hope to deter a threat without a pragmatic and broadly agreed definition of what that threat is. The confusion between potential and actual threats posed in cyberspace has therefore dogged US policymakers attempting to construct a coherent deterrence approach. Without agreement on what the most likely and most dangerous threats are, and how and why they may materialise, it is not possible to target policy appropriately. An example of this is the oft-repeated fear of a 'cyber Pearl Harbour', a term coined by Richard Clarke[803] that entered common usage after a speech by former Secretary of Defense Leon Panetta in 2012:

[800] 'National Cyber Strategy of the United States of America', p.2.

[801] Gen. Paul M. Nakasone, April 2018, 'Command Vision for US Cyber Command: Achieve and Maintain Cyberspace Superiority', United States Cyber Command

[802] Brandon Valeriano and Ryan Maness, Persistent Enemies and Cyber, in Derek S. Reveron, *Cyberspace and National Security: Threats, Opportunities and Power in a Virtual World*, p.155

[803] Alex Wong, 'Seven Questions: Richard Clarke on the Next Cyber Pearl Harbor', Foreign Policy, April 2 2008

> A cyber-attack perpetrated by nation states and violent extremist groups could be as destructive as the terrorist attack on 9/11… the collective result of these kinds of attacks could be a cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life.[804]

Despite this, N.J. Ryan characterises the idea of a cyber 9-11 or Pearl Harbor as an unlikely 'black swan' event.[805] And Nye agrees such threats are exaggerated, arguing that major state actors are more likely to be entangled in interdependent relationships than are many non-state actors.[806] Nye relies on the logic of engagement as a preventer of conflict, however the question of what is conflict in cyberspace and when an attack could be considered an act of war has not been decided in US policy. This is a problem because what the US may regard as 'engagement', an adversary may consider as offensive and provocative activity. On this point the 2015 National Security Strategy stated that 'the danger of disruptive and even destructive cyber-attack is growing, and the risk of another global economic slowdown remains'[807] as well as listing 'malicious cyber activity' as a global threat. [808] But while nowhere in this policy is the term cyber-attack defined, the Strategy claims the military 'will remain ready to deter and defeat threats to the homeland, including against missile, cyber, and terrorist attacks, while mitigating the effects of potential attacks and natural disasters.'[809] There is a clear disconnect here in that while strategists had not yet agreed on the nature of the potential threat, the policy stated the US was ready to deter and defeat it.

4.5 Conceptualising the threat space: Cyber as a domain

In order to create deterrence policy states must not only identify the threat they wish to deter, but also the space in which they wish to deter attacks. But the conceptualisation of cyberspace as a domain has remained a definitional problem for the US despite significant policy effort. The concept of domains evolved as a tool used by militaries to separate areas of warfare, with the traditionally accepted domains being land, sea, air and space.[810] The first US designation of cyber as a domain was in the 2006 National Military Strategy for Cyberspace Operations, which described the cyber domain as 'the use of electronics and the electromagnetic spectrum to store, modify and exchange data via networked systems and associated physical infrastructures.'[811] This was originally a classified document. The first public description of cyber as a domain was in the 2010 National Security Strategy, which argued the military required 'the necessary capabilities across all domains – land, air, sea, space, and cyber'.[812] Once again, this

[804] 'Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City', US Department of Defense

[805] N. J. Ryan, 2018, 'Five Kinds of Cyber Deterrence', *Philosophy & Technology*, 31, 333

[806] Joseph S. Nye, 2019, 'Deterrence in Cyberspace', *The ASPI Strategist* [blog]

[807] Barack Obama, February 2015, 'National Security Strategy', The White House, US

[808] Ibid

[809] Ibid

[810] For a detailed explanation of how domains develop, see: Bryan James Nakayama, 2018, 'From Aerospace to Cyberspace: The Evolution of Domains of Warfare', Doctoral Thesis, University of Minnesota

[811] US National Military Strategy for Cyberspace Operations, 2006, US DoD quoted in A. Wilner, 2020, 'US Cyber Deterrence: Practice Guiding Theory', *Journal of Strategic Studies*, 43:2, 251

[812] President Barack Obama, May 2010, 'National Security Strategy', The White House, US, p.22

definition through the lens of additional military capabilities demonstrates the influence the US military has had on deterrence policy for cyberspace.

In 2010, then US Deputy Defense Secretary Lynn's seminal paper 'Defending a new domain: The Pentagon's Cybersecurity Strategy' designated cyber as a domain and deterrence as the dominant strategic approach to protecting that domain.[813] The subsequent 2010 Quadrennial Defense Review noted 'Future adversaries will likely possess sophisticated capabilities designed to contest or deny command of the air, sea, space, and cyberspace domains.'[814] The 2011 US DOD Strategy for Operating in Cyberspace explains the public reason for adopting this conception:

> Though the networks and systems that make up cyberspace are man-made, often privately owned, and primarily civilian in use, treating cyberspace as a domain is a critical organizing concept for DoD's national security missions. This allows DoD to organize, train, and equip for cyberspace as we do in air, land, maritime, and space to support national security interests.[815]

These policies demonstrate that the decision to treat cyberspace as a domain was a practical one, driven by the US military to allow for better organisation at the operational level. The entrenched nature of this view was explained by former National Security Agency Director Michael Hayden in 2010, who claimed that 'Like everyone else who is or has been in a US military uniform, I think of cyber as a domain.'[816] But while this characterisation may seem logical organisationally, it has implications for creating deterrence strategies.[817] Firstly, as explicitly noted in the 2011 DoD Strategy, there is an immediate problem with the military designating cyberspace as a domain of warfare in that the military was claiming ownership and protection of a space where many targets are privately owned and civilian in use.[818] Perhaps the clearest example of this is the potential for cyber-attacks on networks that control critical civilian infrastructure.[819] US electricity grids, for instance, present a particularly challenging space to defend. As Lynn has argued, an attack on a power grids could severely damage the ability to deploy or re-supply troops,[820] but the protection of those networks is the responsibility of individual private companies. And even within those companies there is great variation between not-for-profit municipal electric utility; electric cooperatives owned by members; private, for-profit electric utility owned by stockholders (often called an investor-owned utility); or the few federally owned power authorities also generate, buy, sell, and distribute

[813] William J Lynn III, 2010, 'Defending a new domain: The Pentagon's Cyberstrategy', *Foreign Affairs*, Sept/Oct 2010

[814] 'Quadrennial Defense Review Report 2010', February 2010, US Department of Defense, p.9, https://history.defense.gov/Portals/70/Documents/quadrennial/QDR2010.pdf?ver=vVJYRVwNdnGb_00ixF0UfQ%3d%3d.

[815] "Department of Defense: Strategy for Operating in Cyberspace', July 2011, US Department of Defense, p.5

[816] Michael V. Hayden, 2011, 'The Future of Things "Cyber"', *Strategic Studies Quarterly*, 3

[817] David J. Lonsdale, 2018, 'Warfighting for Cyber Deterrence: A Strategic and Moral Imperative', *Philosophy & Technology,* 31:3, 410, https://doi.org/10.1007/s13347-017-0252-8

[818] Department of Defense: Strategy for Operating in Cyberspace', July 2011, US Department of Defense, p.5

[819] William J Lynn III, 2010, 'Defending a new domain: The Pentagon's Cyberstrategy', *Foreign Affairs*, Sept/Oct 2010, 100

[820] Ibid

power.[821] Thus the challenge for the federal government is that they are seeking to deter attacks on different levels of private industry with widely varying capabilities, and such private utility companies often lack full understanding of their cybersecurity posture.[822] [823]

At the same time, states such as Russia, China and Iran and non-state actors including foreign terrorist and hacktivist groups are noted by the US government as posing varying threats to the power grid, seeking to exploit cyber vulnerabilities.[824] This interaction with private industry does not occur in any other domain of warfare, and it requires a more carefully managed approach to providing security and conducting operations than the military has experience with or the mandate to implement.[825] Deterrence in this environment is far more complex, as the example of the Sony 'hack' demonstrates. This attack by North Korea took down three-quarters of the computers and servers of a major US-based corporation in retaliation for an unflattering movie about North Korea's leader.[826] The White House declared it a 'serious matter of national security' but President Obama quickly corrected public comments from US senators claiming that the attack amounted to an 'act of war'.[827]

Thus we begin to see the problems with the imprecise language in US policy: what role does, and indeed should, the US military have in attempting to deter attacks on US private corporations? This problem was recognised from the early days of deterrence being considered as an option for improving cybersecurity. Richard Clarke and Robert Knake expressed this concern in 2010, where they noted that the US Cyber Command's mission was to defend the DoD and potentially some other government agencies, but there were no plans or capabilities for it to defend civilian infrastructure.[828] And the US literature on the topic has continued to note the problems posed by the use of the term 'domain' for cyberspace since, but has not reached a settled position as to its usefulness. While such disagreement is not unusual in academic circles, it also carries through the policy space. This is problematic because if strategists and policymakers are unclear on what they are trying to deter attacks from, or even where they are trying to deter those attacks, making effective deterrence policy is immediately impossible. While Osawa is correct that the conception of cyberspace as a domain is not limited to the military, but also used by many national security experts,[829] it is not universal. As Chris Demchak argues that cyberspace does not fit into the

[821] 'Delivery to Consumers – US Energy Information Administration (EIA)', accessed 31 August 2021, https://www.eia.gov/energyexplained/electricity/delivery-to-consumers.php.

[822] Colleen Glenn, Dane Sterbentz, and Aaron Wright, 20 December 2016, 'Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector', p.2-5

[823] Ibid

[824] Ibid

[825] Patrick M. Morgan, 2003, *Deterrence Now*, Cambridge University Press, p.10

[826] Kaplan, p.55

[827] Ibid, p.65

[828] Richard A. Clarke and Robert K. Knake, 2010, 2010, *Cyber War: The Next Threat to National Security and What To Do About It,* New York: HarperCollins, p.43

[829] Jun Osawa, 2017, 'The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?', *Asia-Pacific Review*, 24:2, p.124; see also Christian Leuprecht, Joseph Szeman and David B. Skillicorn, 2019, 'The Damoclean sword of offensive cyber: Policy uncertainty and collective insecurity', *Contemporary Security Policy*, 40:3, p.382

framework of a military domain, because while the term 'domain' is used by the US military to blend 'cybered' conflicts into the traditional mould of armed struggles, cyberspace is in reality not conveniently bounded and the designation does not help guide national leaders in dealing with cybered conflict.[830] The problem of delineating the public/private ownership is explicitly noted in the 2015 DoD Cyber Strategy, which notes:

> The United States government has a limited and specific role to play in defending the nation against cyberattacks of significant consequence. The private sector owns and operates over ninety percent of all of the networks and infrastructure of cyberspace and is thus the first line of defense.[831]

With 90% of US networks infrastructure being privately owned, the decision to treat cyberspace as a domain of warfare is clearly problematic. The US must somehow secure and deter attacks on a space it has no control over but is deemed essential for daily US life. The reality is that any operations in all other domains of warfare depend on cyberspace.[832] And while the military aims to deter threats against US interests, for the first time those interests are in fact mostly civilian. The US DoD 2015 Strategy recognised this:

> One of the most important steps for improving the United States' overall cybersecurity posture is for companies to prioritize the networks and data that they must protect and to invest in improving their own cybersecurity. While the U.S. government must prepare to defend the country against the most dangerous attacks, the majority of intrusions can be stopped through relatively basic cybersecurity investments that companies can and must make themselves.[833]

This would seem to demonstrate that treating cyber as a domain of warfare in and of itself is complex, as it cannot not be considered separately to other domains.[834] Here Kello advocates for the separation of policy for cyberspace as a technical plane comprised of machines and networks, kept apart from policy for the cyber domain which he defines as a political and social plane subject to wholly different interventions and behaviours.[835] However the use of 'domain' as a term encompassing both the human and technical planes is firmly embedded in existing policy; such a separation would require an entirely new approach to US cybersecurity policy which has not received broad endorsement.

But if Jervis is correct that it is far from clear that cyber should be considered a domain, as cyber is 'merely an instrument that can be used to support national policies',[836] then the military's attempts to treat

[830] Chris Demchak, 2012, 'Cybered Conflict, Cyber Power, and Security Resilience as Strategy', in Derek S. Reveron, *Cyberspace and National Security: Threats, Opportunities and Power in a Virtual World*, Georgetown University Press, p.124

[831] Ash Carter, April 2015, 'The DoD Cyber Strategy', US Department of Defense

[832] Jun Osawa, 2017, 'The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?', *Asia-Pacific Review*, 24:2, 124

[833] Ash Carter, April 2015, 'The DoD Cyber Strategy', US Department of Defense

[834] Will Goodman, 2010, 'Cyber Deterrence: Tougher in Theory than in Practice?', *Strategic Studies Quarterly*, Fall 2010, 102

[835] Lucas Kello, The Virtual Weapon and International Order, p.46

[836] Robert Jervis, 2016, 'Some Thoughts on Deterrence in the Cyber Era', *Journal of Information Warfare*, 15:2, 66

it as a domain of warfare are problematic for deterrence in two areas. First, as Clarke and Knake noted in 2010, the perception of cyberspace as a domain where fighting must take place and the US must dominate, pervades American military thinking. [837] This may help explain the US over-reliance on capabilities to the detriment of the other requirements of deterrence. Second, the tendency of military strategists to conflate deterrence with warfare in the US[838] carries the potential for unintended escalation. This is because for the military, the emphasis will always be on engaging and fighting, rather than preventing conflict, particularly in a sphere where lives are not directly threatened.[839]

4.6 Deterrence by denial? The US struggle to define 'success'

This chapter has so far argued the US approach to deterrence has been hamstrung by inconsistent definitions which produced similarly inconsistent policies. It is perhaps then unsurprising that the US also struggled to define what deterrence success might like look like. Regardless of ongoing debates over defining the key issues for deterrence in cyberspace, the evolution in deterrence policy demonstrates that the US policy establishment – led by the military – assessed that deterrence had failed to deter unwanted cyber-attacks or an acceptable level of cybersecurity.[840] And yet that was arguably predictable. As Keith Payne has argued, different players and contexts have different effects on how deterrence operates, or if it can operate at all.[841] A key reason for this may have been the construction of deterrence policy through the lens of denial and punishment to cyberspace, concepts developed as part of the particular circumstances of the Cold War, rather than through the classic lens of deterrence principles adapted for cyberspace.[842]

Deterrence by denial – the idea you can raise your defences to such a level that if an adversary attacked, they would be denied their aim[843] – was an early US policy goal for cyberspace. The 2011 International Strategy for Cyberspace stated: 'The United States will ensure that the risks associated with attacking or exploiting our networks vastly outweigh the potential benefits.'[844] But as already noted, creating deterrence by denial is further complicated by civilian ownership of infrastructure. Part of the difficulty of

[837] Richard A. Clarke and Robert K. Knake, 2010, *Cyber War: The Next Threat to National Security and What To Do About It,* New York: HarperCollins, p.44

[838] Alex Wilner, 2020, 'U.S. cyber deterrence: Practice guiding theory', *Journal of Strategic Studies*, 43:2, 256; see also David J. Lonsdale, 2018, 'Warfighting for Cyber Deterrence: A Strategic and Moral Imperative', *Philosophy & Technology,* 31:3, 409-429, https://doi.org/10.1007/s13347-017-0252-8

[839] Renshon, *National Security in the Obama Administration: Reassessing the Bush Doctrine*, p.126

[840] David J. Lonsdale, 2018, 'Warfighting for Cyber Deterrence: A Strategic and Moral Imperative', *Philosophy & Technology,* 31:3, 429, https://doi.org/10.1007/s13347-017-0252-8

[841] Keith B. Payne, 2001, *The Fallacies of Cold War Deterrence and a New Direction*, Lexington: University Press of Kentucky, p.169

[842] Maj. Timothy M. Goines, 2017, 'Overcoming the Cyber Weapons Paradox', *Strategic Studies Quarterly*, Winter 2017 90; see also Aaron F. Brantly, 2020, 'Entanglement in Cyberspace: Minding the Deterrence Gap', *Democracy and Security*, 16:3, 210

[843] N. J. Ryan, 2018, 'Five Kinds of Cyber Deterrence', *Philosophy & Technology*, 31, 334; see also Lucas Kello, The Virtual Weapon and International Order, p.197

[844] Barack Obama, 2011, 'International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World', The White House, US

applying a policy of denial in cyberspace is technical, in that the types of hardening that produces more secure online environments would not generally be accepted by the majority of a democratic population.[845] This may explain why US policy moved fairly quickly to the view that deterrence by denial alone was insufficient, and further measures would be required. Indeed, as Leon Panetta stated in 2012, 'we won't succeed in preventing a cyber-attack through improved defenses alone.'[846]

The translation of denial and punishment into cyberspace was always going to be problematic for the US[847] given the low barriers to entry for cyber-attacks,[848] and low or no penalties for conducting attacks.[849] The difficulty of establishing deterrence by denial is demonstrated by the 2006 Chairman of the Joint Chiefs view of the desired military end state: 'adversaries are deterred from establishing or employing offensive capabilities against US interests in cyberspace.'[850] The idea of successful denial as adversaries not building or using any offensive capabilities was clearly an ambitious goal which has not been realised. The US has had to greatly reduce their idea of success as this goal proved unachievable. By 2018, the Director of National Intelligence described the cyber threat as a growing risk, stating:

> Russia, China, Iran, and North Korea will pose the greatest cyber threats to the United States during the next year. These states are using cyber operations as a low-cost tool of statecraft, and we assess that they will work to use cyber operations to achieve strategic objectives unless they face clear repercussions for their cyber operations.[851]

This description clearly demonstrates that the US had failed to deter adversaries from establishing or using capabilities against US interests. Despite this description of the perceived threat, the 2018 Statement also noted that the use of cyber-attacks as a foreign policy tool outside of military conflict had been 'mostly limited to sporadic lower-level attacks.'[852] Therefore whether the US has succeeded or failed in creating deterrence depends on the criteria used to judge it. As David J. Lonsdale points out, the US has not deterred daily low-level nuisance attacks; however, if deterrence success is only concerned with preventing large-scale attacks, the picture is more positive.[853] Part of the confusion regarding what comprised success over the period is due to the significant shifts in policy goals over the period. Within six years of the declared US intent to adopt strategies of deterrence by denial in cyberspace, the US had

[845] Lin and Kerr, 'On Cyber-Enabled Information Warfare and Information Operations'.

[846] 'Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City', U.S. Department of Defense, accessed 24 June 2021

[847] See Richard Andres, 2017, 'Cyber Gray Space Deterrence', *PRISM,* 7: 2, 94; see also Lucas Kello, The Virtual Weapon and International Order, p.196; see also Joseph S. Nye Jnr, 2016/17, 'Deterrence and Dissuasion in Cyberspace', *International Security*, 41:3 (Winter 2016/17), 44-71

[848] Stevens, 'A Cyberwar of Ideas? Deterrence and Norms in Cyberspace', 148; see also Gartzke, 2013, The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth, *International Security,* 38:2, p.45

[849] Brantly, 'Entanglement in Cyberspace: Minding the Deterrence Gap', p.210.

[850] Jason Healey, The implications of persistent (and permanent) engagement in cyberspace p.4

[851] Daniel R. Coates, Director National Intelligence, 13 February 2018, Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community

[852] Ibid

[853] David J. Lonsdale, 2018, 'Warfighting for Cyber Deterrence: A Strategic and Moral Imperative', *Philosophy & Technology,* 31:3, 421, https://doi.org/10.1007/s13347-017-0252-8

failed to effectively translate its Cold War deterrence theory into policy and strategy.[854] This is attributed by authors such as Jim Chen to the heavy influence of the nuclear and conventional deterrence models of deterrence; the complexities when attempting to apply these models to cyberspace meant the ideas of success were zero-sum and thus doomed to fail.[855] This view also seems to have influenced the assessment in 2018 from the incoming head of Cyber Command General Paul Nakasone that cyber deterrence had failed.[856] As the 2018 Cyber Command vision statement noted:

> Adversaries direct continuous operations and activities against our allies and us in campaigns short of open warfare to achieve competitive advantage and impair US interests.[857]

This contention over failure occurs because the conceptualisation of success for US deterrence in cyberspace was never clearly defined. Despite the fact that the declared US deterrence strategy had been judged a failure, the 2018 National Cyber Strategy still included a role for deterrence in strategy, stating:

> As the United States continues to promote consensus on what constitutes responsible state behavior in cyberspace, we must also work to ensure that there are consequences for irresponsible behavior that harms the United States and our partners. All instruments of national power are available to prevent, respond to, and deter malicious cyber activity against the United States. This includes diplomatic, information, military (both kinetic and cyber), financial, intelligence, public attribution, and law enforcement capabilities. The United States will formalize and make routine how we work with like-minded partners to attribute and deter malicious cyber activities with integrated strategies that impose swift, costly, and transparent consequences when malicious actors harm the United States or our partners.[858]

Importantly, the Strategy still did not define what successful deterrence was, instead referring to the looser goal of 'securing cyberspace'.[859] Without a clear vision of what cyber deterrence is, or what success might look like in cyberspace, the US was not able to appropriately target policy; unsurprisingly, strategists and policymakers turned their attention towards punishment. But as the next section will show, the idea of the US being able to impose 'swift, costly, and transparent consequences when malicious partners harm the US' in response to cyber-attacks has remained elusive.

[854] Tim Stevens, 2012, 'A Cyberwar of Ideas? Deterrence and Norms in Cyberspace', *Contemporary Security Policy*, 33:1, 148

[855] Jim Chen, 2017, 'Cyber Deterrence by Engagement and Surprise', *PRISM*, 7:2, 101; see also Clorinda Trujillo, 2014, 'The Limits of Cyberspace Deterrence', *Joint Force Quarterly*, 75:4

[856] Cited in Alexander Klimburg, 2020 'Mixed Signals: A Flawed Approach to Cyber Deterrence', *Survival,* 62:1, 110

[857] Gen. Paul M. Nakasone, April 2018, 'Command Vision for US Cyber Command: Achieve and Maintain Cyberspace Superiority', United States Cyber Command, accessed 24 June 2021

[858] 'National Cyber Strategy of the United States of America', September 2018, The White House, US, p.21

[859] Ibid

4.7 The US pursuit of options: Deterrence by punishment

Deterrence by punishment, where the defender prevents major attacks by the pledge of severe penalties,[860] is another concept the US has struggled to deploy for cyberspace. To effectively punish or even threaten punishment, the US must not only know whom to punish, but more importantly make the political decision as to what suitable punishment is – and carry out that punishment. The issue of identifying attackers in cyberspace – attribution – is described by Libicki as the difference between a deterrence policy that says 'don't do this' and one that says 'don't get caught doing this'.[861] The so-called 'attribution problem', as outlined by Clarke and Landau, is that attribution in cyberspace was exceedingly difficult, if not impossible – rendering deterrence by punishment an immediate failure in cyberspace.[862] As then Deputy Secretary for Defense Lynn noted in 2010:

> If you don't know who to attribute an attack to, you can't retaliate against that attack, and as a result, you can't deter through punishment, you can't deter by retaliating against the attack.[863]

This was first noted as a problem the US needed to address in the 2011 DoD Strategy for Operating in Cyberspace.[864]

> The same technical protocols of the Internet that have facilitated the explosive growth of cyberspace also provide some measure of anonymity. Our potential adversaries, both nations and non-state actors, clearly understand this dynamic and seek to use the challenge of attribution to their strategic advantage.[865]

However, the US had clearly solved the attribution problem by 2018, when the US government published its 'Strategies for Cyber Attribution'. The publication of this document as a guide to how the US intended to attribute cyber-attacks was both a communication of intent and capability, and was probably intended to improve US credibility. The 2018 US Cyber Strategy had the stated aim of being able to 'attribute and deter malicious cyber activities with integrated strategies that impost swift, costly and transparent consequences when malicious actors harm the United States or our partners.'[866] And according to its own policy the US is capable of attributing attacks where it chooses to do so. The 2018 Guide to Attribution, published by the Office of the Director of National Intelligence,[867] provided this explanation:

[860] Schelling, Arms and Influence, pp.148-149; see also Morgan, Deterrence Now, pp.15-17; see also Chapter 1 for more detail

[861] Martin C. Libicki, 2016, *Cyberspace in Peace and War,* Annapolis, p.238; see also David D. Clark and Susan Landau, 2011, 'Untangling Attribution', *Harvard National Security Journal*, 2

[862] David D. Clark and Susan Landau, 2011, 'Untangling Attribution'

[863] Quoted in James Joyner, 'Competing Transatlantic Visions of Cybersecurity', in *Derek S. Reveron, 2012, Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, p.160

[864] 'Department of Defense Strategy for Operating in Cyberspace', 2011, p.10

[865] 'Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934', November 2011, US Department of Defense, https://fas.org/irp/eprint/dod-cyber.pdf.

[866] 'National Cyber Strategy of the United States of America', September 2018, The White House, US, p.21

[867] 'A Guide to Cyber Attribution: Leading Intelligence Integration' (Office of the Director of National Intelligence, 14 September 2018), https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf.

> Establishing attribution for cyber operations is difficult but not impossible. No simple technical process or automated solution for determining responsibility for cyber operations exists. The painstaking work in many cases requires weeks or months of analyzing intelligence and forensics to assess culpability. In some instances, the IC (intelligence Community) can establish cyber attribution within hours of an incident but the accuracy and confidence of the attribution will vary depending on available data.[868]

But the publication of this guide did not have the intended effect. One reason for this was the US preference for collective attribution, whereby a group of states jointly attribute an attack to a specific state or location,[869] quickly proved problematic. The intent of collective attribution was to present a united front to attackers, as stated in the first US International Strategy for Cyberspace in 2011[870] which argued not only for a collective approach but for shared military alliances, indicating the seriousness of the threat to the US.

> Moving forward, the United States will continue to work with the militaries and civilian counterparts of our allies and partners to expand situational awareness and shared warning systems, enhance our ability to work together in times of peace and crisis, and develop the means and method of collective self-defense in cyberspace. Such military alliances and partnerships will bolster our collective deterrence capabilities and strengthen our ability to defend the United States against state and non-state actors. [871]

And the importance the US placed on collective deterrence was reiterated in the 2011 US DoD Cyber Strategy:

> Strategically, a unified coalition sends a message that the United States and its allies and partners are aligned in collective defense. In addition to the Five Eyes treaty partners, DoD works closely with key partners in the Middle East, the Asia-Pacific, and Europe to understand the cybersecurity environment and build cyber defense capacity.[872]

However, one of the key issues with collective attribution is that building such a coalition in response to cyber-attacks takes time[873] and a delayed attribution is far less effective.[874] The case of NotPetya provides a clear example of an attribution that was delayed in order to achieve a collective approach. NotPetya was a malware attack that encrypted the hard drives of computers it infected. Unlike the Petya attacks however, which were designed to gain funds through demands for Bitcoin, NotPetya was a state-

[868] 'A Guide to Cyber Attribution: Leading Intelligence Integration', p.2.
[869] Barack Obama, 2011, 'International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World', The White House, US
[870] Ibid
[871] Ibid, p.3
[872] 'Department of Defense Strategy for Operating in Cyberspace', p.2.
[873] John S. II Davis and Rand Corporation, 2017, 'Stateless Attribution: Toward International Accountability in Cyberspace' RR-2081-MS, p.17
[874] Ibid, p.23

sponsored Russian cyber-attack masquerading as ransomware.[875] The attack was launched in June 2017, and an official public US response did not occur until February 2018, over seven months later.[876] Although several other nations joined the US in attribution the attack to Russia, their views of both the severity of the attack and the appropriate response varied. While the US initially cited 'billions of dollars in damage, the UK estimated the costs at $1.2 billion.[877]

By 2019, the global damage bill was estimated at $10 billion. According to Leuprecht et al[878] these different estimates over time demonstrates a further difficulty with assessing the impacts of cyber-attacks in that damages are often not immediately apparent. This is an issue that then complicates designing the appropriate level of response.[879] And even where the attribution of responsibility can be agreed upon, and the level of damage is agreed, a further barrier is the fact that the willingness to punish transgressions – or indeed even what constitutes an appropriate punishment – is not uniform. For example, the perceived inability to accurately predict the effects of a retaliatory cyber act renders a 'like-for-like' cyber response unattractive to decision makers.[880] But if the response is not cyber, the US has struggled to decide on the appropriate alternatives, which results in the second issue: a lack of certainty and predictability for both allies and adversaries. In the case of NotPetya, the delayed US response was limited to threatening unspecified 'international consequences'.[881] This threat of consequences only manifested into a limited response several years later: in October 2020 the US Department of Justice released an indictment against six current and former Russian military intelligence officers.[882] These limited (and much delayed) public responses demonstrates a key problems with the US decision to apply different standards of attribution at different times. The decision to rely on a legal attribution lead to a seemingly low-level response; a response adversaries were likely to judge as not acting as a deterrent.[883] But as Greiman argues, there is no international legal obligation to reveal the grounds on which attribution is based prior to taking appropriate action.[884] The US was effectively limiting its own responses, for reasons that are unclear. Nye argues that this behaviour is a result of the Cold War still influencing US thinking, and that responding with other capabilities remains problematic while 'our minds remain captured by an image of deterrence

[875] John S. II Davis and Rand Corporation, 2017, 'Stateless Attribution: Toward International Accountability in Cyberspace' RR-2081-MS, p.17

[876] Steven Nelson, 15 February 2018, 'White House Accuses Russia of NotPetya Cyberattack, Threatens Unspecified "Consequences"', *Washington Examiner*, sec. Politics

[877] Ibid

[878] See Christian Leuprecht, Joseph Szeman, and David B. Skillicorn, 2019, 'The Damoclean Sword of Offensive Cyber: Policy Uncertainty and Collective Insecurity', *Contemporary Security Policy,* 40:3, 398

[879] Ibid

[880] Jeffrey R. Cooper, A New Framework for Cyber Deterrence, p.106

[881] Steven Nelson, 15 February 2018, 'White House Accuses Russia of NotPetya Cyberattack, Threatens Unspecified "Consequences"', *Washington Examiner,* sec. Politics

[882] Charlie Mitchell, 20 October 2020, 'U.S. Indictment of Russian Intelligence Officers Reflects First Culpability for Devastating "NotPetya" Attack', *Inside Cybersecurity*

[883] Ibid

[884] Virginia Greiman, 2021, 'The Politics and Practice of Cyber Attribution: A Global Legal Perspective', in *International Conference on Cyber Warfare and Security,* Reading, United Kingdom: Academic Conferences International Limited, p.102

shaped by the Cold War: a threat of massive retaliation by nuclear means.'[885] As Senator John McCain argued in 2015:

> Our adversaries see our response as timid and ineffectual. Put simply, the problem is a lack of deterrence. The administration has not demonstrated to our adversaries that the consequences of continued cyber-attacks against us outweigh the benefit.[886]

The lack of certainty, coupled with the preference for collective attribution to unclear attribution standards, has significantly damaged US credibility in cyberspace. The arguments that the US cannot conduct punishment because attribution is too complex, and collective attribution and action is too slow, help explain why deterrence by punishment has been judged an ineffective option in cyberspace.[887] But there are two counter arguments worth considering. On the one hand, the fact the US not only judged attribution was possible but published a guide on how they intended to carry it out speaks to both capability and communication, and indicates that the US had clearly rapidly improved the quality and speed of attribution.[888] Indeed, the view that attribution is too technically complex to be relied upon is outdated and has since been repeatedly debunked as technology has improved.[889] On the other hand, the US attributes activities through many avenues, and in no other aspect of strategy or warfare do states rely on a single source of attribution.[890]

By having a policy which states the US is capable of attributing, and then not carrying out that attribution in a timely manner or imposing serious consequences once attribution had occurred, the US was failing to punish effectively. There is a further option available which the US seemed unwilling to countenance, namely the use of indiscriminate force that could render attribution unnecessary.[891] After all, states can choose to practise indiscriminate retaliation or make an example through excessive punishment.[892] However, this was a step the US has so far seemed unwilling to take in response to cyber-attacks.[893] Thus the US confusion over how to best manage attribution formed a significant barrier to the US ability to enact effective deterrence by punishment. Far from creating credibility, the publication of policy on attribution and then not following that policy severely eroded US credibility.

[885] Joseph S. Nye, 2019, 'Deterrence in Cyberspace', *The ASPI Strategist* [blog]

[886] David J. Lonsdale, 2018, 'Warfighting for Cyber Deterrence: A Strategic and Moral Imperative', *Philosophy & Technology,* 31:3, 421, https://doi.org/10.1007/s13347-017-0252-8

[887] Wilner, 'US Cyber Deterrence: Practice Guiding Theory'; Goodman, 'Cyber Deterrence: Tougher in Theory than in Practice?'

[888] Jason Healey, The Implications of Persistent (and permanent) Engagement in Cyberspace, p.4

[889] Will Goodman (2010) Cyber Deterrence: Tougher in Theory than in Practice? Strategic Studies Quarterly, Fall 2010, p. 124, see also Stateless Attribution: Towards International Accountability in Cyberspace p. 11

[890] Herbert Lin, 2016, 'Attribution of Malicious Cyber Incidents: From Soup to Nuts', *Journal of International Affairs,* 70:1, 75.

[891] Will Goodman, 2010, 'Cyber Deterrence: Tougher in Theory than in Practice?', *Strategic Studies Quarterly*, Fall 2010, 102

[892] N. J. Ryan, 2018, 'Five Kinds of Cyber Deterrence', *Philosophy and Technology*, 31, 332

[893] Chen, 'Does Conventional Deterrence Work in the Cyber Domain?'

4.8 Engagement and entanglement for 'deterrent effect'

Given the difficulty the US has experienced in establishing deterrence by denial or punishment, it is perhaps unsurprising the US strategic community sought additions or alternatives to deterrence, and by 2018 entanglement was offered as such an alternative.[894] The concept of entanglement is not a new one in cyberspace. It was outlined by Scott Jasper and Thomas Mahnken in 2012 as a way of explaining how embedded actors behave cooperatively due to their mutual interests.[895] Entanglement was seen as potentially offering a bridge between denial and punishment, as states seek a continuous relationship whereby they are so entwined that it is difficult and costly to extract themselves.[896]

This concept is similar to the classic international relations concept of interdependence and trade as a disincentive for conflict,[897] but despite arguments that cooperative actions by self-interested parties could achieve desired goals[898] entanglement is an avenue that that offers unclear potential for cyberspace. For instance, Nye has argued that while entanglement could alter the cost-benefit analysis of a major state such as China, it would have limited effects on a state such as North Korea, which is weakly linked to the world economy.[899] Despite this, in 2018 the US Cyber Command announced a new strategic approach, of what it termed 'persistent engagement', arguing this was required to enable the US to compete effectively in cyberspace as states were seeking to alter the international balance of power below the threshold of armed conflict.[900] Persistent engagement was an approach created by Michael P. Fischerkeller, beginning from the principle that deterrence is insufficient to create security in cyberspace.[901] Subsequently adopted in the 2018 DoD Cyber Strategy and released consecutively with the US National Cyber Strategy, the basis of persistent engagement is a defined need for the US to 'preserve peace through strength',[902] and thus the US expects to be 'engaging' from a position of superiority. Indeed, this strength is deemed necessary to create what the US military argued were 'deterrent effects'. The US military casts this policy as helping create deterrence by 'defending forward', defined by the DoD in the following way:

[894] Michael P. Fischerkeller, 2018, 'Persistent Engagement and Tacit Bargaining: A Strategic Framework for Norms Development in Cyberspace's Agreed Competition', *Policy File,* Institute for Defense Analyses

[895] Thomas G. Mahnken and Scott Jasper, 2012, *Conflict and Cooperation in the Global Commons: A Comprehensive Approach for International Security,* Georgetown University Press

[896] Aaron F. Brantly, 2020, 'Entanglement in Cyberspace: Minding the Deterrence Gap', *Democracy and Security*, 16:3, 218

[897] N. J. Ryan, 2018, 'Five Kinds of Cyber Deterrence', *Philosophy and Technology*, 31, 337

[898] Jeffrey R. Cooper, A New Framework for Cyber Deterrence, p.118

[899] Joseph S. Nye, 2019, 'Deterrence in Cyberspace', *The ASPI Strategist* [blog]

[900] Command Vision for US Cyber Command: Achieve and Maintain Cyberspace Superiority, 2018, United States Cyber Command

[901] Michael P. Fischerkeller and Richard J. Harknett, 2017, 'Deterrence is Not a Credible Strategy for Cyberspace', *Orbis*, 61:3, 382; see also Michael P. Fischerkeller, November 2018, Persistent Engagement and Tacit Bargaining: A Strategic Framework for Norms Development in Cyberspace's Agreed Competition, Institute for Defense Analyses p.1

[902] 'National Cyber Strategy of the United States of America', September 2018, The White House, US, p.20; see also US Department of Defense Cyber Strategy September 2018, Summary, p.2

> disrupting or halting malicious cyber activity at its source, including activity that falls short of armed conflict by leveraging our focus outward to stop threats before they reach their targets.[903]

Further, the DOD strategy placed an overwhelming emphasis on the need to use all means, not just cyber means, to respond to cyber-attacks – and be prepared for deterrence to fail:

> The US seeks to use all instruments of national power to deter adversaries from conducting malicious cyber-attacks that would threaten US national interests, our allies or our partners. Should deterrence fail, the Joint Force stands ready to employ the full range of military capabilities in response.[904]

This new policy approach for cyberspace of defending forward, or 'stopping the threats before they reach their targets', echoes the contested and problematic Cold War policy of pre-emptive strikes.[905] Defining such activities as being intended for deterrent effect requires an adversary to understand that such strikes are not intended to be offensive or acts of war – something the US has not achieved. After all, deterrence only works if the other side is interpreting events in the way they were designed.[906] It would seem there is serious potential that what the US government considered as an outwardly-focused strategy to enact deterrence, other states could argue is an act of war (or at least serious provocation). Adversaries could perceive activities aimed at disrupting activity at the source – that is, within another nation's networks – as problematic and risks escalation.[907] Given this risk of escalation, arguments for a warfighting approach, as described by David J. Lonsdale[908] are problematic. Indeed, the US government has publicly indicated it is already engaged in continuous competition with adversaries that were pursuing ongoing capability improvement. According to the 2018 US Cyber Strategy:

> The Administration recognises that the United States is engaged in a continuous competition against strategic adversaries, rogue states, and terrorists and criminal networks. Russia, China, Iran and North Korea all use cyberspace as a means to challenge the United States, allies and partners, often with a recklessness they would never consider in other domains… These adversaries are continually developing new and more effective cyber weapons.[909]

Hence official US policy calls for ongoing engagement of adversaries in cyberspace, despite acknowledging that such engagement was resulting in improved adversary capabilities. Perhaps

[903] US Department of Defense Cyber Strategy 2018, Summary, p.2
[904] Ibid, p.4
[905] Ibid
[906] Richard A. Clarke and Robert K. Knake, 2010, *Cyber War: The Next Threat to National Security and What To Do About It,* New York: HarperCollins, p.62
[907] Joseph S. Nye, 2019, 'Deterrence in Cyberspace', *The ASPI Strategist* [blog]; see also Martin Libicki, 2016, Cyberspace in Peace and War, p.225; Jeffrey R. Cooper, A New Framework for Cyber Deterrence
[908] David J. Lonsdale, 2018, 'Warfighting for Cyber Deterrence: A Strategic and Moral Imperative', *Philosophy & Technology,* 31:3, 409, https://doi.org/10.1007/s13347-017-0252-8
[909] 'National Cyber Strategy of the United States of America', September 2018, The White House, US, pp.2-3

unsurprisingly, the US response to this risk has been the ongoing reliance on the ability to build and maintain capability superiority.

4.9 Superiority

The US decision to pursue deterrence by virtue of building and maintaining superior capabilities in cyberspace, both for defence and offense, has remained remarkably consistent throughout the period; the deterrent effect of brandishing cyber capabilities is a mainstream view in Washington.[910] As outlined in Chapter 1, capabilities are certainly an agreed requirement for deterrence. But the US reliance on capabilities quickly evolved into a drive for cyber superiority as a means of building a credible reputation,[911] and the pursuit of cyber superiority as a critical requirement for deterrence developed into an end in itself. This US reliance on capabilities is not unique to cyberspace, widely acknowledged as being the most offensively capable state in the realm of cyberwar.[912] In fact most US policy documents, including strategies and government statements, take the quest for cyber superiority as an increasing and largely unchallenged goal of broader US security strategy.[913] The 2015 National Security Strategy expressed this as part of its central aim: 'It [the Strategy] aims to advance our interests and values with initiative and from a position of strength.'[914] The 2018 National Cyber Strategy categorised this approach as the need to: 'Preserve Peace through Strength'.[915] The strategy operationalised this concept as the need to 'Identify, counter, disrupt, degrade, and deter behaviour in cyberspace that is destabilising and contrary to national interests, while preserving US overmatch in and through cyberspace.'[916] But the concept of overmatch is complicated by the dual nature of cyberspace, as noted previously in this chapter, where the problem of civilian ownership and management makes the US military superiority (or indeed overmatch) an impossible goal. This view was reiterated in the 2018 DoD Cyber Strategy, which noted:

> The Department must take action in cyberspace during day-to-day competition to preserve US military advantages and to defend US interests… We must ensure the US military's ability to fight and win wars in any domain, including cyberspace. This is a foundational requirement for US national security and a key to ensuring that we deter aggression, including cyber-attacks that constitute a use of force, against the US, our allies and our partners.[917]

[910] Jason Healey, 2019, 'The Cartwright Conjecture: The Deterrent Value and Escalatory Risk of Fearsome Cyber Capabilities', in *Bytes, Bombs, and Spies*, ed. Herbert Lin and Amy Zegart, Brookings Institution Press, p.173

[911] Brandon Valeriano and Ryan Maness, 'Persistent Enemies and Cyber', in Derek S. Reveron, *Cyberspace and National Security: Threats, Opportunities and Power in a Virtual World*, p.145

[912] Ibid

[913] 'Department of Defense: Cyber Strategy 2018', September 2018, United States Department of Defense, pp.1-2

[914] Barack Obama, February 2015, 'National Security Strategy', White House, US, p.29

[915] 'National Cyber Strategy of the United States of America', September 2018, The White House, US, p.20

[916] Ibid

[917] 'Department of Defense: Cyber Strategy 2018', September 2018, United States Department of Defense, pp.1-2

The belief in superiority as necessary to deterrence theory is therefore deeply embedded in US military thinking[918] and thus 'escalation dominance' is treated as a critical component of cyber deterrence.[919] Escalation dominance is based on Herman Kahn's conception of the ability of a state to maintain a markedly superior position over a rival, which will then always see further escalation as a losing bet.[920] Yet as with overmatch or superiority, the notion of escalation and what that would look like in cyberspace is still not clear. And it is made more difficult to ascertain given that the US has repeatedly shown itself unwilling to respond to cyber-attacks with non-cyber responses. Of course, this has not prevented authors such as Osawa arguing that as the number of state-sponsored cyber-attacks grows, stronger measures than cybersecurity or passive cyber defence will need to be taken to prevent the calamities of severe cyber-attack.[921] Far from deterring attacks then the US pursuit of cyber superiority may in fact be increasing risk in cyberspace. And despite the acknowledged issues with a drive for superiority, the US military views such an attempt as necessary for US strategy. This is demonstrated by the 2018 Cyber Command strategy which lists the purpose of Cyber Command as:

> to achieve and maintain superiority in cyberspace as we direct, synchronise, and coordinate cyberspace planning and operations to defend and advance national interests in collaboration with domestic and foreign partners.[922]

In spite of these efforts, far from being deterred by US capabilities, the four identified public adversaries of the US in cyberspace (Russia, Iran, North Korea and China) all made significant strides in their capabilities over the period 2008–18 and continued to use these capabilities against the US. For example, the US decision to create Cyber Command is attributed as a key driver behind the Chinese decision to deploy cyber units within the PLA. Klimburg argues that as friendly and less friendly nations have rushed to compete in an escalating cyber arms race, the US had contributed towards accelerating it even before it turned to persistent engagement.[923] This is a direct counterpoint to Kahn's thesis, in that a more aggressive cyber landscape has resulted from foreign perceptions of US strength, not weakness.[924] Similarly, both Russia and North Korea have continued cyber-attacks despite US strength in capabilities. US indictments from the Sony attacks in 2018 indicate that that North Korea not only conducted cyber-attacks on the entertainment industry but also had deployed malicious cryptocurrency applications,

[918] Gartzke, 2013, The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth, *International Security,* 38:2, p.44

[919] Will Goodman, 2010, 'Cyber Deterrence: Tougher in Theory than in Practice?', *Strategic Studies Quarterly*, Fall 2010, 127

[920] Michael Fitzsimmons, 2017, 'The False Allure of Escalation Dominance', War on the Rocks,

[921] Jun Osawa, 2017, 'The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?', *Asia-Pacific Review*, 24:2, 124; see also Christian Leuprecht, Joseph Szeman and David B. Skillicorn, 2019, 'The Damoclean sword of offensive cyber: Policy uncertainty and collective insecurity', *Contemporary Security Policy*, 40:3, 382

[922] Gen. Paul M. Nakasone, April 2018, 'Command Vision for US Cyber Command: Achieve and Maintain Cyberspace Superiority', United States Cyber Command, p.2

[923] Alexander Klimburg, 2020, 'Mixed Signals: A Flawed Approach to Cyber Deterrence', *Survival*, 62:1, 114

[924] Ibid

multiple spear-phishing campaigns, and significant cyber enabled thefts.[925] And Russia has similarly been accused of conducting multiple cyber-attacks against the US: in 2017 Russian intelligence officers orchestrated a massive cyber-attack[926] that caused billions of dollars in damages.[927] Hence the emphasis on capabilities does not appear to have deterred attacks. It is also worth noting that such attacks are only public examples and that it is likely there have been many more attacks which have not been made public.

4.10 Norms

If the US drive for superiority and overmatch is not creating deterrence, but rather driving potential escalation, then any US attempt at creating norms is likely to fail. Indeed, US attempts to create stability and limitations on state-directed cyber-attacks through support for international norms are continually undercut by its own actions. One of the most significant barriers to US credibility in cyberspace is therefore its contradictory behaviour. After all, given the world has relatively limited experience with cyber, anything the US does is likely to set precedents.[928] And throughout the period examined, the US has consistently advocated for participation in international agreements that supported the rule of law and open and transparent networks such as the 2011 International Engagement Strategy for Cyberspace which called for 'prosperity, security, and openness in a networked world'.[929] The foreword to the strategy by President Barack Obama stated:

> The digital world is no longer a lawless frontier, nor the province of a small elite. It is a place where the norms of responsible, just and peaceful conduct among states and peoples have begun to take hold.'[930]

But despite such sentiments, at the time the strategy was released the Obama administration had already approved not only the development of the Olympic Games suite of offensive cyber capabilities, but had approved their use on Iran's national infrastructure in the attack that became known as Stuxnet. Brandon Valeriano and Ryan Maness point to this decision as an example of the US opening a 'Pandora's Box of cyber risks' because the US went beyond the established taboos of cyber rivalry at that point.[931] This research considers the case of Stuxnet in more detail in Chapter 5, however it is worth considering here as an example of contradictory US behaviour in cyberspace. Far from encouraging a norm of non-intervention, the US had set a new precedent for interfering in another nation's critical infrastructure.

[925] 'Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe', 17 February 2021, https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and.

[926] Joe Walsh, 'Here Are Some Of The Major Hacks The U.S. Blamed On Russia In The Last Year', Forbes, accessed 24 June 2021, https://www.forbes.com/sites/joewalsh/2021/06/01/here-are-some-of-the-major-hacks-the-us-blamed-on-russia-in-the-last-year/.

[927] Landler and Shane, 'U.S. Condemns Russia for Cyberattack, Showing Split in Stance on Putin'.

[928] Robert Jervis, 2016, 'Some Thoughts on Deterrence in the Cyber Era', *Journal of Information Warfare*, 15:2, 73

[929] Barack Obama, 2011, 'International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World', The White House, US

[930] Ibid

[931] Brandon Valeriano and Ryan Maness, 'Persistent Enemies and Cyber', p.155

There is a critical, and very public, disconnect in logic evident in the declared US goal in strategic policy as 'inducing adversary restraint through based on demonstrated capabilities'.[932] This disconnect made credibility an increasingly difficult goal. The 2018 US Strategy for Cyberspace again made a strong case for norms and their importance for stability:

> Encourage universal adherence to cyber norms: International law and voluntary non-binding norms of responsible state behaviour in cyberspace provide stabilizing, security-enhancing standards that define acceptable behaviour to all states and promote greater predictability and stability in cyberspace. The United States will encourage other nations to publicly affirm these principles and views through enhanced engagement in multilateral forums.[933]

Yet the same strategy announced the US intent to pursue persistent engagement, a strategy which by definition involves engaging with adversaries in its networks.[934] Persistent engagement was an attempt to move US policy practice forward, developed to account for the perceived failure of Cold War style deterrence.[935] But not only is this establishing a norm of engagement, rather than a norm of non-action more suited to establishing deterrence, it also further damages credibility due to the US expectation it can behave in ways other states may not tolerate in cyberspace.[936] Norms are certainly not perfect as compliance mechanisms, but they are an important component of international behavioural constraints.[937] By seeking to establish rules and norms that do not unduly inhibit its behaviour, the US is instead creating a new norm of activity within another states' network.[938] Martin Libicki makes the case that an important purpose of deterrence policy is not only to ward off further cyber-attacks but also to maintain a reputation for not being openly trifled with.[939] In setting such a reputational norm the US is encouraging other states to pursue offensive activity in cyberspace, a conundrum the US military neither recognises nor offers options for mitigations.[940]

This case study has so far outlined how expectations of deterrence created through Cold War experiences created an unrealistic view for US policymakers of how deterrence could, and indeed should, operate in cyberspace. Unrealistic expectations of success as a zero-sum proposition and a lack of clarity regarding deterrence goals and policies resulted in a perception, particularly in the military, that deterrence had failed – and thus new or additional theory was needed. The US case study has so far found evidence to support Richard Andres' contention that the fact deterrence was not working in cyberspace was not due

[932] Richard A. Clarke and Robert K. Knake, 2010, *Cyber War: The Next Threat to National Security and What To Do About It,* New York: HarperCollins, p.46
[933] 'National Cyber Strategy of the United States of America', September 2018, The White House, US, p.20
[934] Fischerkeller, 'Persistent Engagement and Tacit Bargaining: A Strategic Framework for Norms Development in Cyberspace's Agreed Competition', p.1
[935] Ibid
[936] Stevens, 'A Cyberwar of Ideas? Deterrence and Norms in Cyberspace', p.159
[937] Jeffrey R. Cooper, A New Framework for Cyber Deterrence, p. 1117
[938] Brandon Valeriano and Ryan Maness, Persistent Enemies and Cyber, p.153
[939] Martin C. Libicki, 2016, Cyberspace in Peace and War, Annapolis, p.237
[940] Richard A. Clarke and Robert K. Knake, 2010, *Cyber War: The Next Threat to National Security and What To Do About It,* New York: HarperCollins, p.46

to the failure of the theory, but rather the strategies used to operationalise it,[941] including the continued US failure to prioritise or create effective credibility and communication strategies for cyberspace. This research has also found that the US also fundamentally misunderstood the importance of clear communication regarding its deterrence stance: its adversaries do not understand what interests are off limits from attack or if they do, are comfortable there will be no significant consequences for doing so.[942] Additionally, the pursuit of superiority may be creating new risks. Rivals tend to overreact to threats posed by enemies,[943] and instead of deterring attacks, the US was potentially creating the conditions for potential escalation. The case study now turns to examining whether these preliminary findings were supported by the views of US cyber experts.

4.11 How effective was US deterrence policy? Expert perceptions of success and failure

As discussed in Chapter 2, this research is framed around considering each state's declared policy against a framework constructed of the basic agreed requirements for deterrence. This methodology aimed to generate comparable findings that consider whether states cybersecurity approaches met those basic requirements while considering how different approaches influenced operationalisation before considering whether states judged their deterrence efforts a success. The inclusion of first-hand views from experts directly involved in creating, implementing, or assessing US deterrence policies increases the likelihood that the findings generated from this research are accurate, and helps ensure the appropriate strategic context is taken into account. This section of the case study provides an overview of participant expertise and considers their overall views on success, before considering their views on each deterrence requirement in turn. It then considers how the US experience of deterrence during the Cold War led to an overwhelming emphasis on capability at the expense of other deterrence requirements, before considering the expert participant's views on this impact this had on US deterrence. Table 4.1 provides a brief summary of each of the US participant's background for context.

As noted in Chapter 2, the interviews were structured to determine whether US policy aligned or differed from the classic conception of deterrence requirements of capability, credibility and communication.[195] The questions generated data on each individual requirement and the perceived success of deterrence as a whole. The interviews also allowed participants significant scope to provide additional information, and used the snowball technique to probe further, particularly where the data appeared to contradict the policy, literature or both. The participants for this study were recruited from academia, think tanks, government, and former government backgrounds. But as with the Israeli case categorising each participant on the basis of their employment proved complex as they all crossed at least two of these categories, and most crossed three.

[941] Richard Andres, 2017, 'Cyber Gray Space Deterrence', *PRISM,* 7:2, 91
[942] Will Goodman, 2010, 'Cyber Deterrence: Tougher in Theory than in Practice?', *Strategic Studies Quarterly*, Fall 2010, 128
[943] Brandon Valeriano and Ryan Maness, 'Persistent Enemies and Cyber', p.156

Table 4.1 US participant expertise and perceptions of deterrence[944]

Participant	Capability	Credibility	Communication	Overall
U1: Senior US cyber strategist; former government strategist, former defence	Equivocal	No	No	No, further theory is required
U2: Senior cyber researcher, former US government cyber expert	Equivocal	No	No	No – failure of implementation, not theory
U3: Former senior State Department cyber expert	Yes, with caveats around the resulting risk of escalation	No	No	No
U4: Senior cyber researcher and strategist	Yes	Equivocal	No	No
U5: Senior former government adviser on nuclear and cyber, senior strategist	Yes	No	No	
U6: Former senior government public servant, senior researcher	Equivocal	No	No	No
U7: Government adviser on cyber, former researcher	Equivocal	Equivocal	No	No, better theory is required
U8: Senior cyber researcher, former official government cyber researcher	No	No	No	No

[944] Eight participants were interviewed: one declined to be recorded, but allowed significant notetaking.

4.12 Defining deterrence success: The problem with vague definitions

As Table 4.1 shows, the participants reflected diverse backgrounds including senior policy making roles, strategists, academics and former military members. Despite this, participants held surprisingly cohesive views on the overall ineffectiveness of measures adopted for the purpose of creating deterrence in cyberspace from 2008 to 2018. Even where participants offered evidence that individual measures were viewed as successful or at least equivocal, they also offered either substantial caveats or evidence to the contrary. These views support the argument presented thus far that the US did not have an effective deterrence approach against cyber-attacks between 2008 and 2018. This section of the case study examines the reasons for the widely differing views on what deterrence is, whether it could (or even should) be applied to cyberspace, and the role of deterrence theory in supporting cybersecurity outcomes. The participants considered that the main reason for the lack of a cohesive US approach was the poor understanding by senior US policymakers of the cyber problem space as well as the potential of deterrence theory as a solution. Participants expressed consistent frustration with differing and often low levels of understanding of the concept of deterrence in cyberspace from political leaders despite its centrality to declared security policy. Participant U8, a former cyber researcher for the US government, stated: 'I get really frustrated when I see senior people talk about deterrence. They don't even know what they're talking about. It's really, really confusing.'[945] Participant U3, a former senior State Department cyber expert pointed out this may be due to leaders not being able to conceptualise the threat as being serious enough to warrant understanding; 'Part of it is leaders just don't intrinsically get this issue. Like no-one died.'[946] And Participant U4, a respected US strategist and cyber researcher argued that the variation in understanding among security and policy experts meant those discussing the basic components of deterrence often misunderstood fundamental terms:

> To me it was a sort of analytical sloppiness in the adoption of cyber deterrence because what most people were not talking about what was the use of cyber means to deter, they were talking about using prospective threats to deter cyber-attacks. Ultimately cyber deterrence was actually covering two things. It was covering the use of deterrence, prospective threat, to deter cyber-attacks, as well as people trying to think about how cyber means could be of such a nature that they would impose significant costs on an adversary so that cyber means could deter. There was some messiness right from the outset in the way it was used.[947]

This lack of fundamental cyber knowledge was noted by participants as operating at all levels of US strategic thinking, particularly in the military. Participant U4 also noted:

[945] Participant U8, Quote 4, p. 1

[946] Participant U3, Quote 5, p.2

[947] Participant U4, Quote 14, p.3

> I really do believe that deterrence had achieved a paradigmatic level in strategic thinking, to the point where the definition of security became interchangeable with deterrence. Deterrence was in fact *ipso facto* the way you secure.[948]

Thus from the outset it seemed that the US approach was viewed as carrying significant risk. Participant U5, a former senior government advisor on cyber and nuclear matters, argued these differing definitions of terms carried a risk of instability:

> In a world in which everybody says there's a distinction between cyber war and real war that's stable. And in a world where people think no, some cyber wars, we can define them like real wars, that's stable. What's unstable? When you have a difference of opinion on what war is. You have instability in cyberspace just like you have instability right across the escalation spectrum.[949]

This suggests that even at the highest levels of strategic thinking, those charged with leading US deterrence efforts for cyberspace were unclear on the most basic concepts and terminology. Participants viewed this vagueness as introducing significant risk into US strategy. Participants also noted the strong and problematic influence of the Cold War mindset on how decision makers conceptualisation of deterrence. Participant U5 summarised this influence:

> We have a huge community of people who cut their teeth on nuclear and then went to cyber. And the dishonest ones say it's just like nuclear and the honest ones say the differences are just too many.[950]

The influence of the nuclear era was clearly visible in the views of Participant U4, who argued deterrence was simply not applicable in cyberspace. He argued the nature of cyberspace meant that it was impossible to achieve his definition of successful deterrence, which he viewed as zero activity:

> the measure of effectiveness of deterrence is the absence of action, specifically the absence of unwanted action… You can't apply a strategy whose measure of effectiveness is the absence of action, in an environment of persistent action. It logically doesn't hold.[951]

Participant U2, a former government cyber expert, stressed that such views from the Cold War were not just inaccurate – indeed, they were potentially costing the US on many levels:

> you still have in the military, special forces folks who say oh you know, cyber is just SIGINT by another name, and again, they're all missing that this is the most transformative thing that's come from human minds in the last 500 years.[952]

A further reason identified by participants as complicating the US approach was the consideration that the level at which participants themselves conceptualised deterrence – whether as a theory, a strategy or a

[948] Participant U4, Quote 1, p.1
[949] Participant U5, Quote 45 p. 11
[950] Participant U5, Quote 58, p.13
[951] Participant U4, Quote 29 p. 6
[952] Participant U2, Quote 59, p. 11

tactic – also influenced conceptions of whether deterrence measures could be described as being successful. Participant U1, a senior cyber strategist and former cyber adviser argued:

> if you are deterring an attack in cyberspace, but an attack is still occurring in other areas, that's not deterrence because you aren't deterring action overall – you are changing the tactics, not the strategy.[953]

Participant U7, a government adviser on cybersecurity, argued the US had struggled with applying the concept of deterrence to cyberspace:

> At least within the US system there has been an effort to grapple with the sort of failure of deterrence as a concept as they understand it. But maybe this is a false start or like a misplaced construct.[954]

The failure to understand and translate these differing understandings into a common understanding of the nature and goals of deterrence in cyberspace at the conceptual level may help explain why deterrence measures were perceived as unsuccessful. Without clear goals and conceptual certainty, success could not be possible. This US failure at the conceptual level to build a clearly defined approach to the requirements of deterrence for cyberspace carried risk and the perceived failure of deterrence was seen as potentially leading the US down a path of escalation. I argue, based on these participant interviews, this approach creates risk. Consider the following view from Participant U7:

> Essentially persistent engagement was borne out of a sort of academic effort to reconcile the fact that deterrence in the nuclear concept doesn't work. Where they have to go with that, which is basically you have to take the fight to the bad guy, I think is probably flawed as well.[955]

So did the participants consider that the US approach met the basic requirements of deterrence? We begin by considering each requirement in turn.

4.13 Perceptions of US capability: Superiority as 'deterrence'

In considering the US approach to developing and using capabilities for deterrence, including how the definition of capability shifted between 2008 and 2018, interviewees presented a broad range of views. Although capability is the one area of deterrence for cyberspace where the participants considered the US came close to meeting the requirement, participants were divided in three main aspects: how capability should be defined and used in order to achieve deterrence; whether the US had sufficient capability; and whether US capabilities had actually deterred cyber-attacks. The divisions in the views of how capability should be defined and used as part of deterrence reflect the conceptual and definitional issues previously noted in this case study. Participants characterised capabilities in a variety of ways, including technical capabilities and offensive use of cyber measures, as well as viewing capabilities in terms of their own

[953] Participant U1, Quote 17, p.2
[954] Participant U7, Quote 6, p.2
[955] Participant U7, Quote 5, p.2

abilities and those of their adversaries. For example, Participant U4 defined capabilities as cyber abilities that would allow the US to dominate activities confined within cyberspace:

> I think it's better to say who has the initiative here? The first state had the initiative by being able to exploit the vulnerability to get inside my network. But because of the capabilities that I've developed, and the operational skill and everything else I bring to bear, I was able to regain, secede that initiative away from you, and in fact regain the initiative by kicking you out and advancing my defence at a higher level.[956]

And Participant U6, a former senior government cyber public servant, also viewed capabilities as referring to US technical capabilities. He argued that there was a continuing need to build superior capabilities to maintain deterrence due to the speed with which technology advances:

> The technology continues to advance, not just with 5G... So I think for our national security interests, we need to be pedal to the metal on the technology side. We need to devote a lot of resources and frankly, more than we are so far to resilience, including the defense, but also through attacking and other measure and through complexity.[957]

In contrast to these views of capability as being based in cyberspace, Participant U5 argued deterrence depended on a far broader view of capabilities. He noted that the US 'can deliver a devastating response well before we get to the nuclear level.'[958] Participant U3 agreed, stating:

> You need to think about what your response options are. They're not just going to be cyber, they're going to be economic, they're going to be diplomatic, there's a range you can use, and you need a way to figure out what's going to be the most effective and you need to figure out how good the equities are.[959]

These variations tended to frame participants' views on whether these capabilities had positive effects on deterrence. Regardless of how they defined capability however, participants agreed more capabilities were required, despite the government not understanding how such capabilities could, or even should, be used. Participant U3 identified the lack of understanding of cyber capabilities at the highest levels of government as a serious issue which could potentially lead to escalation:

> Back when we were first looking at the Russian interference [in the 2016 election] I did have a very senior state department person who was not involved in cyber at all, we had this conversation and she said, well why don't we just turn off the lights in Moscow? First of all no, and secondly no, and thirdly it's probably a violation of international law, and fourth no![960]

[956] Participant U4, Quote 48, p.11

[957] Participant U6, Quote 36, p. 10

[958] Participant U5, Quote 26 p.6

[959] Participant U3, Quote 12, p.3

[960] Participant U3, Quote 45, p.9

Participant U8 agreed that the low level of understanding within the US government was problematic, as it meant the way capabilities were used for deterrence ends was often not well-planned or effective:

> We're not in instituted theory here. We don't even have a basic conception of what the threat matrix is, what the probability of attacks are, early warning indicators, what the impact of disinformation campaigns are. All these basic questions need to be answered. There is no one in government that has any of these answers.[961]

Participant U2 considered that the US has an over-reliance on capability produced an approach that was too narrow, and potentially ineffectual:

> And for just way too many people in this business, I mean three-quarters of people in this business, it just means having more offense. You know, offensive capability and the threat, the willingness to use it.[962]

Participant U2 then used the example of Iran to illustrate that US use of capability had not proved an effective deterrent in other states seeking to gain similar capabilities:

> Look at Iran. It's clear that we punched first….so all these arguments that we've got this capability, we've got this will, they're not going to challenge us, and twice – we've seen two different waves of folks saying oh my god, look at how fast Iran developed this capability.[963]

Participants further noted that the drive for superiority for deterrence ends without establishing what capability superiority meant, how such superiority should be used, or what effects it might have global norms could already be resulting in unintended escalation. Participant U6 pointed out that what the military defines as superiority may not align with broader strategic definitions of superiority:

> You have to understand how narrow the definition of superiority is in US military doctrine. Superiority means gaining local, temporary advantage essential to support military operations.[964]

Despite agreeing the US should probably pursue improved cyber capabilities, participants identified potential risks in the drive for pursuing superior capabilities, including repeated concerns about escalation. Participant U2 argued that building and using capabilities simply encourages other states to do the same, and that deterrence in US policy has been too focused on superiority:

> If you build great capabilities around yourself that others don't understand what you intend to do with those and so even if you only meant them to be defensive they feel threatened, so they build more fearsome capabilities on their end.[965]

[961] Participant U8, Quote 36, p.8
[962] Participant U2, Quote 4, p.1
[963] Participant U2, Quote 32, p. 5
[964] Participant U6, Quote 21, p.6
[965] Participant U2, Quote 16, p.3

And despite the emphasis on building and maintaining superior capabilities, the US approach to deterrence was degraded by US unwillingness to use those capabilities. Participant U7 pointed out the disconnect between the rhetoric on US abilities and their actual responses:

> The fact that Cybercom launched a campaign to constrain the Russian influence during the 2018 mid-term elections… Many people who you speak to who have the inside knowledge of it will tell you it was more sort of theatre than actual impact and that the cost of doing it was probably disproportionate to the effect that was achieved. But at least in terms of the willingness of the US to take action against Russia specifically that is actually probably an outlier in terms of how the rest of the administration has responded to threat actors and particularly Russia.[966]

Some participants argued the confused US approach to the use of capabilities in response to cyber-attacks may also reflect the fact that the US has been trying to deter types of activity in cyberspace that it has not previously had to deal with as part of deterrence. Participant U4 considered that:

> What's happening in my mind is that states that want to challenge that distribution of power are now starting to leverage campaigns – not attacks, not simple espionage or shifts of intellectual property but coordinated campaigns to challenge those sources of power.[967]

Participant U2 also argued the continued use of capabilities was not required for deterrence, pointing to senior government strategists' views that there were examples of states being deterred through the implied use of force:

> I think Fischerkeller and some of the others are just wrong when they say you have to show capability. Clapper sat in that chair and I said did it happen this way – Yes. I'm phrasing this as deterrence, do you think that's accurate – yes. Done, right.[968]

In contrast to that view, Participant U6 argued that non-responses were risky. He argued there was a need to continue to use capabilities despite the risks of norm-setting:

> I believe that we need to be active in the steps that we take to defend our networks, including when that involves, there are a bunch of euphemisms, right? Let me just be explicit. Including where it involves offensive action to take down someone else's capabilities.[969]

And yet, while this case study found evidence there was a fear of escalation, Participant U7 argued conflict in cyberspace could also act as a release valve:

> Although it sounds like a lot of money and risk and all the rest of it, that if you can contain it all to cyberspace and nobody gets killed, that may be an acceptable price to pay relative to the

[966] Participant U7, Quote 19, p.6
[967] Participant U4 Quote 22, p.5
[968] Participant U2, Quote 9, p.2
[969] Participant U6, Quote 18, p. 6

> resources and risks of at least some of the things that you would need to doing in order to completely squash it.[970]

This view may help explain the US decision to create and use the Olympic Games program suite against Iran as noted earlier in this chapter. Indeed, Fred Kaplan argued the US saw the resulting Stuxnet attack as lower risk than sending in US troops.[971] From this viewpoint the operation could certainly be deemed a success if deterrence was considered a holistic goal.

4.13.1 Do US capabilities deter?

Despite the many caveats listed on capabilities, some participants still saw overall US strength as sufficient to maintain the desired state of deterrence. However those that did so were critically not relying on US cyber capabilities, but rather the broader US strategic strength which they saw as sufficient to deter major cyber-attacks. Participant U7 reflected on this point:

> Imagine that in a year's time we have a different President elected, I think structurally and systematically the US is still in a very strong position to be a global leader in that space. Both in terms of the technical capabilities to understand what's going on and the fact that the US continues to have a, despite everything, still has a good set of relationships with countries around the world that at least suits those countries, they're willing to listen to the US.[972]

But this view – that the US could rely on broader deterrence while continuing to pursue superior cyber capabilities – has also arguably led to increased risk of unintended consequences. Participant U2 was particularly scathing on this point, arguing the drive for capability was flawed. He noted: 'The Cartwright conjecture is really just saying we need capability… and my answer to that is when has that ever worked?'[973] The 'Cartwright Conjecture' is the idea that the US needs both fearsome cyber capabilities and adversaries need to know about those capabilities.

Regardless of the reason for efforts to maintaining superior capabilities, participants noted that such behaviour was likely to result in increasing activity in cyberspace. Participant U5 sounded a note of caution and pointed out that this activity is also creating potentially unwanted norms:

> Something else I don't think gets enough attention to, it's very hard to retaliate against something you yourself are doing… We the US normalise behaviour by going out and doing it. As a general rule you can't make a norm against behaviour you've already normalised. That forms a serious constraint in the world of cyber.[974]

[970] Participant U7, Quote 48, p.12

[971] Fred M. Kaplan, 2016, *Dark Territory: The Secret History of Cyber War,* New York: Simon & Schuster, p.203

[972] Participant U7, Quote 30, p.8. This interview was conducted in November 2019, one year prior to the Presidential elections in 2020.

[973] Participant U2, Quote 14, p.3; this is based on General Cartwright's 2011 statement that 'we've got to talk about our offensive capabilities to make them credible so that people know there's a penalty.' See J Healy, the Cartwright Conjecture.

[974] Participant U5, Quote 22, p.5

On the issue of capability, the expert participants noted the problems caused by unclear definitions, the risks of the drive for capability superiority, and the risks of relying on capabilities alone to deter cyber-attacks. Participants were however in agreement that regardless of the US possessing effective capabilities, deterrence also required the use of such capabilities in a manner that built and maintained credibility – something the US struggled with at every level.

4.14 Perceptions of US credibility: Repeated failure

In considering the views of the participants on the credibility of the US deterrence approach for cyberspace, there was consistent agreement that US credibility was perceived as either being equivocal or insufficient for creating desired deterrence outcomes. Participants agreed on the theory behind credibility: for deterrence measures to be considered credible, they needed to be timely, appropriate to the attacker and consistent.[975] Participants were also consistent in their belief that to be truly credible, the US approach should include a visible element of punishment and that this was an area in which the US had consistently failed. Participant U5 noted:

> Deterrence is only deterrence if there are consequences to not carrying it through… The less credible your threat is, the less face you lose. The less face you lose, the less likely you are to make good on your threat.[976]

Participant U7 observed that while the US had acted to constrain Russian interference within the 2018 elections, such activity was not the norm for the US, and in many other cases threats had not met a similar response. But in order for such punishment to be effective – and thus credible – responses needed to be timely and appropriately tailored. Participant U1 characterised this in this way: for a response to be credible, it must be credible to that particular adversary.[977] Tailoring punishments accurately however requires attribution and, unsurprisingly, participants agreed that attribution was a part of credibility. Participant U5 characterised this as:

> In essence, if I do something, what's the odds I'll get punishment, and then its capability, credibility and communications and then how bad will the punishment be, that's capability… for every type of punishment you can design a different credibility.[978]

Participants also noted the need for responses to be timely in order to build credibility. As Participant U5 argued, 'Retaliation is one of those things the value of which declines sharply after the event.'[979] However participants noted the US commitment to collective attribution – while necessary – was problematic, unless coupled with visible responses. Participant U7, supported the collective approach, but also noted

[975] See Chapter 1: Literature
[976] Participant U5, Quote 15 p.3
[977] Participant U1, Quote 33, p.4
[978] Participant U5, Quote 5, p.2
[979] Participant U5, Quote 47, p.11

action was key: 'Collective attribution is the first step towards collective action but it's suspected that collective action is what makes the difference.'[980] And participants were clear that the barrier to such attributions was not a question of technical capability. Participant U6 argued recent US improvements were significant: 'Actually technical attribution tools have dramatically improved over the last five, even six years.'[981] Participant U8 took the question of attribution a step further, arguing that while the US had undoubtedly improved its technical attribution capabilities, it was in fact a much broader question of strategic understanding which the US could improve at: 'There's strategic context in everything, you know who your enemy is. It's not a mystery.'[982]

4.14.1 Barriers to credibility: Consequences, norms and attribution

Despite the idea and requirements of credibility being understood and agreed to, the participants were adamant the US had failed to establish credibility, largely because it failed to punish attacks effectively. Participant U3 argued that the lack of visible responses was a clear failure of deterrence, and described this as a problem of visibility:

> We need to be able to do more visible things where we're explicitly going after things they did…We have been so ineffective at actually causing pain for the adversary that for them, interference is still a cost free enterprise.[983]

Participant U6 gave the following example:

> What's clear is that for Russian interference in the US elections, the costs that have been imposed to date, or the costs that are expected are not sufficient to deter Russia from this type of intervention.[984]

Participant U3 attributed this lack of response to cyber-attacks was a failure of political will, and saw the failure to impose consequences as proof that the US had not managed to implement an actual deterrence approach:

> And being willing to impose the consequences, having the political will to do it, but also doing it effectively… We haven't really tried it. We haven't actually imposed consequences on these actors that are the kind that will actually change. We've done some sanctions to be sure, but have they been persistent and targeted? No.[985]

Yet if the need for swift, visible responses was agreed, why was the US not carrying out such responses? Participant U8 agreed it was the lack of political will that resulted in the lack of credibility.

[980] Participant U7, Quote 25, p.7
[981] Participant U6, Quote 31, p. 9
[982] Participant U8, Quote 48, 11
[983] Participant U3, Quote 44, p.9
[984] Participant U6, Quote 11, p.3
[985] Participant U3, Quote 28, p.6

> There's really no construction of signalling and of course for deterrence to work, you need credibility, you need signalling. You need crisp resolve. None of these things are actually in operation.[986]

Participant U3, additionally, was adamant that the US had failed to create credible deterrence in cyberspace because it had not imposed consequences:

> You can lock the door but if there's no consequences for breaking through the door then that's not a solution. We have to do better… We haven't been timely. And we haven't been really all that credible because they've been short term, they haven't been that strategic.[987]

Participants also agreed that even when an attack did receive a response and consequences were imposed, these consequences were not serious enough to be perceived as effective. That said, participants were divided over the appropriate threshold for response. Participant U1 noted that although the US had declared thresholds in cyberspace prior to 2015, these did not work – largely because its responses were ambiguous – and as the transgressions were at below the thresholds of armed conflict, any threatened response was not credible.[988] Some participants saw the attempt to establish credibility as complicated by the lack of internationally agreed standards of behaviour in cyberspace, including a lack of agreement regarding attributing responsibility. Participant U3 gave an example of this:

> A good example against North Korea where after the Sony Pictures hack everyone was saying, all the pundits were saying it's North Korea. [President] Obama comes out: it was North Korea, we released more evidence than we normally would, we put stuff out there, but not everything, because we're not going to release everything, and then the pundits were like, well it's not, because looking at the evidence that's not enough.[989]

Participant U5, however, again pointed to credibility being linked to responses, and the bigger issue as being the lack of effective consequences for states attacking the US: 'I believe in norms. But they're not norms because I feel bad. They're norms because if I break them there will be consequences.'[990] The bigger problem with norms for US credibility however was noted by Participant U6 who was adamant that US behaviours were undermining US credibility. Participant U6 also pointed out there were strong arguments that US behaviour in cyberspace could be viewed as escalatory by both allies and adversaries:

> My perspective is if you're American, you want to tell Russia and China and Iran, don't you dare put anything in my infrastructure, we will impose costs on you through cyberspace and elsewhere. One, you better be prepared to back it up, and two, you better not put sh*t in their infrastructure

[986] Participant U8, Quote 2, p.1
[987] Participant U3, Quote 50, p.10
[988] Participant U1, Quote 4 p. 1
[989] Participant U3, Quote 22, p. 5
[990] Participant U5, Quote 3 p.1

> either because even if they determine that they're not going to reply, the US credibility with our allies and partners will be sh*t.[991]

Participant U1 saw the link between public attribution and credibility as critical, noting that if a state attributes an attack and then does not respond, it looks weak.[992]

The issue of timeliness was also repeatedly raised as a problem for US credibility. Participant U3 pointed out this was a particular issue for collective attribution: 'I think the biggest problem has been that joint attribution currently is taking too long... If you're really going to deter anything you need to take action.'[993] He also pointed out that managing a timely response was not an issue limited to the US:

> It took [then British Prime Minister] Theresa May about a week to say it was Russia for the poisonings, and it took her another week to assemble a coalition of countries to take action, and then you contrast this with NotPetya, which took six and a half months to do the attribution, or to make the public attribution and then when it was announced… it's not a very strong deterrent message right[994]

The participants thus agreed that the US had consistently failed to create credibility in its deterrence approach, due to four factors: an unwillingness to punish cyber-attacks; the length of time taken; to attribute attacks as a collective; and the decision by the US to continually pursue cyber behaviours which undermined their public stance on international norms.

4.14.2 US credibility: Consistent failure

The only participant who viewed US credibility as being at least partially successful was Participant U7, who viewed collective attribution as being potentially beneficial – if not in dissuading an attacking country, then in dissuading others from attacking:

> It is not obvious to me that either the Russians or the North Koreans have given up doing bad stuff in cyberspace so it's hard to say that there is sort of a direct impact on those places. But I think it is certainly conceivable that by getting a bunch of countries to say 'We know they did it' you're demonstrating to other marginal actors that they could get called out if they do anything in cyberspace. It is by no means guaranteed that you're going to be able to prevent bad guys doing bad things. But you might help prevent people getting into the game where they think they might be able to do it without consequence.[995]

But Participant U5 argued that while the US may have a credible deterrent, this was probably due to its overall size and influence rather than having an effective cyber deterrence policy: 'We're just bad! In that classic gangster sense. We can do nasty stuff, don't mess with us.'[996] Participant U7 argued the fact the US

[991] Participant U6, Quote 9, p.3
[992] Participant U1, Quote 22, p.3
[993] Participant U3, Quote 21, p. 5
[994] Participant U3, Quote 4, p.1
[995] Participant U7, Quote 24, p.7
[996] Participant U5, Quote 9, p.2

policy for creating deterrence in cyberspace was bipartisan was an indication that it was on the right track. However, he argued that the US had a broader credibility problem:

> The fact that in the cyber part of the house it's effectively business as usual, or potentially more… I think the Obama administration would probably be doing something similar if it was around. Remaining in that same track is an indication that I don't think the US has necessarily lost credibility in the way you might have expected. I suspect the credibility that's being lost on the cyber side is relatively smaller in some ways than the wider credibility that the administration has lost as an ally and a partner and the rest of it.[997]

Based on the indications of successful credibility outlined by participants, these interviews indicate that the US policy approach to date was not perceived as achieving overall credibility. Rather, where credibility was thought to be working, participants attributed success to other factors, largely conventional strength. This lack of success in establishing credibility in cyberspace seems thus to be attributed to be due not to a lack of understanding of what would comprise effective policy but rather the choice to not respond to cyber-attacks with appropriate or timely enough consequences. The US view of punishment as a necessary component of credibility was surprisingly cohesive across participants and yet had not been delivered – there was a perceived failure to punish. But was the US creating credibility through other mechanisms? To examine this, I now turn to looking at the US ability to communicate its deterrence stance.

4.15 Perceptions of US communication: Essential, but inconsistent

Regardless of their backgrounds or views on deterrence overall, participants were unanimous in the importance of communication to a successful deterrence policy in cyberspace. Participant U7 firmly stated: 'Messaging is fundamental to deterrence.'[998] Participant U2 argued that the best strategies are simple, and deterrence strategies should similarly be easy to understand: 'You might have disagreed on how to go about it in any particular situation, but everybody agreed it was one word. Like COIN.[999] The strategy was simple to understand.'[1000] Participant U6 agreed that clear communication was critical for deterrence but noted there were challenges that were difficult for states such as the US to overcome:

> Clarity in language I think is very important, and the reality that we have not only a language barrier but conceptual differences even among ourselves, let alone with the Russians or Chinese in particular. As well as allies, talk to the French about deterrence, the Belgians or the Dutch. So

[997] Participant U7, Quote 18, p.6

[998] Participant U7, Quote 11, p.4

[999] COIN refers to counterinsurgency activities, and while it was a well-known term it does not describe an actual theory. See Colin S. Gray's argument that COIN was unhelpful as it is neither a concept nor a strategy but rather 'an acronymic descriptor of a basket of diverse activities intended to counter an insurgency'. See Colin S. Gray, 2012, 'Concept Failure? COIN, Counterinsurgency, and Strategic Theory', *PRISM,* 3:3, 17–32

[1000] Participant U2, Quote 60, p. 11

> different, there's a real possibility of miscommunication and I think it behoves policy makers to be clear in what they're talking about when that talk about these issues.[1001]

Once again, the lack of clarity from US strategic leadership was judged as having reduced the US ability to achieve its deterrence goals. One example of this was the differing ideas about what comprised effective communication for cyberspace. While participants agreed communication was an important principle, the level of detail required for such communication was not agreed. However, participants seemed to err on the idea of preferring ambiguity.

This was evident in relation to red lines, or explicitly communicated areas which are considered off-limits to attacks. Participant U3 argued that it was important to establish clarity without necessarily stating explicitly what would be a red line for the US in cyberspace: 'You know you don't want exact red lines but you want to be clear and message both your friends and your adversaries, it helps you build these alliances.'[1002] Participant U6 agreed with this view, arguing that: 'The idea of having a very clearly defined bright line – this is war, this is not war – is neither necessary nor sufficient to significantly mitigate escalation risks.'[1003] Participant U5 went further, explaining that having an explicit communication policy was not necessarily helpful for deterrence. He posited that perhaps the whole policy should be kept internal: 'The question on a deterrence policy is what do I gain by being explicit about it? And the answer is maybe not so much.'[1004] These standards seem to indicate that the US preference was for flexibility in what it considered a red line. Some level of ambiguity is certainly understandable, but if a communication approach is too ambiguous it risks being misunderstood.

As such it is perhaps unsurprising that participants overwhelmingly considered that the US had been unsuccessful in communicating its deterrence aims, policies, or consequences for activity contrary to its interests in cyberspace. However, participants identified different reasons for, and drew different lessons from, this inconsistency. One reason offered was the complexity of applying deterrence theory within cyberspace. Participant U1 noted that although the messaging on cyberspace had been inconsistent, formulating effective messaging in a new domain is complex, and pointed to the time it took in the 1950s to create a whole new language for nuclear weapons.[1005] But as Participant U3 argued, despite the complexities, consistency was critical for success and the US had not achieved such consistency:

> The example I give you on that is that when we lifted sanctions on one of Putin's cronies, that doesn't sound the right message, you have to be consistent. You have to be willing to engage in some of these sanctions, even on the economic sanctions, and be stronger. We haven't done that.[1006]

[1001] Participant U6, Quote 10, p.3
[1002] Participant U3, Quote 43, p.9
[1003] Participant U6, Quote 4, p.2
[1004] Participant U5, Quote 7, p.2
[1005] Participant U1, Quote 13, p.2
[1006] Participant U3, Quote 29 p. 6

The lack of understanding of the importance of communication as part of a deterrence effort was attributed by Participant U4 as being as a result of the different levels of understanding of deterrence theory, aims, and policies within the US system:

> You go back to the 2014 Sony attack in the US, you've got the FBI initially calling it cyber-crime, President Obama goes on television and calls it cyber vandalism. To this day I still don't know what this term means. And then you have US senators calling it cyber war. And all of those different terms mean very different things.[1007]

The problem of educating and communicating domestically was also noted as a key flaw in the US approach. Participant U3 argued this lack of understanding was partially due to not being taken seriously enough by the US system:

> It shows the issue of cyber not being a main policy issue that people either think it is trivial, or they don't understand escalatory nature of it, on the other hand they're so guarded about their own things, so we have to have dialogue.[1008]

One of the key problems with the flawed US approach to communication was that because the US could not agree on what the threat space was, communicating clear internal domestic measures about protecting that space was not possible. Participants argued that educating policymakers on the importance of clear communication for deterrence takes time, and is complicated by the confusion over deterrence goals. Participant U1 noted that shifting and aligning the thinking of policymakers was made more difficult by the length of time policymakers had thought about deterrence in a particular way.[1009] Participant U2 also noted an issue with the level of understanding of the key threats posed by attacks in cyberspace:

> Everyone knows they're supposed to be worried about it, I mean most politicians, most CEOs they either worry about it or they're supposed to worry about it and are trying to get their arms around what worried about it means. They're scared of it.[1010]

Participant U8 noted communication was complex for all states because it was not yet clear what effective signalling would like in cyberspace:

> We need a very clear idea of what signalling means in cyberspace. If you don't want someone to do something, you need to be very clear in what they're not supposed to do. That's not true right now.[1011]

[1007] Participant U4, Quote 38, p. 8
[1008] Participant U3, Quote 46 p.9
[1009] Participant U1, Quote 8, p.1
[1010] Participant U2, Quote 58, p. 10
[1011] Participant U8, Quote 35 p.7

Participant U3 argued that the reason that communication had been so piecemeal was because the problem space was not well understood and there was a need to make the narrative around cyber threats more compelling:

> It really is hard because it's the long-term consequences and that's why people default to oh, you take down an electrical power grid and everyone will die, which I just don't think is a useful narrative.[1012]

The confusion regarding terminology and concepts was also identified as a barrier to effective communication by Participant U6:

> That was a really crappy title (in reference to the DoD policy of seeking superiority in cyberspace) because everyone is going to think it means superiority over cyberspace… and it means intruding on civilian infrastructure as a matter of course. Doing whatever you feel like in cyberspace. It's not, and if you were to talk to Paul Nakasone (the current head of US Cyber Command) that's not his view at all… that, what I regard as a strategic communication error, it amplifies the general view that the United States is a bull in a china closet.[1013]

Participant U4 pointed out that in part this confusion is due to the US not having an aligned domestic system:

> We haven't gone through the full paradigm shift in the United States, our allies, it depends on [who] you talk to right? There are people in the State Department who are pushing the cyber deterrence initiative, I still don't know what the hell that really is![1014]

It is true that the communicating deterrent intent is complex in any environment, but as Participant U5 argued, confusion over terminology can have serious consequences, particularly in creating a cohesive approach between policymakers and cyber professionals:

> If somebody discovers the government isn't ahead on the story it becomes a cover up. And for the government to say well we didn't talk about it because we didn't think it was very important, that doesn't work either. There's a tendency for people who should know better to say oh my god, oh my god. So the very term cyber-attack, as you recognise, conflates attack and espionage. There is a huge rift between what is commonly accepted to be true and what the professionals believe is true.[1015]

One of the biggest risks caused by ineffective US attempts at communication is that the US is having to focus its efforts internally at educating its own citizens, rather than externally at deterring cyber-attacks. Participant U6 agreed this was a serious issue for the US, and argued that it highlights why the US government is investigating options for improving communication within its own agencies:

[1012] Participant U3, Quote 48, p.8

[1013] Participant U6, Quote 21, p.7

[1014] Participant U4, Quote 36, p.8

[1015] Participant U5, Quote 35, p.8

> One of the projects I'm writing now is arguing for a national cyber center that would bring together all of the relevant departments and agencies, so the authorities to operate would be in one building.[1016]

But Participant U7 notes such internal alignment is unlikely to happen due to the size of the US administration: 'The US government is too big to be shepherded into a single national cyber type of security center and so that may be a false chimera.'[1017]

Participants identified two key risks arising from the US failure to clearly communicate its deterrence policies for cyberspace: first, that the US risked being misunderstood by partners and allies; and second, that there was a risk of policies being misunderstood by adversaries. Participant U1 observed that the thresholds for unacceptable behaviour in cyberspace declared by President Obama did not work because no adversary could understand what the thresholds were.[1018] In contrast, Participant U3 argued that the thresholds were initially effective but this lapsed in due to a different policy emphasis under President Trump:

> When we did the China deal, it wasn't just me saying this, it was Obama, Rice, Gates, I mean everyone was communicating on the same page. Again and again and again. Obama kept raising it, it was part of the overall fabric. And it has to be part of the overall fabric. It can't be just cyber. Now politics aside, when you have (President) Trump saying, second guessing whether Russia actually did things, no matter what else the government is doing, that substantially undercuts the message. You need consistent messaging from the top.[1019]

Participant U1 noted US adversaries were increasingly confused about US policy and referred to the example of attending a diplomatic dialogue in China, where interlocutors were confused over the policy differences between the DoD, Cyber Command, the White House and the State Department.[1020] Participant U6 contended that the uncertainties regarding communication were also an issue for America's allies, particularly where it seemed that the US did not have a cohesive policy approach:

> I am told by some of our European allies and partners that there have been multiple cases where they've met with people from State [the State department] and then people from DHS and people from either Cyber Command or NSA separately and have the sense that they're two to three completely separate policies. Mutually exclusive approaches that the United States is advocating. This is not the optimal way to operate as a major power.[1021]

The internal divisions within the US policy approach were also identified as a potential risk for the development of stable international norms for cyberspace. Participant U8 noted, 'In America, the state department is not locked into the Department of Defense. That's a problem, because the state

[1016] Participant U6, Quote 43, p. 12
[1017] Participant U7, Quote 13, p.4
[1018] Participant U1, Quote 5, p.1
[1019] Participant U3, Quote 55, p.10
[1020] Participant U1, Quote 14, p.2
[1021] Participant U6, Quote 47, p.13

department is not in charge of the UNGGE[1022] process.'[1023] And beyond adversaries, even US allies struggled to understand US intent. Participant U6 further identified that the lack of clear communication could create risks more serious than merely being misunderstood. He argued this could potentially result in unintended escalation:

> If I saw you undertaking actions in cyberspace that looked to me preparatory, the most important steps you'd want to take if you were planning an armed invasion of a US ally, then that could have a significant impact on my expectations and my sense of what is an appropriate course of action.[1024]

Given the participants' views that the US communication around deterrence was inconsistent and incomplete, it is not surprising that expert views of the communication regarding the pivot to persistent engagement has proved similarly problematic. Participant U8 identified this risk as occurring because success was not clearly defined:

> I would say the biggest problem with persistent engagement is there's no sense there. There's no theory of effect. There's no theory of when you know it's working and when you know it's not working. To me that's not necessarily suitable for any sort of strategic theory.[1025]

He also observed that a key issue was the lack of understanding of what effects attacks had, and thus what message may be being communicated, either on purpose or by accident:

> We don't have a clear vision of metrics, of battle damage assessment. Really, everything we're doing right now is just a shot in the dark. That's very concerning to me as a strategic planner and a strategist.[1026]

Participants also agreed that there was a risk of conflict in cyberspace escalating due to poor or incomplete communication strategies. Participant U3 argued that clear communication was an essential requirement for de-escalation, and it should be conducted through multiple channels:

> We have to be willing to take some risks and people were worried about escalation, I get that, I agree with that, however there's a way to control escalation and one of them is to have direct dialogue with the adversary, political channels, military channels.[1027]

But the shift to persistent engagement requires a substantially different approach if it is to have the intended deterrent effect. As Participant U7 argued, communication was a critical part of any de-

[1022] The United Nations Group of Government Experts (GGE) on Advancing responsible State behaviour in cyberspace in the context of international security) is a UN-mandated working group in the field of information security. For further information see https://www.un.org/disarmament/group-of-governmental-experts/

[1023] Participant U8, Quote 28, p.6

[1024] Participant U6, Quote 4, p.2

[1025] Participant U8, Quote 20, p.4

[1026] Participant U8, Quote 37, p. 8

[1027] Participant U3, Quote 33 p. 7

escalation efforts. He considered that the importance of such efforts had likely increased due to the policy shift towards persistent engagement:

> Basically if you're monkeying around on sort of engaging with the enemy in other people's systems there is a risk that they don't fully understand what exactly you're up to and that creates all sorts of potential problems.[1028]

The risk of escalation (that adversaries could interpret US activities in cyberspace as inflammatory) was raised by Participant U6 as a serious issue the US needed to manage: 'There are actions that may clearly fall below the threshold of armed conflict that could be highly escalatory because of how it would cause the other side to interpret.'[1029] But Participant U8 offered a slightly different view, arguing that there was potential for persistent engagement to offer cyberspace as a place for states to compete without kinetic conflict:

> Cyber is a release valve when you can't do things conventionally. That's why [redacted] and I say this is a de-escalatory option. It's another option in the toolbox, like sanctions, where you can express discontent… why would you ever expect you're going to be able to prevent that.[1030]

Nonetheless, Participant U8 agreed that unless the US effectively communicated this aim, the risk of escalation was a real possibility: 'The reality is that we don't know enough about escalation to really understand that risk. That risk is still there. The reality is that escalation really differs by country.'[1031]

Such uncertainty would seem to be a strong argument for more communication. Participant U3 argued there was significant uncertainty regarding escalation, and it was this uncertainty that made communication so critical for stability and security:

> I think we've overestimated it, but it's hard to really measure because you don't know, we don't have clear escalation paths, we don't have that doctrine, and actually often the adversaries don't understand their own doctrine let alone understand ours so it's sort of unpredictable what actions will be taken… if you have clear communication channels you can address that.[1032]

It is also worth noting that merely having the channels is not sufficient for effective communication: the message is also critical. Participants noted that what US officials viewed as successful communication may be interpreted differently by adversaries. This is evident in Participant U4's discussion of the best ways to produce security. He argued:

[1028] Participant U7, Quote 8, p.3
[1029] Participant U6, Quote 4, p.1
[1030] Participant U8, Quote 44, p.9
[1031] Participant U8, Quote 26, p.6
[1032] Participant U3, Quote 60, p.12

> Through anticipatory action, and most of this is defensive right? It's action to remove my vulnerabilities so that you can't exploit them. It's in my anticipating your intent to use such capabilities that you may develop so that you can't use those capabilities against me.[1033]

The likelihood of an adversary accepting such anticipatory action as a purely defensive manoeuvre seems low. As Participant U2 argued, deterrence works differently when your adversaries are sure they're hitting back, not hitting first. This misperception arises when communication is not sufficient:

> Signalling with adversaries? There is no signalling, other than the fight itself, or there's very little. There's almost nothing outside, like operational, transparency mechanisms… there's no hotline between military commands, if we go too far and China says you really gotta back off on this or there's gonna be a real problem – how are they going to get that message to us? So that's very problematic.[1034]

Participants also noted that the narrative around attribution was an important element of communication for deterrence. Participant U3 highlighted this as an issue both in terms of managing how adversaries see US actions, and how the domestic audience understood such actions:

> If you attribute conduct, and then you don't do it, because there are times you won't want to for various reasons, then the sense will be we don't know, and that's simply not true. So you have to always be careful about messaging. It's one thing to convince people we have to do this public attribution. It's another thing to take action, because that will have more of a potentially escalatory impact.[1035]

Some participants considered persistent engagement could be used as a tool for communication. Participant U4 pointed out the DoD could be doing so deliberately:

> The DoD strategy actually gives the explanation why, it says, that states are deterred from going to war with the US in cyberspace, so they're seeing cyberspace as a means to strategically compete.[1036]

And Participant U7 claimed 'The costs of inaction are far higher than the costs of action, if that action is done in a smart way.'[1037] However, Participant U3 also observed that this avenue was unlikely to provide a useful avenue for communication:

> We should be explicit about this, not tacit bargaining, and to use something like persistent engagement to shape the environment and what norms are, is silly because that requires a level of strategy that I just haven't seen so far, from any of these guys.[1038]

[1033] Participant U4, Quote 46, p.10
[1034] Participant U2, Quote 39 p. 6
[1035] Participant U3, Quote 23, p.6
[1036] Participant U4, Quote 38 p.9
[1037] Participant U7, Quote 25, p.7
[1038] Participant U3, Quote 35, p.7

There are also consequences for US division over the best approaches to communicating deterrence aims. Participant U7 argued a key issue with this domestic misalignment is the resulting opportunity for the military to provide thought leadership on deterrence in cyber policy:

> Messaging is fundamental to deterrence. One of the problems of the application, if not the theory of persistent engagement is that… and this comes back to the dysfunction within the US government and that has meant that the individual departments have basically done their own thing. And within DoD, there's basically no policy shop either so that has further pushed the brain work out of Cyber Command.[1039]

It therefore seems clear that participants viewed US attempts at communicating their deterrent intent as having failed on both the domestic and international levels, resulting in allies being uncertain and adversaries adopting escalating behaviour in response to perceived US aggression.

4.16 Perceptions of overall US deterrence: incomplete, ad hoc and risky

Having considered these basic requirements of deterrence both individually and as a whole, participants identified the US had at best partial success in developing capabilities, and failed on the requirements of credibility and communication. I therefore expected to find participants would consider the overall US approach a failure. But despite varying evaluations of the effectiveness of US activities against each individual element of deterrence, some participants were quite optimistic about the effectiveness of US deterrence policy in cyberspace as an overall proposition. Participant U2 argued that deterrence could be viewed as working effectively enough because no one had crossed the line into death and destruction in any significant way:

> I get very frustrated with the folks who say you can't tell if deterrence has worked. Well, you know if it failed. And when you see the mushroom cloud you can say hey, that didn't work. For me, that's what I look for in the measurement. We can see if it's failing.[1040]

Similarly, Participant U7 argued deterrence was working, at least to some extent:

> At some level deterrence is working. It might be because there are a lot of bad things that could happen through cyber means and they haven't happened for the most part… on the other hand to expect a complete prevention of bad guys doing anything bad, not least because how we define badness is different from country to country.[1041]

But Participant U7 also sounded a note of caution in judging whether deterrence had succeeded or failed and that it is hard to know when deterrence is working:

[1039] Participant U7, Quote 11, p.4

[1040] Participant U2, Quote 65, p.12

[1041] Participant U7, Quote p.11

> There are quite a lot of people who would tell you that we haven't done a very good job of putting some of the ideas into practice. So, it's kind of difficult to know whether they work or not. The government and people in the academic think tank world have talked a better game than we've actually delivered on… the rhetoric and the outcome need to be kind of moderated through what has actually happened.[1042]

In contrast to these views, Participant U1 argued that we know deterrence is effective, as much as we can judge these things, by where there are no attacks.[1043] For Participant U1, the implication is that deterrence cannot be judged effective in cyberspace as long as attacks are frequent and ongoing, and thus deterrence in cyberspace had clearly failed. Participant U3, however, argued the problem was not that such attacks were ongoing, but rather that the US was not resilient enough to these attacks. He argued the US was being terrible at deterrence and needing to do better at implementation:

> There's also deterrence by denial of course, I'm less sanguine on deterrence by denial because we've trying that, and we're terrible at that too, and I hope we get better, we absolutely need to invest resources in hardening the targets and improving cyber security.[1044]

Despite these notes of optimism, the confusion over key terms and how success in cyberspace is conceptualised overall resulted in an unclear path forward for US attempts to create deterrence. Participants identified many areas where the US needed to improve, most notably in communication. Participant U6 argued that US behaviour under the policy of persistent engagement may be creating instability in alliance relationships, and significantly degrading trust and credibility.

> The question, the number of Europeans have said is 'we knew you were already tramping around in our networks gaining intelligence. Now you're saying that you reserve the right to do whatever you want, including creating disruptive effects. Do you plan to talk to us about it, before, after, and are you going to protect our interests as well as yours? So these questions have to be answered, and if they're not appropriately answered the US is going to find itself isolated on this area.[1045]

Participants also identified many barriers to improvements, including the newness of cyberspace as a policy problem. Participant U1 argued that cyber is an entirely new strategic environment where the concepts do not yet fit.[1046] Participant U6 agrees, arguing 'It [cyberspace] is clearly a new dynamic and new factor. Not just in international relations, but in the way that citizens relate to each other and to their governments.'[1047] But the US is not creating deterrence policy in a vacuum – the newness of the strategic space is something that all states must manage. Participants were worried the US was focusing its deterrent efforts on unhelpful avenues. Participant U2 argues that in the US, deterrence is trying to do too

[1042] Participant U7, Quote 1, p.1
[1043] Participant U1, Quote 17, p.2
[1044] Participant U3, Quote 50, p.10
[1045] Participant U6, Quote 24, p.7
[1046] Participant U1, Quote 7, p.1
[1047] Participant U6, Quote 14 p. 4

much; 'It's an academic theory of cause and effect, it's a strategy, it's a DoD mission, it's a tactical measure.'[1048] And Participant U4 argued that some avenues, such as the pursuit of norms in cyberspace, were unlikely to produce tangible outcomes: 'In cyberspace nobody has a monopoly on the distribution of those benefits or the imposition of costs.'[1049] But Participant U3 viewed the creation of rules as important: 'The rules come first, and then you have to enforce those rules. I don't think you negotiate the rules of the road by things like persistent engagement.'[1050]

Lastly, participants had differing views on the future of deterrence for cyberspace. Participant 3 argued that deterrence in cyberspace was absolutely critical: 'It's not just a technical boutique issue but a core issue of national security and economic security, and ultimately foreign policy.'[1051] In contrast, Participant U5 noted that the debate over cyber deterrence may not be helpful. He argued, 'At the end of the day, people fight who they want to fight. And they line up their narrative to do that.'[1052] He continued:

> The issue is the relative unimportance of cyber. The numbers simply aren't there…There is no country for which cyber is the number one problem. Trade relationships trump cyber for China, nukes and conventional military trump cyber for Iran, nukes trump cyber in North Korea.[1053]

Finally, overall, Participant U8 saw no value in deterrence: 'I don't think there's any real useful approach to deterrence right now.'[1054] This departure from deterrence as a central goal of US cybersecurity represents a substantial, and perhaps unprecedented shift away from deterrence as a preferred course of policy action. This is a substantial shift in US strategy. Deterrence has played a significant role as part of US security since the 1950s. The analysis of the expert interviews demonstrated several common concerns, including that actions the US pursued in cyberspace in an attempt to create credibility could be perceived by others as detracting from the establishment of norms. Several participants also expressed concerned at the military lead in cyberspace policy, noting that activities such as pre-positioning through 'forward defence' could also cause problems within alliance relationships with many states. Finally, participants were concerned that the US did not have the will or intent to communicate its policies effectively. These concerns, taken together with the literature and policies, would seem to indicate that the shifting US approach to deterrence may contain serious risks.

4.17 Preliminary finding: The US approach does not meet core deterrence requirements

By examining declared US cyber deterrence policy, including the pivot to entanglement and engagement through a classic deterrence framework from 2008–18, this case study presents the initial finding that the US has achieved, at best, only a partial success in one of the required elements of creating deterrence in

[1048] Participant U2, Quote 2, p.1
[1049] Participant U4, Quote 54, p. 12
[1050] Participant U3, Quote 37, p. 7
[1051] Participant U3, Quote 80, p.16
[1052] Participant U5, Quote 48, p.11
[1053] Participant U5, Quote 52, p.13
[1054] Participant U8, Quote 2, p.1

cyberspace – with capability being the only the measure the US had established and maintained, albeit to a limited degree. The continued focus on implementing deterrence through denial and punishment, rather than developing policies specific to cyberspace based on classic deterrence principles, resulted in an overwhelming perception of failure as these policies did not drive sufficient effort towards creating credibility or communicating US intent in cyberspace. It finds that the shift to persistent engagement as a deterrence approach is flawed, as persistent engagement is instead creating new norms and potentially triggering unintended escalation. This case study posits that while the US views persistent engagement as supporting deterrence by establishing capability superiority and becoming engaged with threat actors, it is possible that adversaries could perceive such actions as acts of war, or at least grounds for escalation.

4.18 Conclusion

This chapter has explored how and why the US chose to apply aspects of a deterrence approach to its policies for securing cyberspace from 2008 to early 2018, and considered the reasons for the pivot away from deterrence in mid-2018. It found that strategists and cyber experts judged the US approach as having largely failed in deterring cyber-attacks, and presented the variation in reasoning for this failure – including arguments that the repeated failure to respond to cyber-attacks or effectively communicate US deterrence intent and consequences had resulted in a lack of credibility. The case study also found that despite the US creating multiple policies mentioning deterrence for cyberspace, none of the research participants considered that the US had established a deterrence strategy. While a few authors in the literature have argued such a strategy did exist, these authors relied on deterrence being delivered through US superior capabilities. This was a key arena that participants identified as problematic. Instead, the expert participants repeatedly voiced concerns that the US reliance on overwhelming capabilities or 'capability superiority and dominance' was insufficient for deterrence, and considered that this pursuit could be triggering escalation and a potential arms race in cyberspace. The case also study examined the origins of the shift towards the new policy approach of persistent engagement, and the evidence shows that while persistent engagement was aimed at creating 'deterrent effects' the norm of engagement, it set carried significant risk of escalation rather than deterrence. Finally, at no point during the period examined did US practice meet its own definitions of deterrence, nor did US policy present a balanced approach to the basic requirements of deterrence. Further implications of this, and potential lessons that may be drawn from the US approach are considered in Chapter 5.

Chapter 5 Cross-case analysis

5.1 Introduction

Having examined the Israel and US cases in Chapters 3 and 4, this chapter now considers what they reveal about the adoption of deterrence theory into cybersecurity policy. The chapter begins by noting the complexities both cases have faced in applying deterrence theory before considering the influence of their prior experiences of deterrence on the construction of deterrence theory for cyberspace. It then goes on to compare each cases' approaches to the deterrence requirements of capability, communication and credibility as presented in Chapter 3. The chapter argues that we can judge the US approach a failure for two main reasons: unrealistic expectations of deterrence in cybersecurity policy; and an overt focus on capabilities without supporting policy measures for credibility and communication. The US expected its deterrence approach to succeed, was surprised when it continued to fail, and has sought to adapt its policy dramatically over the 10-year period. However, at no point did the US approach meet the three requirements for classic deterrence, reflecting a failure of policy design rather than failure of deterrence theory.

The chapter contrasts these findings with the Israel case, arguing Israel expected its deterrence to be repeatedly challenged in cyberspace, as it had in other spheres of strategy, and that these challenges would require strong responses. Israel's expectations of deterrence were based on decades of practical experience in a contested environment and emphasised resilience to cyber-attacks rather than prevention. Thus the research found that because Israel judges its success holistically cyber-attacks were not considered an indication of Israeli deterrence failure but rather the need for a policy approach which was flexible, resilient and underwritten by the regular use of substantial force. But while this approach met the classic deterrence requirements and Israel considers it successful, this self-perceived success did not necessarily translate into reducing the risks Israel faces in cyberspace. As the implementation of Israel's deterrence approach is heavily reliant on the regular use of offensive measures and overwhelming force, adversaries were unlikely to perceive this as seeking to achieve deterrent aims. Rather they perceived Israel's activities in cyberspace as a serious threat which required an ongoing response.

The chapter concludes with a consideration of the lessons from both cases for strategy and theory and contends that despite both states investing significant effort into policies and measures designed to deter attacks in cyberspace, both still face cyber-attacks from increasingly capable adversaries. Far from creating deterrence in cyberspace these case studies demonstrate that the inclusion of deterrence in policy, whether complete or otherwise, is inherently risky.

5.2 Constructing deterrence policy for cyberspace: Different approaches to complexity

As discussed in Chapter 1, while the key requirements of deterrence theory are well established, views differ on whether deterrence theory can, or indeed should, be adapted to cyberspace.[1055] Chapters 3 and 4 considered why the cases covered in this research chose to adopt deterrence in spite of these difficulties, and then analysed how they constructed policies aimed at creating deterrence in cyberspace, as well as how they managed the challenges of implementation. Of course, the challenges faced by the two cases under consideration are by no means unique. As argued in Chapter 2, while deterrence theory is by nature elegant and parsimonious,[1056] cyberspace is a complex and swiftly evolving domain that policymakers have struggled to understand, let alone formulate policy for. The cases also demonstrated that deterrence theory is often not well understood by policymakers.[1057] And where it is understood, its application as part of cybersecurity policy has often been complicated by broader national security strategy.[1058] Thus the human element of deterrence remains a factor, regardless of the nature of cyberspace. It is also the case that identifying when deterrence has succeeded is difficult and depends on knowledge of both sides of a deterrence relationship[1059] – something that scholars or policymakers rarely have. But despite the challenges, by looking at the both the policies and visible practices between 2008 and 2018 the case studies produced significant data that helps explain why the approaches and expectations of the two states were so different. The next section of this chapter examines the key areas of differentiation in the cases' policy approaches.

5.3 Military leading policy: High risks, low reward

In Chapters 3 and 4, I outlined how in both Israel and the US the military took a leading role in the development and implementation of deterrence policy for cyberspace. While this role proved problematic for both nations, it was far more serious for the US than Israel, causing significant problems for both the construction and implementation of effective deterrence policy. Consider the example of the US military's insistence on cyberspace as a domain of warfare, despite its inability to articulate even the most basic policy for military-civilian demarcation of responsibilities. This was not an unexpected finding: in Israel it seemed logical that the military leadership of deterrence for cyberspace would be broadly accepted as the separation between state and non-state assets is traditionally lower than in states such as the US – and Israeli society is, to a certain extent, acclimated to the idea of its assets being co-opted to ensure Israel's

[1055] N. J. Ryan, 2018, 'Five Kinds of Cyber Deterrence', *Philosophy and Technology*, 31, 338

[1056] Robert Jervis, 'Deterrence Theory Revisited', ed. Alexander George and Richard Smoke, *World Politics* 31, no. 2 (1979): 289–324

[1057] Tim Stevens, Deterrence in Cyberspace: Silver Bullet or Sacred Cow p.431

[1058] Richard Andres, 2017, 'Cyber Gray Space Deterrence', *PRISM,* 7:2

[1059] Richard Ned Lebow and Janice Gross Stein, 'When Does Deterrence Succeed and How Do We Know', CIIPS Occasional Paper No. 8 p.12

survival.[1060] The higher the stakes involved, the higher the tolerance demonstrated by Israeli society.[1061] However this research did find that the acceptance of the centrality of military leadership in this space was not entirely uncontested. As Adamsky has argued, Israel had had to manage the reluctance of parts of the private sector to submit to protection by the Shabak[1062] due to concerns over innovation and growth, contending also it was this discontent that led to the 2017 Israeli Cyber Security Strategy.[1063] Although the policy itself does not openly acknowledge it, the fact this was the first publication of any formal Israeli security strategy indicates the Israeli government saw a new need for transparency. And the strategy did note the following reason for carefully delineating responsibility between the public and private sector: 'the three-layer approach derives from the unique nature of the cyber threat and the central role of private organizations in achieving national cyber security'.[1064]

By explicitly restricting the military role to only the third and most serious layer of 'National Cyber Defense', the Israeli government gave the military responsibility for only 'severe threats by determined, resource-rich nations who pose serious danger to the nation'. [1065] This seems to support Adamsky's argument that there was a need to reassure civilian stakeholders. However, as noted in Chapter 3, this carefully constructed policy role and restricted responsibility is not always reflected by the reality of IDF practices: the 2019 IDF bombing of 'Hamas cyber headquarters' was in response to defacement of a public website,[1066] and it is difficult to see how defacing a website could possibly constitute a 'severe threat that poses serious danger to the nation,' or require what was euphemistically referred to by an official spokesperson as the complete 'removal' of Hamas cyber capabilities.[1067] Israeli media has at times been critical of the influence the IDF has over cyber strategy.[1068] Yet the overall perception of the IDF's role as essential for defending Israeli survival has been a consistent and largely unchanging and accepted role in policy related to creating deterrence in cyberspace. In fact, the military has increased its role through the creation of new cyber units in the Israeli National Signals Intelligence and Code Decryption Unit (Unit 8200), units tasked to coordinate and manage military operations in cyberspace.[1069] Despite Adamsky's concerns, then, the case study showed consistent – although not comprehensive – support for the IDF's role in leading deterrence in cyberspace. The support for military leadership on deterrence

[1060] Martin Sicker, Israel's Quest for Security; Michael I Handel, 1973, Israel's Political Military Doctrine, Harvard; see also Avi Kober, 'Blitzkrieg to Attrition: Israel's Attrition Strategy' p.234

[1061] Avi Kober, 'Blitzkrieg to Attrition: Israel's Attrition Strategy' p.220

[1062] Israeli internal security service; the Israeli General Security Service is called *Sherut HaBtiachon HaKlali* in Hebrew. It is often abbreviated as Shabak and is commonly referred to as Shin Bet. See https://www.jewishvirtuallibrary.org/directors-of-the-general-security-service-shabak

[1063] Dima Adamsky, Israeli security odyssey p. 115

[1064] 'Israel National Cyber Security: In Brief', September 2017, State of Israel

[1065] Ibid

[1066] Judah Ari Gross, 2019, 'IDF Says It Thwarted a Hamas Cyber Attack during Weekend Battle', *The Times of Israel*

[1067] Ibid

[1068] 'Cyberattacks on Israel: The State's Stupidity Is Putting Officials at Risk', Haaretz.com, accessed 24 June 2021, https://www.haaretz.com/israel-news/tech-news/.premium-cyberattacks-on-israel-the-state-s-stupidity-is-putting-officials-at-risk-1.9389796.

[1069] Netolicka and Mares, 'Arms Race "in Cyberspace" - A Case Study of Iran and Israel', p.422.

policy indicates that despite ongoing cyber-attacks Israel views its deterrence effects best managed by the military under the leadership of the Prime Minster. This view reflects broader Israeli strategy whereby the IDF is 'the guarantor of Israel's national existence'.[1070]

In comparison, I expected to find that the US military leadership of deterrence policy for cyberspace would be less accepted, with civilian corporations far more concerned than their Israeli counterparts regarding the role of the US military in securing cyberspace. The US case indeed revealed a complicated military–civilian relationship which was exacerbated by the lack of certainty over roles and responsibilities for deterrence. While the US has noted the problem of military taking responsibility for protecting civilian infrastructure, no US policy contains a clear demarcation between civilian and military responsibilities.[1071] Indeed US policy has openly and repeatedly acknowledged the issue of conflicting responsibilities[1072] without offering any mitigations, meaning the US military continues to have a leading – but essentially unclear – role in deterrence for cyberspace. This has led to a significant gap whereby uncertainty over roles and responsibilities frequently led to delayed US responses to attacks on private infrastructure, or worse: no visible response at all. Further, the sheer number of US government agencies with a role in cybersecurity[1073] means that the military is also frequently at odds with other government agencies – let alone private industry. This research found that the gap in relevant policy has allowed US Cyber Command taking an increasingly ambitious role for itself. Consider that the original intent for Cyber Command on establishment in 2009 was to:

> plan, coordinate, integrate, synchronize and conduct activities to: direct the operations and defense of specified DoD information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.[1074]

This was a broad and contradictory remit even at the outset. How could the US hope to achieve the goal of freedom of operation for itself and allies while denying the same to its adversaries? Yet despite this obvious policy overreach, in 2017 President Trump went further and decided to elevate Cyber Command to a unified combatant command[1075] based on the perceived the need for the military – led by Cyber Command – to take a greater role in leading on deterrence. By 2018, the vision of Cyber Command was expanded significantly to:

[1070] 'Israeli Defense Forces' Defense Doctrine - English Translation', *Policy File* (Belfer Center for Science and International Affairs, 2016), Conclusion

[1071] S. Massoud Amin, 2015, 'Power and Energy Infrastructure: Cyber Security, Defense, and Resilience', *Georgetown Journal of International Affairs,* 16:SI, 70

[1072] Ash Carter, 'The DoD Cyber Strategy', April 2015, US Department of Defense ,

[1073] Alex S. Wilner, 2020, 'US Cyber Deterrence: Practice Guiding Theory', *Journal of Strategic Studies*, 43:2, 271

[1074] 'U.S. Cyber Command – U.S. Strategic Command', 16 April 2014, https://web.archive.org/web/20140416192156/http:/www.stratcom.mil/factsheets/2/Cyber_Command/.

[1075] 'Statement by President Donald J. Trump on the Elevation of Cyber Command – The White House', accessed 24 June 2021, https://trumpwhitehouse.archives.gov/briefings-statements/statement-president-donald-j-trump-elevation-cyber-command/.

> Achieve and maintain superiority in the cyberspace domain to influence adversary behaviour, deliver strategic and operational advantages for the Joint Force, and defend and advance our national interests.[1076]

Since then, Cyber Command has increasingly driven US cybersecurity policy towards engagement rather than deterrence.[1077] Given that the role of Cyber Command is to provide the US government with options to punish cyber aggressors[1078] this effort is perhaps not surprising. Militaries are, after all, designed to view their role as being fundamentally capability-based and results driven. But the shift towards persistent engagement rather than deterrence marked a worrisome shift in US policy. The US was no longer building capabilities it could use but chose not to, advocating restraint as they did during the Cold War. Rather it was choosing to build and develop capabilities with the express intention of using them despite the lack of clearly defined expectations or red lines.

Thus in both cases, the military has a central role in driving and implementing deterrence policy for cyberspace, but at widely differing levels of organisation and acceptance. And while the Israeli role may appear overbearing, within its strategic context it is not unusual. The US experience, however, has been more problematic. Its failure to carefully outline the role of the military and appropriate protections and responsibilities has resulted in uncertainty for civilian partners and an increased role for Cyber Command.

5.4 Problematic success

This research found the US and Israel's historical experiences of deterrence deeply influenced their conceptions of successful deterrence for cyberspace, including influencing their respective understanding of the threat. As outlined in Chapters 3 and 4, both cases had adopted deterrence in other spheres prior to adopting it for cyberspace. Both judged it as having achieved its aims and this perceived success was a strong contributing factor in utilising it in relation to cyberspace. However, the significantly different experiences of deterrence leading up to 2008 produced significantly different definitions of success and expectations. For Israel, the influence of the immediate and kinetic nature of the threats it faced from both state and non-state actors throughout its modern history can be traced through its policy – where cyber threats are described as part of a broader integrated threat environment, emblematic of particular threat actors and viewed as an ongoing risk to be managed rather than prevented.[1079] Israel's definition of

[1076] Gen. Paul M. Nakasone, 'Command Vision for US Cyber Command: Achieve and Maintain Cyberspace Superiority', April 2018, United States Cyber Command, p.5

[1077] 'Elevation of U.S. Cyber Command to a Unified Combatant Command: Memorandum for the Secretary of Defense', 23 August 2017, Federal Register, 82:162

[1078] Wilner, 'US Cyber Deterrence: Practice Guiding Theory', p.271.

[1079] See threat actors listed in the Eizenkot Doctrine: 'The threats facing the State of Israel are the following: States – distant (Iran) and nearby (Lebanon), failed states and states in a process of disintegration (Syria); substate organizations (Hezbollah, Hamas); terrorist organizations without links to a particular state or community (Islamic Jihad, Palestinian Islamic Jihad, ISIS, and others).' See Gadi Eizenkot, August 201 'Deterring Terror: How Israel Confronts the Next Generation of Threats', Belfer Center for Science and International Affairs, 6; see also Yigal Unna, director general of the Israel National Cyber Directorate (INCD) statements in 2019: 'Iran and its proxies continue to pose a main cyber threat on the Middle East. Israel is prepared for cyber-threats and we have the cyber-attacks is similarly telling, as the use and targeting of computers, networks, or other technologies for malevolent, destructive or disruptive purposes[1080] represents a broad and effects-based definition consistent with the Israeli approach of treating threats in cyberspace as an extension of the threats it faces in other domains. Prime Minister Netanyahu has similarly made a number of statements indicating that while Israel takes the threats to its interests through cyber-attacks very seriously, such attacks must also be considered in the context of Israel's broader threat space.[1081]

The Israeli approach of treating threats as part of its broader threat spectrum leads the government to expect attacks. Israel's experience with deterrence was that it could fail and fail dangerously.[1082] And while Israel's strategy seeks to deter cyber-attacks, it is also designed to mitigate the failure of that deterrence. Thus although Israel accepts that attacks in cyberspace will occur, it also has dedicated significant effort to mitigating their effects.[1083] This conception of success as survival means the threats posed by cyber-attacks are viewed as symptoms and mechanisms of broader threats, rather than treating these as fundamentally new or different. While consistent with Israeli strategy, this research identified there was however risk in this approach, because while Israeli responses to attacks might be defensible in Israel due to the well-understood nature of these threats, to the broader international environment and indeed to adversaries such responses might seem so disproportionate as to represent provocation rather than deterrence.[1084]

In contrast, the US seemed uncomfortable describing the threats posed to its interests in cyberspace and uncertain in how best to manage these as part of the strategic environment. This is illustrated by the 2010 Annual Threat Assessment from the intelligence community, which described the cyber threat:

> The United States confronts a dangerous combination of known and unknown vulnerabilities, strong and rapidly expanding adversary capabilities, and a lack of comprehensive threat awareness. Malicious cyber activity is occurring on an unprecedented scale with extraordinary sophistication. While both the threats and technologies associated with cyberspace are dynamic, the existing balance in network technology favors malicious actors, and is likely to continue to do so for the foreseeable future. [1085]

capability to respond forcefully to cyber-attackers.' Kacy Zurkus, 'Netanyahu Boasts of Israel's Cyber Intelligence', *Infosecurity Magazine*, 26 June 2019

[1080] Cohen, Freilich, and Siboni, 'Israel and Cyberspace: Unique Threat and Response', p.309.

[1081] 'Netanyahu: Iran behind Cyber Attacks on Israel', *The Jerusalem Post* | JPost.com, accessed 24 June 2021, https://www.jpost.com/isr ael-news/watch-live-netanyahu-addresses-cyber-security-conference-375290. see also 'Netanyahu', 29 January 2019.

[1082] Zeev Maoz, 2007, 'Evaluating Israel's Strategy of Low-Intensity Warfare, 1949-2006', *Security Studies,* 16:3, 319-49; Shmuel Bar, 2020, 'Israeli Strategic Deterrence Doctrine and Practice', *Comparative Strategy,* 39:4, 321-53

[1083] Netolicka and Mares, 'Arms Race "in Cyberspace" - A Case Study of Iran and Israel', p.420.

[1084] Libicki, 'Expectations of Cyber Deterrence', p.52.

[1085] Dennis C. Blair, 2 February 2010, Annual Threat Assessment of the U.S. Intelligence Community for the Senate Select Committee on Intelligence, from https://www.dni.gov/files/documents/Newsroom/Testimonies/20100202_testimony.pdf

The 2018 US Cyber Command Vision noted the US view that the threat posed against it had changed significantly:

> The cyberspace domain that existed at the creation of US Cyber Command has changed. Our adversaries have exploited the velocity and volume of data and events in cyberspace to make the domain more hostile. They have raised the stakes for our nation and allies. In order to improve security and stability, we need a new approach.[1086]

US policy has, however, been remarkably consistent on listing vulnerabilities. The US 2010 Threat Assessment described the threat in these terms: 'We cannot be certain that our cyberspace infrastructure will remain available and reliable during a time of crisis.'[1087] This view was reiterated in former President Trump's Foreword to the 2018 US Cyber Strategy:

> Cyberspace is an integral component of all facets of American life, including our economy and defense. Yet our private and public entities still struggle to secure their systems, and adversaries have increased the frequency and sophistication of their malicious cyber activities.[1088]

Uncertainties over how to best manage the cyber threat is further illustrated by the hesitant US approach to name and respond to cyber-attacks. As argued in Chapter 4, the US policy position of seeking to collectively attribute cyber-attacks is problematic for effective deterrence because it takes valuable time to establish collective attribution, significantly lengthening the time between the attack and attribution. Second, collective attribution requires agreement on not only the threat actor but also the appropriate response, requiring either sharing of methods and sources of attribution, or accepting others' assessments. Both avenues require substantial trust between partner nations.[1089] In this context the hesitancy around US willingness to attribute cyber-attacks may be due – at least in part – to not wanting to admit either that attacks had occurred or the seriousness of attacks, because to do so would reinforce that US deterrence in cyberspace had failed.

Beyond the problem of attributing cyber-attacks, the US has also repeatedly demonstrated its unwillingness to impose visible consequences for conducting cyber-attacks, leading then Senator John McCain to state in 2015 that the lack of timely responses to cyber-attacks led adversaries to perceive there were no consequences for attacking the US through cyber means.[1090] This thesis has found there was a significant issue with having an explicit deterrence stance in public strategy stating the US would respond to cyber-attacks in certain ways, and then consistently failing to do so. This disconnect between

[1086] Gen. Paul M. Nakasone, April 2018, 'Command Vision for US Cyber Command: Achieve and Maintain Cyberspace Superiority', United States Cyber Command, p.2

[1087] Dennis C. Blair, 2 February 2010, Annual Threat Assessment of the U.S. Intelligence Community for the Senate Select Committee on Intelligence, p.47

[1088] 'National Cyber Strategy of the United States of America', September 2018, The White House, US, Foreword

[1089] Davis and Rand Corporation, 'Stateless Attribution: Toward International Accountability in Cyberspace', p. 25.

[1090] Quoted in David J. Lonsdale, 2018, 'Warfighting for Cyber Deterrence: A Strategic and Moral Imperative', *Philosophy & Technology,* 31:3, 421, https://doi.org/10.1007/s13347-017-0252-8 explicit US public strategy and practice was noted by the cyber experts participating in this research as a key reason for the US having failed to establish any credibility in cyberspace: 'for deterrence to work, you need credibility, you need signalling. You need crisp resolve. None of these things are actually in operation.'[1091] This disconnect was described by a former US senior State Department Cyber Adviser as a failure of political will and ultimately, US credibility.[1092] As reviewed in the case study, these decisions are seemingly difficult to understand. However, if considered in light of US expectations of success – having built the internet, the US could control the security environment – and achieve 'cyber deterrence' in the same way it had achieved 'nuclear deterrence'[1093], the lack of suitable response is perhaps more understandable.

Israel's fundamentally different expectation of deterrence is visible in its approach to attributing cyber-attacks. Between 2008 and 2018 Israel adopted a strategy of not only publicly identifying the origin of many cyber-attacks swiftly, but also responding to them with overwhelming force.[1094] The willingness to attribute attacks helped Israel build a perception that attacks on its interests would not be tolerated, which is a critical requirement for credibility.[1095] PM Netanyahu has publicly stated that Iran is responsible for significant attacks on Israel 'on a daily basis'.[1096] Israel has attributed a number of cyber-attacks to Hamas and Hezbollah, and responded to such attacks quickly. It has also named a number of attacks as emanating from certain groups, without noting a country of origin.[1097] The 2019 response to a 'Hamas cyber-attack' was claimed by the IDF as a real time response[1098], something that would have been unthinkable to the US. The Israeli narrative regarding attribution is thus bold in comparison to the US, however it is not necessarily entirely transparent.

There is a difference between attributing and responding to known and relatively low-capability threat actors, and states with advanced capabilities and unclear objectives, such as Russia.[1099] Indeed, this research found that there were substantial caveats on this seemingly strong approach to attribution, an issue raised by several participants in the expert interviews. Participants noted that Israel suffered many attacks which it chose not to attribute – a decision that participants identified as being political choice, rather than a technical inability to identify the relevant adversary. One of Israel's leading strategists argued this was a deliberate decision to maintain credibility, as attribution without an associated response was

[1091] See Participant U8, Chapter 4.

[1092] Participants U5 and U3 made these cases, see Chapter 4.

[1093] Eric Sterner, Retaliatory Deterrence in Cyberspace (Strategic Studies Quarterly Spring 2011), see also Warfighting for Cyber Deterrence, David J Lonsdale.

[1094] See Shmuel Barr, Dima Adamsky and Gil Baram 'Israel and Iran just showed us the future of cyberwar'.

[1095] Eric Sterner, 2011, 'Retaliatory Deterrence in Cyberspace', *Strategic Studies Quarterly,* Spring 2011; see also David J. Lonsdale, 2018, 'Warfighting for Cyber Deterrence: A Strategic and Moral Imperative', *Philosophy & Technology,* 31:3, 409-429, https://doi.org/10.1007/s13347-017-0252-8

[1096] 'Netanyahu', 29 January 2019.

[1097] Rami Ayyub, 12 August 2020, 'Israel Says It Thwarted Foreign Cyber Attack on Defence Industry', *Reuters*, sec. Aerospace and Defense

[1098] Gross, 'IDF Says It Thwarted a Hamas Cyber Attack during Weekend Battle'.

[1099] Leyden, 'Russia's to Blame for pro-ISIS Megahack on French TV Network'.

unhealthy.[1100] If they are correct, the Israeli approach is carefully nuanced to maintain credibility while accepting that there were situations where attributing was not politically useful. It may also indicate that despite Israel's view of its deterrence approach in cyberspace as successful, it is still wrestling with the problem of how best to manage cyber threats posed by advanced nations, including whether they can be deterred.

Such uncertainty also helps explain Israel's extraordinary efforts to increase its capabilities in cyberspace, as well as its ongoing commitment to cyber strategies.[1101] Importantly, even when taking such non-attributed attacks into consideration, case study participants did not consider that these were an indication deterrence had failed. Rather, they were viewed as an indication Israel needed to continue building its capabilities and deterrence posture in order to be able to manage emerging threats. Thus the view of Israel's deterrence as a cumulative process meant the ongoing and increasing attacks by advanced threat actors was viewed as a sign that deterrence needed refreshing, not that it had failed.

5.5 States versus the rest: Defining the threat

Both Israel and the US recognise the need to manage cyber threats from both state and non-state actors, but each has managed the variety of threats very differently. However although deterrence has traditionally been a matter for states,[1102] Israel's broader threat environment has long included non-state threats, including state-like entities, terrorist organisations and individuals.[1103] Thus Israel's approach to deterrence has traditionally been 'attacker agnostic': a product of needing to ensure security, regardless of the origin of a threat.[1104] As well as its traditional adversaries,[1105] Israel also potentially faces new threats not captured in official policy, and in order for its deterrence to be considered successful it must manage these threats as well. On this point Raska has argued that by focusing on traditional adversaries Israel was potentially not managing the emerging threats from more advanced cyber nations.[1106] However, Israel's attacker-agnostic approach theoretically allows for the management of new threat actors, and this research has found that Israeli cyber experts were certainly aware of the threat posed by cyber advanced nations. Israel's experience of states using non-state actors as proxies is lengthy, such as the example of Iran regularly sponsoring Hezbollah activities.[1107] Participants noted the risks posed by nations, most notably China[1108] and Russia.[1109] And Israeli academics have noted cyber-attacks emanate from not only

[1100] Participant I4, Chapter 3.

[1101] Netolicka and Mares, 'Arms Race "in Cyberspace" - A Case Study of Iran and Israel', 420.

[1102] Eric Sterner, 2011, 'Retaliatory Deterrence in Cyberspace', *Strategic Studies Quarterly,* 5:1, 62

[1103] Gadi Eizenkot, August 2016, 'Deterring Terror: How Israel Confronts the Next Generation of Threats', Belfer Center for Science and International Affairs Ch.i

[1104] 'Israel National Cyber Security: In Brief', September 2017, State of Israel, p.13

[1105] Gadi Eizenkot, August 2016, 'Deterring Terror: How Israel Confronts the Next Generation of Threats', Belfer Center for Science and International Affairs Ch.i

[1106] Michael Raska, 2015, 'Confronting Cybersecurity Challenges: Israel's Evolving Cyber Defence Strategy', *Policy File,* S. Rajaratnam School of International Studies

[1107] Amos Malka, 2008, 'Israel and Asymmetrical Deterrence', *Comparative Strategy*, 27:1, 1

[1108] Participants I4, I6, and I7.

[1109] Participants I3, I7, and I2.

traditional enemies such as Iran, Hamas and Hezbollah, but also China's PLA, Turkey and North African nations.[1110] In fact, the Israeli government used the threat of emerging adversaries as evidence of the need to continue its drive for improved capability.[1111] Israel's awareness of the potential for emerging adversaries with advanced cyber capabilities has also been widely reported in the Israeli media.[1112]

In contrast, the US public identification of threat adversaries in cyberspace took much longer. US policy did eventually name its four main state adversaries in 2018. However while acknowledging the threat it faced from non-state actors, the US failed to articulate intended responses or consequences for cyber-attacks from non-state actors beyond broad statements of intention to 'impose costs'.[1113] This arguably emboldened state actors to use non-state actors as cyber proxies, an issue recognised in US policy without any solution being identified.[1114] And despite the acknowledgment in policy of the threat from non-state actors, US literature continued to focus on states, leaving an important gap.[1115]

The US experience during the Cold War taught it that states could be deterred, however cyber-attacks can be launched by states, non-state actors, or individuals and can target military, government or civilian systems.[1116] By publicly stating that the threats in cyberspace required new strategy – rather than adapting existing strategy – the US was designating its previous attempts in deterrence strategy as ineffective. Hence the inability of US cyber policy to identify and manage deterrence options against non-state actors proved to be yet another area where the US cyber deterrence policy could not be judged a success. Former US President Donald Trump acknowledged this in his 2018 National Cyber Strategy, when he stated that:

> New threats and a new era of strategic competition demand a new cyber strategy that responds to new realities, reduces vulnerabilities, deters adversaries, and safeguards opportunities for the American people to thrive.[1117]

5.6 The cyber domain: an isolated or integrated battlespace?

This thesis initially expected to find that the question of whether cyberspace was a domain of warfare would be relatively settled and accepted. Indeed, the literature review conducted in Chapter One certainly found that the terminology of domain was widely used to describe the space in which states were attempting to enact cyber deterrence policy.[1118] Both Israel and the US had designated cyberspace as a

[1110] Cohen, Freilich, and Siboni, 'Israel and Cyberspace: Unique Threat and Response', p.310.
[1111] Ibid
[1112] 'Shin Bet Deputy Chief R: Mossad, Shin Bet, IDF Borders May Need Redo - The Jerusalem Post', accessed 24 June 2021, https://www.jpost.com/israel-news/shin-bet-deputy-chief-r-mossad-shin-bet-idf-borders-may-need-redo-664571.
[1113] Barack Obama, 'National Security Strategy', February 2015, The White House, US, p.13
[1114] Gen. Paul M. Nakasone, April 2018, 'Command Vision for US Cyber Command: Achieve and Maintain Cyberspace Superiority', United States Cyber Command, p.3
[1115] Wilner, 'US Cyber Deterrence: Practice Guiding Theory', p. 252.
[1116] Cohen, Freilich, and Siboni, 'Israel and Cyberspace: Unique Threat and Response', p.309.
[1117] 'National Cyber Strategy of the United States of America', September 2018, The White House, US, Preface
[1118] Sterner, 'Retaliatory Deterrence in Cyberspace', p.66.

domain of warfare early in their policy approaches, and as Netolicka has argued, states which perceive cyberspace as an additional operational domain establish and gradually build their cyber capabilities, both offensive and defensive.[1119] However, the designation 'domain' had different meanings and different implications for each case study. For Israel, the 2009 designation of cyberspace as a 'strategic and operational battle zone'[1120] was perceived as a logical extension of existing Israeli strategy. The designation reflected Israel's intent to treat cyberspace as integrated part of the total threat space it faced.[1121] This view of the cyber domain as a holistic part of broader strategy arguably saved Israel significant intellectual effort, however it did not eliminate the difficulty of securing a space that is largely privately owned.

According to Adamsky, Israel's 2017 cybersecurity strategy, while appearing to represent a remarkably cohesive and whole-of-society approach was in fact the product of many years of policy and government effort to reassure the Israeli business community.[1122] The strategy established clear lines of demarcation between civilian and military responsibilities. Putting the military in charge of the cyber domain went only so far as 'national cyber defense', defined as being triggered by 'determined, resource-rich attackers who pose serious damage to the nation'.[1123] This means the Israeli military efforts are, at least in theory, targeted only at responding to the most serious threats; based on this policy we would expect to see the military responses limited to these high-risk attacks. But Israeli practice has actually proven far broader than this policy would suggest. As noted previously, the 2019 IDF response to 'Hamas cyber-attacks' was in fact triggered by temporary defacing of a public Israeli website,[1124] yet it is difficult to see how this could be described as 'serious damage to the nation'.[1125] If this is considered in the context of Israel's view of cyberspace as an integrated domain of warfare, the logic is more apparent. Israel is used to having 'very short wars and very big victories'.[1126] Thus the Israeli conceptualisation of cyberspace as an extension of other domains means it treats what may appear as relatively minor threats in cyberspace as part of a broader threat scape, rather than isolated events. These responses are more logical if considered in the context of cyberspace as an integrated domain, and help explain why Israel's responses to cyber-attacks may appear disproportionate. However, there is a risk that adversaries may not accept such an approach, potentially leading to unintended consequences. Iran provides a potential example of this – while it may consider that its cyber-attacks on Israel are relatively low-level, Israel considers such attacks

[1119] Netolicka and Mares, 'Arms Race "in Cyberspace" - A Case Study of Iran and Israel', p.426.

[1120] Baram, 'Israeli Defense in the Age of Cyber War'.

[1121] Gadi Eizenkot, August 2016, 'Deterring Terror: How Israel Confronts the Next Generation of Threats', Belfer Center for Science and International Affairs

[1122] Adamsky, 'From Israel with Deterrence: Strategic Culture, Intra-War Coercion and Brute Force'.

[1123] 'Israel National Cyber Security: In Brief', September 2017, State of Israel

[1124] Judah Ari Gross, 'IDF Says It Thwarted a Hamas Cyber Attack during Weekend Battle', *The Times of Israel*, 2019

[1125] 'Israel National Cyber Security: In Brief', September 2017, State of Israel

[1126] Avi Kober, 2005, 'From Blitzkrieg To Attrition: Israel's Attrition Strategy and Staying Power', *Small Wars & Insurgencies,* 16:2, 220 as serious.[1127] And yet even so, Israel's definition of cyberspace as a domain of warfare where attacks are expected and planned for remained consistent over the period reviewed in this thesis.

In stark contrast, US attempts to classify and manage cyberspace as a domain of warfare have not been coherent. This includes the stark divisions in the US literature on the topic over whether cyberspace should be considered a domain of warfare.[1128] In policy terms, the US has indeed designated cyberspace as a domain of warfare that needed to be secured by the military from the outset of its earliest cyber policies.[1129] Yet this definition has presented a number of challenges in the policy space.

First, the US views domains of warfare as interrelated but separate, and at times this results in fragmented policy. This disconnect is evident in the 2018 National Cyber Strategy, which promised to 'defend the homeland by protecting networks, systems, functions and data'[1130] while also admitting hit had so far failed to do so, as 'public and private entities have struggled to secure their systems as adversaries increase the frequency and sophistication of their malicious cyber activities.'[1131] As in Israel, the US academic community noted concerns about the military claiming ownership and protection of a space that was largely civilian-owned and managed. But unlike Israel, these concerns are explicitly noted in US public policy. US strategy has not offered a solution to this problem, nor has the military been given specific responsibilities or roles beyond 'the protection of military assets and infrastructure'.[1132] This immediately renders deterrence unachievable, as the majority of spaces that the US needed to deter and protect are in fact civilian.[1133]

Second, while the US military accepts cyberspace as a domain of warfare, it has not resolved the question of whether cyberspace should be integrated into the broader battlespace, or considered as a separate domain. Disagreements over this have proved repeatedly problematic for US cyber strategies and may account for their disjointed nature. The clearest example of the US expectation it could manage cyber as a separate domain was the creation of the US Cyber Command as a separate military command, established at the same level of responsibility as Pacific Command and Northern Command. By setting up a separate command structure the military was not only signifying its intent to keep leadership of cyber strategy in the military, but it was also setting up the expectation that the military could keep cyber conflict confined

[1127] Bahgat, 'Iranian-Israeli Confrontation: The Cyber Domain'.

[1128] See Jim Chen, 2018, 'Does Conventional Deterrence Work in the Cyber Domain?', in *European Conference on Cyber Warfare and Security,* Reading: Academic Conferences International Limited, 106-X; William J. Lynn, 2010, 'Defending a New Domain: The Pentagon's Cyberstrategy', *Foreign Affairs*, 89:5, 97-108; and Dorothy E. Denning, 2015, 'Rethinking the Cyber Domain and Deterrence', *Joint Force Quarterly,* 77:8

[1129] 'Department of Defense: Strategy for Operating in Cyberspace' (United States Department of Defense, July 2011), 5,

[1130] 'National Cyber Strategy of the United States of America', September 2018, The White House, US, Foreword

[1131] Ibid, p.2

[1132] Gen. Paul M. Nakasone, April 2018, 'Command Vision for US Cyber Command: Achieve and Maintain Cyberspace Superiority', United States Cyber Command, p.2

[1133] Kenneth J. Knapp and William R. Boulton, 2006, 'Cyber-Warfare Threatens Corporations: Expansion into Commercial Environments', *Information Systems Management,* 23:2, 76-87 to that domain – an expectation that was unachievable as evidenced by Cybercom's 2018 statement regarding needing support from other agencies.

5.7 Superiority: A problematic goal

Despite different approaches to defining and constructing deterrence, by 2018 both Israel and the US had established and maintained a consistent drive towards superiority in cyberspace. Both cases have exhibited a history of strong military capabilities as an essential component of successful deterrence. The two case studies arrived at this need for superiority in cyberspace through very different paths: Israel did so to reinforce its perceived deterrence success; while the US was attempting to mitigate its perceived deterrence failure. The US 2018 Cyber Security Strategy identified the risk of ceding superiority in cyberspace as serious and responded by stating the new goal of 'preserve US overmatch in and through cyberspace'.[1134] Beyond superiority, the concept of overmatch decrees that the US retain 'military and technological superiority over all current and future challenges'.[1135] The US military interprets this as ensuring the 'US military's ability to fight and win in any domain, including cyberspace'.[1136]

There are several serious problems with the US attempt to establish overmatch as part of a deterrence posture for cyberspace. First, it is meant to occur in concert with 'deterring behaviour in cyberspace that is destabilising and contrary to national interests', [1137] which is an enormous and poorly defined remit. 'Overmatch… is about fighting and winning but overmatch is also about the ability to deter.'[1138] The logic behind this approach is presented in the 2018 Cyber Command vision, which declares:

> Through persistent action and competing more effectively, we can influence the calculations of our adversaries, deter aggression, and clarify the distinction between acceptable and unacceptable behavior in cyberspace.[1139]

Second, overmatch shows the lingering influence of Cold War thinking on strategy that further demonstrates the influence of the US military. The pursuit of overmatch is a singular goal, rather than a carefully designed policy position supported by a whole-of-government or broad domestic approach. Laura Junor Pulzone and Justin Lynch argue this is the case even within the DoD, where without a parallel effort to develop the civilian workforce, the US will not achieve overmatch in cyberspace.[1140] The

[1134] 'National Cyber Strategy of the United States of America', September 2018, The White House, US

[1135] Michael T. Klare, 2019, 'Why "Overmatch" Is Overkill', *The Nation,* 308:2; see also the US 2017 National Security Strategy

[1136] 'Department of Defense: Strategy for Operating in Cyberspace', July 2011, United States Department of Defense

[1137] 'Modernization Gives Army Overmatch, Deterrence | AUSA', accessed 24 June 2021, https://www.ausa.org/news/modernization-gives-army-overmatch-deterrence.

[1138] 'Modernization Gives Army Overmatch, Deterrence | AUSA'.

[1139] Gen. Paul M. Nakasone, April 2018, 'Command Vision for US Cyber Command: Achieve and Maintain Cyberspace Superiority', United States Cyber Command

[1140] 'Intellectual Overmatch Is Impossible If We Teach Only Half The Team: A Call For Professional Civilian Education', *States News Service*, 2021 lack of support from broader US policies or strategy is also explicitly noted in the 2018 US Cyber Command strategy:

> The Department of Defense is building the operational expertise and capacity to meet growing cyberspace threats and stop cyber aggression before it reaches our networks and systems. We need a policy framework that supports and enables these efforts.[1141]

Third, publishing policy which designates overmatch as a goal – while acknowledging the US does not have the broader governance or strategy to support such a goal – is clearly problematic. Although the US drive for superiority was designed with the aim of deterring attacks, deterrence fails where strategy is poorly executed.[1142] Given the explicit lack of supporting policy and cross-government efforts, US cybersecurity strategies have clearly not been well executed over the period in question. Further, deterrence also fails where the challenger feels under threat[1143] and the increasing US reliance on overmatch is not a passive capability. Rather, it relies on 'defending forward', a polite term for operating within adversaries' systems:

> Defending forward as close as possible to the origin of adversary activity extends our reach to expose adversaries' weaknesses, learn their intentions and capabilities, and counter attacks close to their origins.[1144]

Far from creating deterrence, such activity could easily be perceived by adversaries as being of aggressive intent; 'defending forward' is certainly a level of activity the US does not accept in its own systems.[1145] There is also a further argument that seeking overmatch may come at an enormous cost to taxpayers and threaten the independence of tech companies; Michael T. Klare argues the pursuit of overmatch in cyberspace could force the tech sector into military-only applications.[1146] The pursuit of 'overmatch' and 'superiority through persistence' were deliberate choices driven by the military's perception that deterrence in cyberspace had failed.[1147] This is understandable given the US experience with successful overmatch. Yet even if the US could achieve overmatch in the capability space, it lacks the required credibility or communication to convert it into successful deterrence in cyberspace. While it is true malicious cyber actors frequently posed threats that law enforcement of diplomatic means could not

[1141] Gen. Paul M. Nakasone, April 2018, 'Command Vision for US Cyber Command: Achieve and Maintain Cyberspace Superiority', United States Cyber Command

[1142] Lebow, Stein, and Canadian Institute for International Peace and Security, 'When Does Deterrence Succeed and How Do We Know?', p.60.

[1143] Ibid

[1144] Gen. Paul M. Nakasone, April 2018, 'Command Vision for US Cyber Command: Achieve and Maintain Cyberspace Superiority', United States Cyber Command

[1145] Klimburg, 'Mixed Signals: A Flawed Approach to Cyber Deterrence', p. 111.

[1146] 'Why "Overmatch" Is Overkill | The Nation', see also Donald J. Trump, December 2017, 'National Security Strategy Of the United States of America', The White House, US

[1147] Gen. Paul Nakasone, Senate Confirmation Hearing, March 2018: Preliminary Remarks 'Nakasone_03-01-18.Pdf', accessed 25 June 2021, https://www.armed-services.senate.gov/imo/media/doc/Nakasone_03-01-18.pdf.

contain without military assistance,[1148] the lack of public constraints or delineation of responsibilities has proved problematic.

5.8 Superiority in a civilian domain

Israel also identified the need for superior capabilities in cyberspace, however from the outset their policies recognised the need for a balanced approach which included civilian entrepreneurship and resilience – requirements more closely aligned with classic deterrence. The Israeli approach to building superiority was part of an ongoing commitment to developing superior capabilities in every sphere in which Israel emphasises its defensive capabilities in the hope it will succeed in showing potential attackers that their chances of success are limited, and that hostile actions are not worth the effort.[1149] It is difficult to overstate the role of the IDF in Israeli society, including in driving strategy, although this is a role that Israeli society largely accepts and agrees with.[1150] Unlike the US, the IDF views the development of capability not as an end in and of itself, but rather as a lever for overall deterrence.

As demonstrated by the case study, developing capabilities alone was not enough for the IDF; the goal was rather the use of capabilities to underwrite Israeli credibility, and communicate messages about Israeli internet and acceptable behaviours, thus contributing to overall deterrence. Participants in this research argued that while cyber technology was a major enabler, it did not fundamentally shift the goals of adversaries – a major consideration for deterrence. Further, Israel views capability superiority (as it does the threats and domain) as an integrated issue not confined to cyber responses to cyber-attacks. Lastly, the drive for superiority largely has whole of nation support, perceived as an essential requirement for Israel's continued successful deterrence in their region where superior technology and capabilities are perceived as successfully deterring neighbouring adversaries in far greater numbers.

Thus although both states defined cyberspace superiority as a necessary policy goal, the construction and use of capability as a requirement for deterrence in each case has been quite different. The US reliance on capabilities and military-led drive for overmatch has not been supported by measures designed to create credibility, or to communicate US intent and expectations clearly. In contrast, participants considered the Israeli pursuit of superiority is part of a broader, well-understood policy approach which supported Israel's ongoing deterrence success.

5.9 Deterrence policy in cybersecurity policy: Two different approaches

The case studies demonstrate that these states held fundamentally different views of the usefulness and role of deterrence theory in cybersecurity policy: Israel viewed theory as arising from practice, while the US held mixed views but largely agreed theory was necessary to inform policy. Yet these differing views

[1148] Gen. Paul M. Nakasone, April 2018, 'Command Vision for US Cyber Command: Achieve and Maintain Cyberspace Superiority', United States Cyber Command, p.2.
[1149] Cohen, Freilich, and Siboni, 'Israel and Cyberspace: Unique Threat and Response', p.310.
[1150] Asher Arian, 1995, *Security Threatened: Surveying Israeli Opinion on Peace and War*, Cambridge Studies in Public Opinion and Political Psychology, Cambridge: Cambridge University Press

had the opposite effect to that which one might expect on cybersecurity policy. As Chapter 3 demonstrated, Israel considered its deterrence approach as unique, cumulative and based on experience. This view was repeatedly raised as in the expert interviews. Participants argued Israel's uniquely practical experience of deterrence meant it understood the practice of deterrence better than many other nations. The Israeli case also revealed a tendency, particularly in the academic community, to evaluate Israeli strategy as operating in contrast with 'Western deterrence' which was described as being unduly influenced by nuclear weapons and the Cold War.[1151] The concept of deterrence in cyberspace being potentially cumulative – as in broader Israeli strategy – has been the subject of several academic papers[1152] that make a contribution to theory.

Thus, while Israeli academics remain sceptical about the role of deterrence theory in policy, this thesis has found that there was evidence both that theory was considered, and that Israel contributed to that theory. Such contributions have important implications for strategy. Israel's cybersecurity strategy has been judged a public success and is unlikely to change substantially in the coming years. Where cyber-attacks occur, they are considered a sign of either needing to respond appropriately – as in the 2019 attack[1153] – or as a sign deterrence needs refreshing, rather than deterrence failure. Although it could be argued the sheer number of attacks suggests otherwise,[1154] the framing of deterrence in cyberspace as a cumulative phenomenon means it would be quite difficult for Israel to judge it a failure. This interpretation of theory influences not only Israeli cybersecurity policy, but also evaluations of its strategy.

The Israeli interpretation is in stark contrast to the US approach. As Chapter 4 demonstrated, the US journey to adopting deterrence theory into cyberspace was driven by theory from the outset. This originated primarily from US academics and designated the nuclear realm as its own form of deterrence, conceptually separate from conventional deterrence.[1155] This had long-lasting implications, because as long as nuclear deterrence prevented nuclear war, it could be judged a success regardless of conflict in other domains.[1156] This non-integrated version of deterrence had a strong influence on the conceptualisation of cyber deterrence, visible in the initial US approaches which sought to confine deterrence activity to cyberspace.[1157] And although several US academics argued against viewing cyber deterrence as a separate concept (notably Jervis and Libicki)[1158], US policy embraced it. The widespread use of 'cyber deterrence' in official US policy, despite the lack of conceptual clarity, unsurprisingly proved

[1151] Bar, 'Israeli Strategic Deterrence Doctrine and Practice', p.329.
[1152] Tor, '"Cumulative Deterrence" as a New Paradigm for Cyber Deterrence'; Bar, 'Israeli Strategic Deterrence Doctrine and Practice'.
[1153] Zak Doffman, 'Israel Responds To Cyber Attack With Air Strike On Cyber Attackers In World First', Forbes, accessed 25 June 2021, https://www.forbes.com/sites/zakdoffman/2019/05/06/israeli-military-strikes-and-destroys-hamas-cyber-hq-in-world-first.
[1154] Cohen, Freilich, and Siboni, 'Israel and Cyberspace: Unique Threat and Response', p. 313.
[1155] Alex S. Wilner, 2020, 'US Cyber Deterrence: Practice Guiding Theory', *Journal of Strategic Studies*, 43:2, 250
[1156] Schelling, *Arms and Influence*. Schelling's Afterword pp.287-303 captures the enormity of conflict post Hiroshima, and the extraordinary non-use of nuclear weapons.
[1157] Obama, 'International Strategy for Cyberspace', p.8
[1158] Martin C. Libicki, Cyberspace in Peace and War, p. 222-224; see also Robert Jervis, Some Thoughts on Deterrence in the Cyber Era, *Journal of Information Warfare* 15:2, 66-73.

problematic and illustrated a broader problem for US cyber strategy – without a clear understanding of what was being deterred or how deterrence theory should apply, the policies developed lacked explicit goals and necessary clarity. This meant reaching any degree of success was quite unlikely given expectations of US deterrence were unreasonably high.

The two case studies elicited different views on theory, which also influenced Israeli and US definitions of deterrence. These then had a direct impact on the construction and implementation of deterrence, and how closely each case's deterrence approach matched the classic deterrence requirements. In exploring the surprising coherence of the Israeli deterrence approach, Chapter 3 argued that despite this approach not being enshrined in policy prior to the 2017 policy, it was well-understood as a pragmatic, whole-of-society requirement. The decision to capture this approach in policy for cybersecurity was remarkable for its completeness against the classic deterrence requirements and its public nature. Notably, this did not represent a substantial shift in the Israeli approach.[1159]

As argued in Chapter 4, the Israeli definition of deterrence in cyberspace includes defined roles for capability, credibility and communication and was operationalised as a cumulative practice necessary for survival. Israel defined its concept of deterrence for cyberspace, operationalised that concept, and then adhered to the resulting strategy. While the support for the Israeli approach is not universal – for instance, Amir Lupovici has noted concerns regarding the prevalence of deterrence in Israeli society[1160] – cumulative deterrence for cyberspace is not a new approach. Indeed, it is an extension of the Israeli approach to deterrence in broader strategy, applied regardless of domain and broadly considered as an essential component of Israel's survival. The acceptance of this approach may indicate deterrence strategies have a better chance of being judged a success where they are based on a practical, multi-domain integrated approach, well understood across academia and society. This may also indicate that a consistent approach is more likely to be judged a deterrence success.

By contrast, deterrence is not well defined for cyberspace in the US, and nor does it have an established long-term role in US strategy outside of the nuclear realm.[1161] Chapters 2 and 4 of this thesis have illustrated that the US academic literature is divided over the applicability of deterrence theory to cyberspace, and US policy and practice – despite repeatedly stating deterrence was the goal – did not at any point have the three elements required for deterrence between 2008 and 2018. The US approach to deterrence in cyberspace was repeatedly revised with competing versions of deterrence policy and differing aims from different areas of the US government. Given that by 2018 the US has judged its own

[1159] Dmitry (Dima) Adamsky, 2017, 'The Israeli Odyssey toward Its National Cyber Security Strategy', *The Washington Quarterly,* 40,:2, 122

[1160] Amir Lupovici, 2016, *The Power of Deterrence: Emotions, Identity and American and Israeli Wars of Resolve*, https://doi.org/10.1017/CBO9781316534540

[1161] See Bruce W. MacDonald 'Strategic Nuclear Policy in a Time of Fundamental Change' in Tritten and Stockton, *Reconstituting America's Defense: The New U.S. National Security Strategy*, pp.105-117 policies a failure, it is clear that poorly defined or inconsistent strategies are less likely to be judged a success.

5.9 Expectations: Shaping policy, influencing 'success'

The radically different expectations of the case studies towards deterrence resulted in significant and lasting implications for deterrence policy and practice; and yet neither has proved a success in terms of deterring cyber attacks. Israel expected its deterrence policy to be repeatedly challenged; the US expected its deterrent to succeed. The Israeli expectation of failure was not seen as a reason to not extend deterrence to cyberspace. Rather the potential for failure was a critical component in shaping policy development in the three-layered approach described in Chapter 3, based on resilience and survival. This expectation of failure is articulated in the 2015 Eizenkot Doctrine, which listed the preparation for expected attacks as the second of five aims for the IDF in cyberspace.[1162] By defining success as survival – rather than prevention of all attacks – and building policy in layers, Israel's approach was able to be perceived as a success even though it still faced ongoing and serious cyber-attacks, sometimes as reprisals for its own actions. Israel's self-proclaimed deterrence success is also, importantly, cross-domain and part of its larger deterrence strategy – a strategy notable for its perceived success despite many attacks across different domains.[1163] Thus the paradox of Israeli deterrence policies in cyberspace is that Tel Aviv views them as successful, whereas Israel's adversaries characterise its behaviour as offensive and escalatory.

In contrast to Israel, the US expected to be able to treat deterrence in cyberspace in a similar manner to deterrence in the nuclear sphere – an approach based initially on denial, expecting to be able to deter all attacks that remained confined to a single domain. Further, the US expected the military to be able to take the lead on deterrence in cyberspace, just as it had in the land, air, sea, and space domains.[1164] These expectations proved to be unrealistic in a relatively short timeframe, with policies unable to deliver on unclear goals. Participants in this research were especially scathing about this disconnect. Participant U7 argued 'rhetoric and outcomes need to be moderated through what actually happened'.[1165] Unrealistic expectations and lack of clarity were also clearly highlighted by Participant U1, who argued deterrence could only be considered effective where there were zero attacks.[1166]

In sum, the US policy approach was neither stable nor founded on a basis of practical experience. Its policies had to evolve to take into account the unexpected continuation and rise in cyber-attacks after initial policies based on strategies of denial failed. And yet this failure was not unexpected. As

[1162] Gadi Eizenkot, August 2016, 'Deterring Terror: How Israel Confronts the Next Generation of Threats', Belfer Center for Science and International Affairs
[1163] Jean-Loup Samaan, 1 May 2014, 'From War to Deterrence? Israel-Hezbollah Conflict Since 2006', Fort Belvoir, VA: Defense Technical Information Center, p.484
[1164] Ibid
[1165] See Participant U7, Chapter 4
[1166] See Participant U1, Chapter 4

Will Goodman argued in 2010, denial was not in itself sufficient to deter aggression in cyberspace.[1167] And the shifting emphasis to deterrence by punishment, and later to persistent engagement and 'defending forward' with the intent of deterring attackers through offensive measures, demonstrates that US elites had indeed found this approach unworkable. Yet in 2016 the International Institute for Strategic Studies was still arguing deterrence by denial could be more viable than deterrence by retaliation.[1168] As demonstrated in Chapter 4, the US reliance on capabilities and then overmatch at the expense of credibility and communication meant that two of the three deterrence requirements were not present in US policy from the outset.

The deep academic divide in this space also reveals an important truth for the US: that unrealistic expectations led to repeated shifts in its deterrence approach to cope with perceived failures. This helps explain how Israel's cyber strategy has been published once, and is widely considered a success, despite shifting technologies, ongoing cyber-attacks, and a changing international environment. It may also indicate that where states base deterrence strategies for cyberspace on a model which factors in an expectation of engagement, they are potentially more likely to judge their efforts a success.

5.10 Deterrence by any other means? The classic deterrence requirements

A reasonable expectation at the outset of this project would have been that Israel's approach was too reliant on offensive measures to meet the requirements of classic deterrence. But despite differing from the US approach to deterrence in terms of implementation, Chapter 3 demonstrated that it is possible to identify sufficient evidence from the Israeli case to meet a definition of classic deterrence between 2008 and 2018. The decision to construct public deterrence policy documents describing this approach for cyberspace is remarkable given Israel's historic reticence to publish policy on any issues related to national security or strategy, and provides several insights into how Israel had managed to create a holistic deterrence approach. The four pillars of Israeli defence were well understood; capturing these in public policy had not been judged necessary. However as argued in Chapter 3, Israel's decision to release multiple government resolutions, a specific cybersecurity strategy[1169], defence doctrine[1170], as well as numerous high-level government statements[1171], all specifically aimed at creating deterrence indicates a new commitment to transparency. These efforts, combined with multiple swift kinetic responses to cyber-attacks[1172], indicate Israel considered it necessary to make an unusual effort to communicate its deterrent intent in cyberspace.

[1167] Goodman, 'Cyber Deterrence: Tougher in Theory than in Practice?', 108.
[1168] 'Cyber Conflict and Deterrence', 2016, *Strategic Comments* 22:7, iii–v
[1169] 'Israel National Cyber Security: In Brief', September 2017, State of Israel
[1170] Gadi Eizenkot, August 2016, 'Deterring Terror: How Israel Confronts the Next Generation of Threats', Belfer Center for Science and International Affairs
[1171] PM Netanyahu 'background for establishing the bureau'.
[1172] Tabansky, Lior, 'Israel's Cyber Security Policy: Local Response to the Global Cybersecurity Risk', in *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications*, 2018, 1125–45, https://doi.org/10.4018/978-1-5225-5634-3.ch054.

Israel's commitment to achieving and maintaining its superiority edge, as well as degrading the capabilities of its adversaries, also indicated a significant commitment to developing capabilities. Its willingness to use force, often pre-emptively, fits within a classic deterrence definition of an actor attempting to convince another that the probable cost would exceed the anticipated gain.[1173] In contrast, given its academic leadership on deterrence theory, I initially expected to find that US policy would easily meet the requirements of classic deterrence. However as Chapter 4 demonstrated, the US only met one out of the three requirements at any one point over the period under investigation. Despite a plethora of public policies, the US has evidently struggled to create a cohesive deterrence approach.[1174] The substantial differences between the approaches of the two case studies toward the classic deterrence requirements provides significant insights into the relative importance of each measure individually and as a whole. I now turn to considering how the policies of the two case studies could be argued to support each measure, before considering the implications for cyber strategies and theory.

5.10.1 Capability

The case studies showed that both Israel and the US have understood the importance of capabilities for deterrence, and both have dedicated significant resources into building and maintaining capability superiority. Although both did so with explicit deterrent aims, the fundamentally different reasons for developing these capabilities resulted in different definitions and uses of capabilities, and ultimately differing views about their perceived respective successes.

The US preoccupation with 'capabilities' resulted in the drive for superiority, and then overmatch, as discussed earlier in this chapter. However this came at the expense of the other deterrence requirements, did not produce the desired deterrence outcomes, and was frequently misunderstood. Participant U3 argued that although the US had access to range of capabilities, it frequently constrained itself unnecessarily to cyber responses; he argued this was dangerous.[1175] Participants further argued that the lack of agreement on what comprised capabilities, and how they could – or even should – be used. Participant U2 argued the use of capabilities had not proved an effective deterrent, using the example of Iran.[1176] These concerns were echoed in the academic research, but from widely differing viewpoints. David J. Lonsdale has argued the use of capabilities by the US had been so insufficient that the US should instead pursue warfighting in cyberspace,[1177] while Libicki has claimed that the relative cheapness of

[1173] If deterrence is the attempt by states to convince another actor not to act, then the Israeli policy could be argued to more closely fits a definition of compellence. However as noted in Chapter 1, the distinction between deterrence and compellence is often difficult to establish, particularly in an environment where engagement is ongoing – and cyberspace has proved such an environment. See also Lebow, Stein, and Canadian Institute for International Peace and Security, 'When Does Deterrence Succeed and How Do We Know?' p.10.

[1174] Ewan Lawson, 2017, 'Deterrence in Cyberspace: A Silver Bullet or a Sacred Cow?', *Philosophy & Technology*, 31:3, p.432

[1175] Participant U3, Chapter 4

[1176] Participant U2, Chapter 4

[1177] David J. Lonsdale, 2018, 'Warfighting for Cyber Deterrence: A Strategic and Moral Imperative', *Philosophy & Technology,* 31:3, 410-412, https://doi.org/10.1007/s13347-017-0252-8 operational cyberwar capabilities make them worth developing.[1178] The military seemed to reflect this view, and through Cyber Command began a major drive to building and maintaining capabilities. But as demonstrated in this thesis there was a recognised disconnect between US rhetoric on its capabilities and the actual responses, and several participants highlighted concerns that the shift towards using offensive capabilities under the doctrine of persistent engagement was normalising dangerous behaviours.[1179] Further, the US proved reluctant to use its capabilities, something that some participants viewed as a key risk. Participant U6 argued the US needed to be more active, including 'where it involves offensive action to take down someone else's capabilities'.[1180]

The Israeli approach to capability also prioritised the development of options to overwhelm adversaries, but from the outset, these options were diversified. Israel spent significant effort and resources to build a strong public private partnership for cyberspace.[1181] It invested in military superiority, including but not limited to cyber capabilities.[1182] It put significant effort into consistently reforming its governance to centralise control and ensure consistent messaging. However, as Chapter 3 highlighted, none of these decisions or behaviours were unique to Israel. Rather they reflect Israel's broader strategy of using the best responses available, regardless of the vector of attack.[1183] Thus the stated priorities of the IDF are unsurprising: to establish a cyber arm; build cyber capabilities; plan and implement combat in cyberspace; and develop technological capabilities for cyber defense of all operational systems and defense capabilities of the support system[1184]. Further, unlike the US, Israel viewed demonstrations of capabilities – such as responding to attacks – as a critical requirement for deterrence. As Doran Almog argued, cumulative deterrence was based not just on threats, but the use of military force.[1185] Indeed, case study participants overwhelmingly agreed that the use of force, not just threats, was essential for protecting Israeli interests: 'you can deter any type of attack if you are prepared to retaliate heavily'.[1186]

Even in the use of capabilities, however differences in the Israeli approach are visible. This is apparent, for instance, in a description of rationales behind capability development by Participant I3:

> Whatever you do, you are never able to defend everything, so build your capability to defend. To make sure the event does not happen. Build your capability to manage when it happens. And now build your capability to recover.[1187]

[1178] Martin C. Libicki et al., 2009, *Cyberdeterrence and Cyberwar*, Santa Monica, CA: RAND
[1179] Participant U5, Chapter 4
[1180] Participant U6, Chapter 4
[1181] 'Israel National Cyber Security: In Brief', September 2017, State of Israel
[1182] Bar, 'Israeli Strategic Deterrence Doctrine and Practice', p. 350
[1183] Participant I7, Chapter 3
[1184] Gadi Eizenkot, August 2016, 'Deterring Terror: How Israel Confronts the Next Generation of Threats', Belfer Center for Science and International Affairs
[1185] Almog, 'Cumulative Deterrence and the War on Terrorism'.
[1186] Participant I1, Chapter 3
[1187] Participant I3, Chapter 3

This view of capabilities as a layered response, designed for strength but with the underlying principle of resilience and recovery, demonstrates the Israeli expectation that their deterrence in cyberspace is likely to fail at some point. Thus while deterrence is important, it is not the end goal of strategy.

5.10.2 Credibility

The findings of this thesis reinforce the argument that while credibility is one of the most critical deterrence requirements, it also one of the most difficult to establish.[1188] Only one of the two cases, Israel, made significant efforts to establish credibility in its deterrence approach in cyberspace. As Chapter 3 showed, Israel's conception of cumulative deterrence meant that credibility has long been prioritised in its strategy, and cyberspace is no exception. Perhaps the most obvious example of Israel's attempts to enhance its credibility is its willingness to attribute and respond to cyber-attacks, particularly with kinetic means. The decision to respond to cyber-attacks with overwhelming force is a deliberate one, designed to 'remove hope from the mind of the enemy'.[1189] It is also a carefully managed approach, with not all attacks being attributed, or responded to publicly. Israel's willingness to participate in strategic ambiguity has not damaged its credibility but rather helped build the Israeli response mystique. The 'wink and nod' method of unofficially claiming responsibility, while being able to escape any consequences is a method of plausible deniability it has used in many other spheres, such its likely contribution to the Stuxnet attacks or participation in unattributed political assassinations more broadly.[1190]

The US has not made many explicit or implicit attempts at establishing credibility. Although US policy states that there would be consequences for those conducting cyber-attacks on their interests or those of its allies[1191], the US has repeatedly failed to deliver consequences for attacks. For example, in December 2014 a cyber-attack was conducted on a major US health insurer, with 80 million records being accessed.[1192] Although the breach was discovered in January 2015, it was not until 2017 that state insurance commissioners announced that a nation-state was behind the attack and it was not until 2019 that the US Department of Justice charged a single Chinese person.[1193] For an adversary, it would seems apparent that the gap between the attack becoming known and the response occurring is so lengthy as to not be a deterrent. Further, when the response occurred – five years later – it was only targeted at an individual, not a state. An adversary viewing such an example would likely determine that the cost-benefit calculation was in favour of continued attacks, rather than non-action.

[1188] Goodman, 'Cyber Deterrence: Tougher in Theory than in Practice?', p.107
[1189] Participant I3, Chapter 3
[1190] This program of political assassinations is well-documented: see Ronen Bergman and Ronnie Hope, *Rise and Kill First: The Secret History of Israel's Targeted Assassinations*, (New York: Random House, 2018), https://go.exlibris.link/WNWMSLdk.
[1191] 'Summary of the 2018 National Defense Strategy of The United States of America: Sharpening the American Military's Competitive Edge'. Barack Obama: 2015 Media Statement
[1192] Virginia Greiman, 2021, 'The Politics and Practice of Cyber Attribution: A Global Legal Perspective', in *International Conference on Cyber Warfare and Security*, Reading, United Kingdom: Academic Conferences International Limited, p.103
[1193] Ibid

The US emphasis on collective attribution further slowed responses and created an artificial sense of the level of proof required to impost consequences. The US approach – aimed to be proportionate and using like-for-like responses – was described by research participants from both case studies as a major cause of US credibility failure. The claim that the US would 'deter malicious cyber activities with integrated strategies that impost swift, costly and transparent consequences when malicious actors harm the US or our partners'[1194] was not realised between 2008 and 2018. This was the case with NotPetya, whereby the US response to a 2017 attack that paralysed healthcare, transport and other systems around the globe to an estimated cost of $10 billion was a collective attribution that was not made public until February 2018. Whereas the US promised the attack would be met with 'international consequences'[1195] and yet there were no visible consequences until the US Department of Justice issued an indictment against six individual Russian military intelligence officers – over three years after the attack.[1196]

The difficulty of establishing credibility – and to some extent communication – in cyberspace is further illustrated by the complex and contradictory relationship each case study exhibited towards with norms. The role of norms in Israel and the US provides insight into each state's expectations, including how realistic these were. Both cases have repeatedly used offensive cyber measures and capabilities on adversaries in ways they do not consider acceptable against their own interests.[1197] By arguing for norms that restrain behaviour, and then contravening them, both cases undercut their deterrence stance. The effect was most significant for the US, where it was more obvious that US behaviour was in direct contravention of its own stated norms, whereas the Israeli approach of strategic ambiguity provided a great deal more flexibility. While both cases made explicit (and in the case of the US, substantial) policy commitments towards the creation and maintenance of international norms in cyberspace regarding acceptable activities between 2008 and 2018, neither have abided by the norms that they argued other states should follow. These measures, far from creating or enhancing deterrence, created a new norm of engagement in cyberspace which potentially risks unintended escalation.[1198]

5.10.3 Communication

Given the visible inconsistencies in US public policy on cybersecurity strategy described in Chapter 4, it is perhaps unsurprising that research participants also judged US communication attempts as incomplete, and thus not able to meet the classic requirements of deterrence. The major policy pivot from deterrence to 'persistent engagement with deterrent aims' represented a significant shift in government focus, yet in the same year US Cyber Command had argued it was unable to achieve its strategic intent because it did

[1194] Donald J. Trump, December 2017, 'National Security Strategy of the United States of America', The House, US, p.13

[1195] Steven Nelson, 'White House Accuses Russia of NotPetya Cyberattack, Threatens Unspecified "Consequences"', Washington Examiner, 15 February 2018, sec. Politics

[1196] Charlie Mitchell, 'U.S. Indictment of Russian Intelligence Officers Reflects First Culpability for Devastating "NotPetya" Attack', *Inside Cybersecurity,* 20 October 2020

[1197] Kaplan, *Dark Territory: The Secret History of Cyber War.*

[1198] Wilner, 'US Cyber Deterrence: Practice Guiding Theory'.

not have sufficient support from other US agencies. If messaging is (as Participant U7 argued) fundamental to deterrence[1199] then the US is not well-positioned to accomplish it. Further, as well as inconsistent policy, US messaging was also inconsistent. For instance, Participant U4 claimed this was partially due to many involved parties not having a complete or accurate understanding of terminology, and confusion over the difference between cyber-crimes, cyber vandalism and cyber war.[1200] Participant U6 noted that such confusion could at times represent a serious enough problem to lead to a strategic communication error, and likened the resulting view of the US to a 'bull in a china shop'.[1201] Overall, the research revealed that the US was still struggling with building consistent messaging between government agencies on the domestic stage. It had not managed to create or maintain consistent messaging to allies, let alone adversaries. Further, US messaging was undermined by its actions in other nation's networks, such as through the Operation Olympic Games suite of cyber offensive actions against Iran.[1202]

The Israeli approach provided an interesting contras to this experience. As discussed in Chapter 3, Israel's efforts to record and publicise its deterrence approach for cyberspace were inconsistent with Israel's strategic history and represented an ostensible shift towards clarity and transparency. Further, the number of government resolutions and public statements it issued seemed to indicate that Israel saw the need to communicate its intentions and expectations in cyberspace. These statements, coupled with swift, kinetic responses to transgressions represent a significant effort towards creating an effective suite of communication measures.

The logical question that follows here is that if Israel's communication was so effective, why were its adversaries not deterred? One of the key issues with Israel's approach is its reliance on offensive measures. The use of disproportionate force has been named by other states as setting a precedent, and media reporting on the 2019 response to Hamas cyber-attack labelled it a world-wide precedent for a state responding to a cyber-attack with kinetic force.[1203] However within Israel the event was not perceived in the same way. Rather it was considered by strategists and research participants to be an unremarkable extension of Israel's broader deterrence strategy. Indeed, many participants were bemused by the public narrative around this event: the overwhelming response when asked if this event set a new precedent was that this was just standard Israeli procedure. This demonstrates the danger of strategists and states attempting to judge the efficacy or impact of another state's behaviour, as what one state views as a major new precedent, another considers as ordinary business.

[1199] Participant U7, Chapter 4
[1200] Participant U4, Chapter 4
[1201] Participant U6, Chapter 4
[1202] Jon R. Lindsay, 'Stuxnet and the Limits of Cyber Warfare', Security Studies 22, no. 3 (2013): 365–404
[1203] Gross, 'IDF Says It Thwarted a Hamas Cyber Attack during Weekend Battle'; 'What Israel's Strike on Hamas Hackers Means For Cyberwar | WIRED', accessed 25 June 2021, https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/; 'Israel Sets Precedent by Launching Air Strike against Hamas Hackers', accessed 25 June 2021, https://www.scmagazine.com/home/security-news/israel-sets-precedent-by-launching-air-strike-against-hamas-hackers/.

Both Israel and the US described their policy approaches as being explicitly designed to create deterrence in cyberspace. But the underlying expectations and context for each case was quite different, and examining deterrence policies outside of these contexts is potentially misleading. Examining the two cases against classic deterrence theory revealed that Israel's approach could be argued to meet a definition of classic deterrence, with clearly identifiable capability, credibility and communication measures. By contrast, the US policy approach had visible capability measures, but had not managed to establish credibility or communication – and arguably would not meet such a definition.

5.11 Unplanned escalation, unintended consequences: Stuxnet

The case of Stuxnet is often used to make arguments for or against taking offensive action in cyberspace, or the ways states can use cyber harms to cause kinetic harm. However Stuxnet was far more than significant and with broader-reaching implications. Stuxnet was a worm (a piece of malicious software, or malware) directed at Iran's nuclear processing facility in Natanz.[1204] An ambitious and damaging attack, the worm operated by sending messages to Iranian centrifuges to spin out of control and damage themselves while simultaneously sending code to the relevant control panels indicating normal operation.[1205]At the time Stuxnet became public, it was estimated to have set back the Iranian nuclear program by around three years.[1206] However the reality of Stuxnet is far more interesting, and illustrates how it shaped both Israeli and US approaches to deterrence in cyberspace.

As Fred Kaplan has pointed out, the decision by the US to use a cyber weapon in preference to a conventional attack was due to the Bush administration in 2006 being unwilling to become engaged in a third Middle Eastern conflict.[1207] The US had the close cooperation of the Israeli cyber unit 8200.[1208] And although the program of cyber capabilities (known as Olympic Games) was approved by Bush, the decision to use it against Iran was made by then President Obama, who viewed it as a way for the US to take action without costing the lives of American troops.[1209] Importantly, Olympic Games was not meant to cause such catastrophic damage that it became public. On the contrary, the code was designed to cause damage in such a way that the Iranians would not be able to trace the cause. By early 2010 nearly one-quarter of Iranian centrifuges were damaged beyond repair, Iran was unaware of the cause, and Stuxnet continued causing stealth harm until the worm escaped in 2011.[1210] Once the worm was identified as malware, Obama ordered the maximum possible damage to be enacted before Iran could remove it from its systems.[1211]

[1204] William J. Broad, John Markoff, and David E. Sanger, 2011, 'NYT: Israeli Test on Worm Called Crucial in Iran Nuclear Delay – Council on Foreign Relations'
[1205] Ibid
[1206] Ibid
[1207] Kaplan, *Dark Territory: The Secret History of Cyber War*, p.204-5.
[1208] Ibid, p. 207.
[1209] Kaplan, *Dark Territory: The Secret History of Cyber War*, p.208.
[1210] Ibid, p. 211.
[1211] Ibid, p. 211.

The risk for the US attempts at deterrence was that this activity meant it was the US that conducted the world's first known cyber-attack on another nation's critical infrastructure. Once it became public, this attack did significant damage to US credibility and established a new norm, the consequences of which were fairly immediate.[1212] In 2012, an attack known as Flame (based on the same NSA virus from which Olympic Games was derived) wiped the hard drives at Iran's Oil Ministry and the National Iranian Oil Company.[1213] Four months later, Iran launched the Shamoon virus, which wiped every hard drive at Saudi Aramco, a joint US-Saudi oil company. Kaplan argues it was the Stuxnet and Flame attacks that spurred Iran to create a cyber war unit, and that the Shamoon attack was part of its initial response.[1214] If his assessment is correct, then the pre-emptive use of Stuxnet may have temporarily reduced Iranian nuclear capabilities, but it did not deter Iran from seeking to replace them. Nor did it deter Iran from acquiring and using cyber capabilities against the US and its allies.[1215] Kaplan alleges President Obama was concerned about the risk of the Stuxnet worm escaping its intended target system and causing harm to civilian infrastructure. But perhaps he should have been more concerned about the potential for escalation, for Iran to use this attack as justification for its own drive to build and use cyber capabilities. Further, although Israel never openly admitted to participating in Stuxnet, its involvement arguably led directly to Israel's focus on increasing cybersecurity after 2012.[1216]

5.13 Judging 'success'

As outlined in Chapter 2, ascertaining the success of a state's policies in deterring attacks against it in cyberspace is complex. However it is possible to examine how effective states judge their own policies to be, and consider these judgments against practice. Here, US policy developments in 2017–18 clearly indicate that US policymakers had judged deterrence a failure. The 2018 Cyber Strategy gave the following conception of success:

> The Strategy's success will be realized when cybersecurity vulnerabilities are effectively managed through identification and protection of networks, systems, functions, and data as well as detection of, resilience against, response to, and recovery from incidents; destructive, disruptive, or otherwise destabilizing malicious cyber activities directed against United States interests are reduced or prevented; activity that is contrary to responsible behavior in cyberspace is deterred through the imposition of costs through cyber and non-cyber means; and the United States is positioned to use cyber capabilities to achieve national security objectives.[1217]

This paragraph in the strategy is remarkable because it lists four measures of success: vulnerabilities managed and responded to; activities against the US are reduced or prevented; cost imposition prevents

[1212] Ibid, p. 212.
[1213] 'Meet "Flame," The Massive Spy Malware Infiltrating Iranian Computers | WIRED'.
[1214] Kaplan, *Dark Territory: The Secret History of Cyber War*, p. 213.
[1215] Ibid, p. 214.
[1216] Ibid
[1217] 'National Cyber Strategy of the United States of America', September 2018, The White House, p.3

activity contrary to interests; and the US is able to use cyber capabilities. The inclusion of these four measures indicates markers for success that the US has not yet met.

In contrast, Israel has defined success very differently. According to its 2017 Strategy:

> Israel's national cyber security strategy is, first and foremost, a means of realizing the Israeli cyber vision by keeping cyberspace safe and by confronting the various cyber threats, in accordance with the country's national interests. In addition, the strategy aims to ensure Israel's continuing role in the international arena, as a leader in technological innovation and as an active partner in the global processes of shaping cyberspace.[1218]

As detailed in Chapter 3, Israel's definition of successful deterrence differed from the US. For Israel, deterrence is not a theory – rather, it is state practice that is widely accepted because of its perceived role in the survival of the Israeli state.[1219] Participants repeatedly characterised deterrence as part of Israeli identity and pointed to the existence and survival of the Israeli state as proof that Israel's deterrence was successful.

The contrast with the US was stark. The US experts participating in this research noted the significant impact of the Cold War and argued that policymakers had tended to view US cyber deterrence through the nuclear deterrence lens, and this led to unrealistic expectations of deterrence. Participant U5 claimed this was because 'the dishonest ones say it's just like nuclear, and the honest ones say the differences are just too many'.[1220] So how can Israel consider its deterrence approach in cyberspace a success even though cyber-attacks are ongoing? The answer lies in the fact that Israel has extended its holistic view of deterrence to cyberspace, and if we accept cumulative deterrence as a variation or operationalisation of classic deterrence, then its policy and practices can be argued to have met that definition, and the operationalisation of the theory matches Israel's operationalisation of deterrence elsewhere. This should not therefore come as a surprise to adversaries. Further, deterrence is not a static position or point in time. It is a relationship between parties, and relationships must necessarily change and evolve as circumstances change.

5.14 General findings: Implications for deterrence theory

At the point we can offer some general findings for deterrence theory based on its two case studies. It is important to recognise here that as this field of research is relatively new, many of these findings are preliminary. Further research is required both into the practices and policies of these two cases beyond 2018, and into other cases over the time period in order to generate more data. Future research may also wish to consider other methods of considering the practical implications of the adoption of deterrence into cybersecurity policies as additional information enters the public domain. With that caveat, this thesis

[1218] 'Israel National Cyber Security: In Brief', September 2017, State of Israel

[1219] Adamsky, 'The Israeli Odyssey toward Its National Cyber Security Strategy'.

[1220] Participant U5, Ch. 4

has found evidence to support the contention by strategists like Goodman, Healey and Jervis[1221] that states will behave in cyberspace the same way they behave in any other arena: indeed, that cyberspace allows states to engage with each other through new avenues but it does not change the fundamental goals or behaviours of states.

The thesis has also found that in the cases of Israel and the US, both had defined and adopted deterrence with substantial reference to their historical experiences of it, which may indicate that other states will do the same. As demonstrated in the case studies, this produced substantially different policy approaches, particularly the definition of success that each case adopted. The Israeli experience of deterrence as an iterative process with a goal of survival produced a policy approach focused on resilience and punishment, rather than prevention of all attacks or deterrence by denial. This shaping of Israel's approach through an expectation that deterrence would fail (even many times) and yet could still be considered an overall success could lead to a view that states that define resilience as success, rather than zero-sum, are more likely to judge their efforts successful. Further, the resulting approach supports an argument that deterrence can reduce harm but not prevent it entirely, suggesting that reliance on any one theory is unlikely to be effective. It is also worth noting that while participants viewed Israel's deterrence approach as successful, they by no means considered it as complete, or static. Participants were forthright about the risks and difficulties of trying to understand how deterrence was operating in cyberspace. Further, they noted the difficulty of evaluating deterrence in one domain rather than as an integrated whole. Thus deterrence is very much a process, a relationship, rather than a fixed goal.

In contrast, the case study of the US also demonstrated a deeply influential historical experience with deterrence, but this manifested in a significantly different policy approach. The US experience of deterrence during the Cold War led to the expectation that deterrence in cyberspace would be successful, and that the US could create an environment where they could deny adversaries their goals. Further, the case study material indicated the US approach relied heavily on developing overwhelming capability and did not give sufficient attention to the requirements of credibility or communicating their intent clearly. The US judged their deterrence as having failed. This supports an argument that incomplete application of a theory may make it more likely to judge the theory as having failed, rather than the policies application being poorly designed or incompletely applied.

By 2018 both cases faced increasingly capable and motivated adversaries, and yet neither had seemingly managed to deter attacks against their interests in cyberspace. Despite both Israel and the US having quite different policy approaches, the policies of both states relied on capability superiority as a pillar of their deterrence. This reliance meant both states were engaged in building and using offensive cyber capabilities for ostensibly deterrent purposes – and yet if the intent was to deter cyber-attacks, nether state succeeded.

[1221] Will Goodman, 2010, 'Cyber Deterrence: Tougher in Theory than in Practice?', *Strategic Studies Quarterly*, Fall 2010, 102-35; Jason Healey, 2019, 'The Implications of Persistent (and Permanent) Engagement in Cyberspace', *Journal of Cybersecurity,* 5:1); R. Jervis, 2016, 'Some Thoughts on Deterrence in the Cyber Era', *Journal of Information Warfare,* 15:2, 66-73

This seems to indicate that states relying on offensive capabilities and capability superiority to create deterrence might instead be risking escalation.

5.15 Conclusion

While Israel's deterrence policies and practices are consistent across domains, their operationalisation has required the use of overwhelming and often kinetic means. The risk of such an approach is that deterrence which relies on overwhelming force, particularly via pre-emptive strikes, can easily be misunderstood by adversaries. This issue is recognised by the IDF, which has been continually seeking a balance between responses which are proportionate enough to cause severe damage and deter future attacks, but not so disproportionate that they trigger a larger conflict.[1222] Where responses to cyber-attacks are kinetic, the adversary could easily construe Israel's intent as an overly aggressive response which is designed to prepare the battlespace for war, or even as an act of war. The public narrative from Iran would certainly seem to indicate that it treats Israel as an active adversary. Regardless of whether this public perception is accurate for either Israel's intent, or Iran's status, the pre-emptive/offensive actions by Israel in response to Iran's cyber-attacks allows Iran a potentially effective self-designation as a victim. This could also lead to offensive activity escalating, as each side can claim they are merely responding to the other. Although outside the period of analysis, from 2018–2020 the Israeli–Iranian relationship has demonstrated an escalating pattern of conflict, particularly in cyberspace. Importantly however, the choice to allow and indeed encourage this narrative is a deliberate policy choice by Israel.

The risks engendered by the US approach are similar, in that its policy practices could be misinterpreted and lead to escalation. However, the US has reached this position of risk not by deliberate intent, but through an incomplete application of deterrence theory and the resulting perception of failure. It is the perception that deterrence has failed, and the resulting move towards persistent engagement that is causing risk. There are several reasons for this. First, the definition of persistent engagement and why it was created to replace deterrence is not clearly understood by either academia or policymakers. Second, the aims of persistent engagement as a policy direction are not clear. Persistent engagement is claimed to potentially add to deterrence, but this approach exists because deterrence had been judged a failure in cyberspace. It is not clear how the US expects persistent engagement to contribute to deterrence, if at all. And this uncertainty and failure to communicate aims or intent is a critical failure. One could also argue that the US, having publicly declared that deterrence was not creating the desired effects in cyberspace, then lacks credibility for attempts to create deterrence through increased engagement. It is risky to declare a strategy has not worked and then attempt to introduce a new approach to try and produce effects it had previously declared were not possible. Persistent engagement as a policy approach accepts ongoing activity, which seemingly mirrors the Israeli approach of conceptualising success not as the absence of attacks, but rather resilience to ongoing attacks.

[1222] Yaakov Katz, 4 August 2010, 'Israel's deterrence needs a boost', *Jerusalem Post*

By exploring the approaches of the two case studies to deterrence in cyberspace this research found deterrence as a theory is not contested. Indeed, its requirements are generally agreed upon and understood. But implementation of that theory varies widely, and evaluations of success depend entirely on context and definitions of success. Thus, how states define the problem space, and deterrence as a solution to that problem, will influence how states define and design policy for cyberspace.

Chapter 6 Conclusion

6.1 Findings

This thesis began with the question: why do states employ deterrence theory as part of their efforts to secure their interests in cyberspace, how successful have they judged doing so? It found that despite substantial divisions in the literature on the applicability of deterrence for cyberspace, policymakers had adopted deterrence approaches and that this application, particularly the rapid expansion in security strategies for cyberspace after 2007, provided a rich field of data. By narrowing the field to major states that had explicit deterrence goals, faced significant cyber threats, and had advanced their strategic policy in this domain, I considered the extent to which having deterrence goals had been translated into deterrence strategy and policy. By bounding the research to two states with significantly differing geostrategic circumstances – the US and Israel – within a timeframe between 2008 and 2018, the thesis has sought to consider not only the strategic context for each state but also their historical experiences with deterrence. This has included how their experiences influenced expectations of deterrence, focusing in particular on definitions of success and implementation in policy for cyberspace. And by considering the approaches of the two cases against not only their own policy rhetoric but the framework of the basic agreed requirements for a deterrence strategy – namely capability, credibility and communication – the thesis has examined whether the US and Israel actually had a deterrence strategy, before considering perceptions of its success.

In examining the question of the extent to which states employing deterrence as a cyberspace strategy considered it successful, this research found that after ten years of deterrence efforts and different policy approaches, both states still had active adversaries in cyberspace, and both have increased their efforts to protect their respective state and societal infrastructure. In the US case, deterrence was perceived as a failure due to incomplete construction and implementation of classic deterrence requirements. The thesis found that while the US had deterrence as a declared policy goal and made repeated references to its deterrence approach throughout national security strategies and specific cyber policies until late 2018, its approach could not be argued to meet more than one of the three basic deterrence requirements. Influenced by its experience during the Cold War, the US developed and maintained a significant commitment to capabilities for cyberspace, including offensive and defensive capabilities. Despite being arguably the world leader on deterrence scholarship, the US did not apply the same level of effort towards creating an approach that included credibility or effective communication.

Indeed, the US emphasis on being able to behave as it chose in cyberspace while limiting the activities of others undercut its moral credibility; the decision to conduct attacks on other states (such as the Stuxnet attack) may well contribute towards an escalating cyber arms race. Further, the US response to cyber-attacks during the period was not only inconsistent, it lacked visible timely responses, and attacks were thus seen as a cost-free way of damaging US interests. The reliance on collective attribution and the provision of publicly available evidence for attribution led to the US making attribution some months after attacks, if at all. The failure to impose consequences is a critical requirement for credibility, and one the US repeatedly failed to deliver despite policy statements to the contrary. Lastly, the US struggled to create or maintain a coherent communication plan on its intent for cyberspace. Its commitment to international rules and norms was undercut by its behaviours. In contrast, its public strategies were largely focused on illuminating the problem, not creating or publicising US solutions or intentions.

6.2 Implications

These findings have implications both for the states examined and their future policy direction, and for deterrence as a practice more broadly. The US perception of deterrence as a failed strategy and subsequent public commitment to persistent engagement instead is problematic. The US declared deterrence approach did not achieve US goals of making cyberspace more secure or reducing cyber-attacks. But the US experience was not a fair test of deterrence in cyberspace, as the decision to move away from deterrence is based on incomplete data. Even if the US had developed a more complete deterrence strategy through a balanced policy approach its inability to accept resilience as a goal, rather than prevention of cyber-attacks, makes it likely the US would still have judged such a strategy a failure. The US fundamentally expected its deterrence to be successful in a similar way to its self-perceived 'success' in nuclear deterrence. The realisation this was not the case (and nor was such success likely to be achievable in cyberspace) contributed to the narratives of fear, black swan events, and the potential for a 'cyber-Pearl Harbour'.

The resulting shift in US policy towards statements increasingly emphasising offensive power and superiority as the answer are dangerous. Without corresponding measures of credibility and communication, both partners and adversaries are left wondering about what the US will do next. The policy of persistent engagement is intended to have 'deterrent effects'; and yet the policy itself is neither well understood nor clearly communicated. In the US context it is not clear what 'deterrent effects' means, nor how it could be judged. The US move away from deterrence in cyberspace as a strategic approach is also likely to influence other states, either because they accept the argument that deterrence does not work in cyberspace, or because they have less incentive to try given that the US has moved away from deterrence.

In contrast, the Israeli approach also has significant implications for the future of deterrence in cyber policy, but for very different reasons. As argued in the case study, Israel's approach did contain the required elements for a deterrence strategy and is considered by the Israeli government as a success, despite it seemingly not actually deterring cyber-attacks. While Israel terms such acts part of its deterrence posture, it is clear other states do not interpret such actions as deterrence, but rather as offensive activities and at times, as acts of war. The potential risk for escalation is clear. Israel's operationalisation of that strategy however is something that few, if any, states would wish to emulate given the entrenched reliance on offensive and pre-emptive measures. Israel's perceived success comes at a significant cost; it has required ongoing government effort; and yet may still have triggered an arms race with Iran. At the very least, Israel's approach has encouraged other states to increase their cyber capabilities. At worst, Israel's use of kinetic force in response to alleged cyber-attacks sets alarming precedents for the future of cybersecurity.

These cases demonstrate that when considering success, states are more likely to judge their efforts as successful when their goals are clearly defined and grounded in resilience rather than in zero sum conceptions of success. Further, when state policies and practices meet the three minimum requirements of capability, credibility and communication – that is, the closer they are to mirroring deterrence theory – the more likely they are to be considered effective. The cases also demonstrate the importance of operationalization being consistent with existing policy, noting that comparisons are fraught due to the lack of agreed definitions. Lastly, deterrence will continue to be judged a failure if judged in only one domain.

6.3 Implications for theory

The thesis also makes several findings for the future role of deterrence theory in cyberspace that may be interest to scholars and policymakers alike. First, as demonstrated in the case of Israel, states may be more likely to consider their own deterrence efforts successful when goals are clearly defined and understood as being grounded in resilience to attacks, rather than in their prevention. Second, states may be more likely to consider their approaches successful when they contain at least the agreed minimum requirements for deterrence. Third, it is not just the policy approach alone that is important: states also should consider how such polices will be operationalised. The measures taken to create deterrence should be carefully considered, particularly in relation to the norms their behaviours might be creating. Fourth, despite the widespread use of the term deterrence, there is a temptation to define it to mean different things. Finally, despite the US judging its deterrence approach a failure, and Israel judging it to be a success, neither state has managed to deter cyber-attacks on their national interests. But this finding does not necessarily translate to deterrence being unsuitable for cyberspace. Rather it indicates that far from adopting deterrence as part of a carefully developed theoretical approach, the states examined both used deterrence as a branding exercise to justify behaviours they had already determined were in their national interests. Thus the cases do not demonstrate that the theory had failed. They demonstrate that the theory is merely only one part of states decision-making. Deterrence should thus be judged as a strategy, against strategic goals set by states.

6.4 The future of deterrence in cyberspace

This research aimed to explore the behaviours of states attempting to improve security in cyberspace through the application of deterrence theory to national security policies. It considered the different approaches Israel and the US have utilised, taking into consideration their historical experiences with deterrence and the influence these experiences had on their expectations and definitions of deterrence. Both states endorsed deterrence as an approach over the 10-year period under review, and both faced (and continue to face) adversaries in cyberspace that are increasingly active and capable. Neither state had deterred their acknowledged adversaries from developing capabilities or conducting attacks against their interests. The willingness of both states to engage in 'pre-emptive' actions against adversaries is creating norms of activity in cyberspace that may have unintended consequences including escalation to warfare. These risks are clearly serious. States considering deterrence as a practice to supplement their cybersecurity practices would be advised to carefully consider whether the risks of such an approach outweigh the benefits. Given the acknowledged complexities of deterrence it would seem that cybersecurity strategies based on deterrence are more likely to be considered effective where they target a state's effort or assist in directing a state's effort towards reasonable deterrence goals.

After a decade of practice, the evidence from these two case studies strongly suggests that deterrence is not the silver bullet for cybersecurity that many strategists and policymakers have treated it as.[1223] To have a positive impact on cybersecurity outcomes, deterrence requires an extraordinary effort from those states choosing to pursue it. It needs to meet the basic requirements of deterrence theory and be balanced across those requirements. It must also be appropriately tailored to the adversary, have visible consequences, and – even counterintuitively – be expected to fail.

Deterrence theory has always had to be adapted, both for the environment states wished it to operate in and to account for new types of weapons which allowed states to behave, or countenance behaving, in new ways. Cyberspace, while challenging, is yet another strategic environment that does not change the principles of deterrence. But states wishing to use deterrence would do well to understand that deterrence has always been complex, subject to definitions, and dependent on the broader relations between the states involved. Strategic theory can only provide states with guidance – states must adapt such theory to meet both their own needs and those of the environment. Lastly, states that choose to define deterrence differently to classic definitions may also be creating unnecessary risk. Labelling an action as deterrence that is in fact not deterrence is confusing for both allies and adversaries and increases the risk of strategic miscalculation. In the final analysis, a state choosing to adopt a deterrence posture in cyberspace should ensure its rhetoric matches its practices.

[1223] Martin C. Libicki, 2018, 'Expectations of Cyber Deterrence', *Strategic Studies Quarterly : SSQ 12*, no. 4: 44–57; David J. Lonsdale, 'Warfighting for Cyber Deterrence: A Strategic and Moral Imperative', ed. Mariarosaria Taddeo and Mariarosaria Taddeo, 2018, *Philosophy & Technology 31*, no. 3: 409–29, https://doi.org/10.1007/s13347-017-0252-8; Eric Sterner, 'Retaliatory Deterrence in Cyberspace', Strategic Studies Quarterly : SSQ 5, no. 1 (2011): 62–80; Brad D. Williams, 'US Urges "Like-Minded" Countries To Collaborate On Cyber Deterrence', Breaking Defense (blog), 24 April 2019, https://breakingdefense.sites.breakingmedia.com/2019/04/us-urging-likeminded-countries-to-collaborate-on-cyber-deterrence/; 'Modernization Gives Army Overmatch, Deterrence | AUSA', accessed 24 June 2021, https://www.ausa.org/news/modernization-gives-army-overmatch-deterrence.

Bibliography

'A Breakdown and Analysis of the December 2014 Sony Hack'. Security, 5 December 2014. https://www.riskbasedsecurity.com/2014/12/05/a-breakdown-and-analysis-of-the-december-2014-sony-hack/.

'A Guide to Cyber Attribution: Leading Intelligence Integration'. Office of the Director of National Intelligence, 14 September 2018. https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf.

'A New Level in the Cyber War between Israel and Iran | INSS'. Accessed 8 August 2021. https://www.inss.org.il/publication/iran-israel-cyber-war/.

Abunimah, Ali. *The Battle for Justice in Palestine*. Chicago, UNITED STATES: Haymarket Books, 2014. http://ebookcentral.proquest.com/lib/anu/detail.action?docID=1321783.

Adamsky, Dmitry (Dima). 'From Israel with Deterrence: Strategic Culture, Intra-War Coercion and Brute Force'. *Security Studies* 26, no. 1 (2017): 157–84. https://doi.org/10.1080/09636412.2017.1243923.

———. 'The Israeli Odyssey toward Its National Cyber Security Strategy'. *The Washington Quarterly* 40, no. 2 (2017): 113–27. https://doi.org/10.1080/0163660X.2017.1328928.

'Advancing National Cyberspace Capabilitites: Resolution No. 3611 of the Government of August 7, 2011'. State of Israel, 7 August 2011. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Israel_2011_Advancing%20National%20Cyberspace%20Capabilities.pdf.

Ahren, Raphael. 'In Netanyahu's New Illustrated World, Israel Has Just Five Enemies'. Accessed 7 August 2021. http://www.timesofisrael.com/in-netanyahus-new-illustrated-world-israel-has-just-five-enemies/.

Almog, Doron. 'Cumulative Deterrence and the War on Terrorism'. *Parameters (Carlisle, Pa.)* 34, no. 4 (2004): 4–19.

Alsoos, Imad. 'From Jihad to Resistance: The Evolution of Hamas's Discourse in the Framework of Mobilization'. *Middle Eastern Studies* ahead-of-print, no. ahead-of-print (2021): 1–22. https://doi.org/10.1080/00263206.2021.1897006.

Amin, S. Massoud. 'Power and Energy Infrastructure: Cyber Security, Defense, and Resilience'. *Georgetown Journal of International Affairs* 16, no. SI (2015): 70.

Andres, Richard. 'Cyber Gray Space Deterrence'. *Prism (Washington, D.C.)* 7, no. 2 (2017): 90–99.

Arian, Asher. *Security Threatened: Surveying Israeli Opinion on Peace and War*. Cambridge Studies in Public Opinion and Political Psychology. Cambridge: Cambridge University Press, 1995. https://doi.org/10.1017/CBO9780511625732.

Arnould, EJ, and M. Wallendorf. 'Market-Oriented Ethnography - Interpretation Building And Marketing Strategy Formulation'. *Journal of Marketing Research* 31, no. 4 (1994): 484–504. https://doi.org/10.2307/3151878.

‘Australia’s Cyber Security Strategy 2020’. Commonwealth of Australia, 6 August 2020. https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf.

Ayyub, Rami. ‘Israel Says It Thwarted Foreign Cyber Attack on Defence Industry’. *Reuters*, 12 August 2020, sec. Aerospace and Defense. https://www.reuters.com/article/us-israel-cyber-attack-idUSKCN25825T.

Bahgat, Gawdat. ‘Iranian- Israeli Confrontation: The Cyber Domain’. *Middle East Policy* 27, no. 3 (2020): 115–24. https://doi.org/10.1111/mepo.12516.

Bahgat, Gawdat, and Anoushiravan Ehteshami. ‘Iran’s Defense Strategy: The Navy, Ballistic Missiles and Cyberspace’. *Middle East Policy* 24, no. 3 (2017): 89–103. https://doi.org/10.1111/mepo.12292.

Banerjea, Aparna. ‘NotPetya: How a Russian Malware Created the World’s Worst Cyberattack Ever’. *Business Standard India*, 27 August 2018. https://www.business-standard.com/article/technology/notpetya-how-a-russian-malware-created-the-world-s-worst-cyberattack-ever-118082700261_1.html.

Bar, Shmuel. ‘Israeli Strategic Deterrence Doctrine and Practice’. *Comparative Strategy* 39, no. 4 (2020): 321–53. https://doi.org/10.1080/01495933.2020.1772624.

Baram, Gil. ‘Israeli Defense in the Age of Cyber War’. *Middle East Quarterly* 24, no. 1 (2017): 1C-10C.

Bar-Joseph, Uri. ‘Variations on a Theme: The Conceptualization of Deterrence in Israeli Strategic Thinking’. *Security Studies* 7, no. 3 (1998): 145–81. https://doi.org/10.1080/09636419808429353.

Basrur, Rajesh M. ‘Minimum Deterrence and India’s Nuclear Security’. In *Minimum Deterrence and India’s Nuclear Security*, 2006.

Bergman, Ronen, and Ronnie Hope. *Rise and Kill First: The Secret History of Israel’s Targeted Assassinations*. First. Book, Whole. New York: Random House, 2018. https://go.exlibris.link/WNWMSLdk.

Bertram, Christoph and International Institute for Strategic Studies. *Strategic Deterrence in a Changing Environment*. Vol. 6. Book, Whole. Farnborough, Eng.;Montclair, N.J.; Gower Pub. Co, 1980.

Boulianne, Shelley, Karolina Koc-Michalska, and Bruce Bimber. ‘Right-Wing Populism, Social Media and Echo Chambers in Western Democracies’. *New Media & Society* 22, no. 4 (1 April 2020): 683–99. https://doi.org/10.1177/1461444819893983.

Brantly, Aaron F. ‘Entanglement in Cyberspace: Minding the Deterrence Gap’. *Democracy and Security* 16, no. 3 (2020): 210–33. https://doi.org/10.1080/17419166.2020.1773807.

Broad, William J., John Markoff, and David E. Sanger. ‘NYT: Israeli Test on Worm Called Crucial in Iran Nuclear Delay - Council on Foreign Relations’, no. Generic (2011).

Bryman, Alan. *Social Research Methods*. 4th ed. Book, Whole. New York;Oxford; Oxford University Press, 2012.

Bush, George W. 'The National Strategy to Secure Cyberspace'. White House, United States of America, February 2003. https://www.energy.gov/ceser/downloads/national-strategy-secure-cyberspace-february-2003.

Byman, Daniel. *A High Price: The Triumphs and Failures of Israeli Counterterrorism*. Book, Whole. New York: Oxford University Press, 2011. https://doi.org/10.1093/acprof:osobl/9780195391824.001.0001.

Israel Defense Forces. 'C4I and Cyber Defense Directorate', Sunday, October 29, 20174:56 PM. https://www.idf.il/en/minisites/c4i-and-cyber-defense-directorate/.

'CABINET APPROVES ESTABLISHMENT OF NATIONAL CYBER AUTHORITY'. *Info - Prod Research (Middle East)*. 2015.

Canada and Sécurité publique Canada (2007). *National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age.*, 2018. http://epe.lac-bac.gc.ca/100/201/301/weekly_acquisitions_list-ef/2018/18-27/publications.gc.ca/collections/collection_2018/sp-ps/PS4-239-2018-eng.pdf.

Carter, Ash. 'The DoD Cyber Strategy'. US Department of Defense, April 2015. https://info.publicintelligence.net/DoD-CyberStrategy.pdf.

Chen, Jim. 'Does Conventional Deterrence Work in the Cyber Domain?' In *European Conference on Cyber Warfare and Security*, 106–X. Reading: Academic Conferences International Limited, 2018.

Cimbala, Stephen J. 'Nuclear Deterrence and Cyber Warfare: Coexistence or Competition?' *Defense & Security Analysis* 33, no. 3 (2017): 193–208. https://doi.org/10.1080/14751798.2017.1351142.

Clark, David D., and Susan Landau. 'Untangling Attribution'. In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, 400. National Research Council, 2010. https://www.nap.edu/read/12997/chapter/4.

Clarke, Richard A., and Robert K. Knake. *Cyber War: The next Threat to National Security and What to Do about It*. 1st ed. Book, Whole. New York: Ecco, 2010.

Cohen, Matthew S., Charles D. Freilich, and Gabi Siboni. 'Israel and Cyberspace: Unique Threat and Response'. *International Studies Perspectives* 17, no. 3 (2015 2016): 307–21. https://doi.org/10.1093/isp/ekv023.

Cohen, Yoel. *Whistleblowers and the Bomb: Vanunu, Israel and Nuclear Secrecy*. New. Book, Whole. London: Pluto, 2005.

Columbus, Cristie, Karen B. Brust, and Alejandro C. Arroliga. '2019 Novel Coronavirus: An Emerging Global Threat'. *Baylor University Medical Center. Proceedings* 33, no. 2 (April 2020): 209–12. http://dx.doi.org.virtual.anu.edu.au/10.1080/08998280.2020.1731272.

'Cyber Conflict and Deterrence'. *Strategic Comments* 22, no. 7 (2016): iii–v. https://doi.org/10.1080/13567888.2016.1237761.

'Cyber Security Strategy for Germany'. Federal Ministry of the Interior, February 2011. http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile.

Haaretz.com. ‘Cyberattacks on Israel: The State’s Stupidity Is Putting Officials at Risk’. Accessed 24 June 2021. https://www.haaretz.com/israel-news/tech-news/.premium-cyberattacks-on-israel-the-state-s-stupidity-is-putting-officials-at-risk-1.9389796.

‘Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934’. US Department of Defense, November 2011. https://fas.org/irp/eprint/dod-cyber.pdf.

David, Matthew, and Carole D. Sutton. ‘Social Research: An Introduction’. In *Social Research: An Introduction*, x–x, 2011.

Davis, John S. II and Rand Corporation. ‘Stateless Attribution: Toward International Accountability in Cyberspace’ RR-2081-MS., no. Generic (2017).

‘Delivery to Consumers - U.S. Energy Information Administration (EIA)’. Accessed 31 August 2021. https://www.eia.gov/energyexplained/electricity/delivery-to-consumers.php.

Demchak, Chris C., and Peter Dombrowski. ‘Rise of a Cybered Westphalian Age’. *Strategic Studies Quarterly : SSQ* 5, no. 1 (2011): 32–61.

Denning, Dorothy E. ‘Rethinking the Cyber Domain and Deterrence’. *Joint Force Quarterly*, no. 77 (2015): 8.

‘Department of Defense: Cyber Strategy 2018’. United States Department of Defense, September 2018. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

‘Department of Defense: Strategy for Operating in Cyberspace’. United States Department of Defense, July 2011. https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

‘Department of Defense Strategy for Operating in Cyberspace’, n.d., 19.

Defense One. ‘Did Israel Have the Right to Bomb Hamas’ Cyber HQ?’ Accessed 8 August 2021. https://www.defenseone.com/ideas/2019/05/did-israel-have-right-bomb-hamas-cyber-hq/156829/.

INSS. ‘Disproportionate Force: Israel’s Concept of Response in Light of the Second Lebanon War’. Accessed 7 August 2021. https://www.inss.org.il/publication/disproportionate-force-israels-concept-of-response-in-light-of-the-second-lebanon-war/.

Doffman, Zak. ‘Israel Responds To Cyber Attack With Air Strike On Cyber Attackers In World First’. Forbes. Accessed 25 June 2021. https://www.forbes.com/sites/zakdoffman/2019/05/06/israeli-military-strikes-and-destroys-hamas-cyber-hq-in-world-first/.

Efrony, Dan, Yuval Shany, and this link will open in a new window Link to external site. ‘A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice’. *The American Journal of International Law* 112, no. 4 (October 2018): 583–657. http://dx.doi.org.virtual.anu.edu.au/10.1017/ajil.2018.86.

Egloff, Florian J, and Max Smeets. ‘Publicly Attributing Cyber Attacks: A Framework’. *Journal of Strategic Studies*, no. Ahead of Print (2021). https://doi-org.virtual.anu.edu.au/10.1080/01402390.2021.1895117.

Eizenkot, Gadi. ‘Deterring Terror: How Israel Confronts the Next Generation of Threats’. Belfer Center for Science and International Affairs, August 2016. https://www.belfercenter.org/sites/default/files/legacy/files/IDFDoctrineTranslation.pdf.

Eizenkot, Gadi, and Gabi Siboni. ‘Guidelines for Israel’s National Security’. *The Washington Institute for Near East Policy*, no. Policy Focus: 160 (October 2019). https://www.washingtoninstitute.org/media/4613?disposition=inline.

‘Elevation of U.S. Cyber Command to a Unified Combatant Command: Memorandum for the Secretary of Defense’. Federal Register, Vol. 82, No. 162, 23 August 2017. https://www.govinfo.gov/content/pkg/FR-2017-08-23/pdf/2017-17947.pdf.

‘Finland’s Cyber Security Strategy 2019’. Secretariat of the Security Committee, 3 October 2019. https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf.

Fischerkeller, Michael P. ‘Persistent Engagement and Tacit Bargaining: A Strategic Framework for Norms Development in Cyberspace’s Agreed Competition’. *Policy File*. Institute for Defense Analyses, 2018.

Fischerkeller, Michael P., and Richard J. Harknett. ‘Deterrence Is Not a Credible Strategy for Cyberspace’. *Orbis (Philadelphia)* 61, no. 3 (2017): 381–93. https://doi.org/10.1016/j.orbis.2017.05.003.

FRANTZMAN, SETH J. ‘Cyber Warfare, Israel, Iran and the New Way of Total War’. *The Jerusalem Post (Online)*. 2020, English edition.

Freedman, Lawrence. *Deterrence*. Book, Whole. Malden, MA: Polity Press, 2004.

Frei, Jasper. ‘Israel’s National Cybersecurity and Cyberdefense Posture: Policy and Organizations’. Application/pdf. ETH Zurich, 2020. https://doi.org/10.3929/ETHZ-B-000438397.

Gaddis, John Lewis. *On Grand Strategy*. Book, Whole. New York: Penguin Press, 2018.

Gartzke, Erik. ‘The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth’. *International Security* 38, no. 2 (2013): 41–73. https://doi.org/10.1162/ISEC_a_00136.

Gcaza, Noluxolo, Rossouw Von Solms, Marthie M. Grobler, and Joey Jansen Van Vuuren. ‘A General Morphological Analysis: Delineating a Cyber-Security Culture’. *Information and Computer Security* 25, no. 3 (2017): 259–78. https://doi.org/10.1108/ICS-12-2015-0046.

General Tao Hanzhang. *Sun Tzu’s The Art of War*. Translated by Yuan Shibing. New York: Sterling, 1990.

George, Alexander L., and Andrew Bennett. *Case Studies and Theory Development in the Social Sciences*. Book, Whole. Cambridge, Mass: MIT Press, 2005.

George, Alexander L., and Richard Smoke. *Deterrence in American Foreign Policy: Theory and Practice*. Book, Whole. New York: Columbia University Press, 1974.

Gerring, John. *Case Study Research: Principles and Practices*. Book, Whole. New York: Cambridge University Press, 2007. https://doi.org/10.1017/CBO9780511803123.

Gjesvik, Lars, and Emil Jorgensen Overbo. 'Deter Who? The Importance of Strategic Culture for Cybersecurity'. *Internasjonal Politikk* 77, no. 3 (2019): 278–87. https://doi.org/10.23865/intpol.v77.1396.

Glenn, Colleen, Dane Sterbentz, and Aaron Wright. 'Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector', 20 December 2016. https://doi.org/10.2172/1337873.

Gold, Josh. 'The Five Eyes and Offensive Cyber Capabilities: Building a "Cyber Deterrence Initiative"', n.d., 30.

Goodman, Will. 'Cyber Deterrence: Tougher in Theory than in Practice?' *Strategic Studies Quarterly : SSQ* 4, no. 3 (2010): 102–35.

GRAY, COLIN S. 'Concept Failure? COIN, Counterinsurgency, and Strategic Theory'. *Prism (Washington, D.C.)* 3, no. 3 (2012): 17–32.

Gray, Colin S. *Weapons Don't Make War: Policy, Strategy, and Military Technology*. Book, Whole. Lawrence, Kan: University Press of Kansas, 1993.

Greenstein, Fred I., and Nelson Woolf Polsby. *Handbook of Political Science*. Book, Whole. Reading, Mass: Addison-Wesley, 1975.

Greiman, Virginia. 'The Politics and Practice of Cyber Attribution: A Global Legal Perspective'. In *International Conference on Cyber Warfare and Security*, 102–8. Reading, United Kingdom: Academic Conferences International Limited, 2021. http://dx.doi.org.virtual.anu.edu.au/10.34190/IWS.21.116.

Groll, Elias. 'The Future Is Here, and It Features Hackers Getting Bombed'. *Foreign Policy* (blog). Accessed 8 August 2021. https://foreignpolicy.com/2019/05/06/the-future-is-here-and-it-features-hackers-getting-bombed/.

Gross, Judah Ari. 'IDF Says It Thwarted a Hamas Cyber Attack during Weekend Battle'. *The Times of Israel*. 2019.

Handel, Michael I. *Israel's Political-Military Doctrine*. Vol. no. 30. Book, Whole. Cambridge, Mass.: Center for International Affairs, Harvard University, 1973.

HEALEY, JASON. 'The Cartwright Conjecture: The Deterrent Value and Escalatory Risk of Fearsome Cyber Capabilities'. In *Bytes, Bombs, and Spies*, edited by Herbert Lin and Amy Zegart, 173. Brookings Institution Press, 2019. https://doi.org/10.7864/j.ctv75d8hb.12.

Healey, Jason. 'The Implications of Persistent (and Permanent) Engagement in Cyberspace'. *Journal of Cybersecurity* 5, no. 1 (26 August 2019). https://academic.oup.com/cybersecurity/article/5/1/tyz008/5554878.

Henriksen, Dag. 'Deterrence by Default? Israel's Military Strategy in the 2006 War against Hizballah'. *Journal of Strategic Studies* 35, no. 1 (2012): 95–120. https://doi.org/10.1080/01402390.2011.601095.

Hillen, Sven, and Nils D. Steiner. 'The Consequences of Supply Gaps in Two-dimensional Policy Spaces for Voter Turnout and Political Support: The Case of Economically Left-wing and

Culturally Right-wing Citizens in Western Europe'. *European Journal of Political Research* 59, no. 2 (2020): 331–53. https://doi.org/10.1111/1475-6765.12348.

Hinton, Patrick. 'Strategic Culture: In Defiance of a Structural World Order'. *The RUSI Journal* 165, no. 4 (6 June 2020): 80–87. https://doi.org/10.1080/03071847.2020.1816736.

'House Committee on Armed Services Hearing on Cyber Warfare'. *Political Transcript Wire*. 3 March 2017. http://www.proquest.com/docview/1874238660/abstract/D72E2687EE404A2DPQ/1.

Housen-Couriel, Deborah. 'National Cyber Security Organisation: ISRAEL', n.d., 22.

'IDF Forms New Force to Combat Cyber Warfare - Haaretz Com - Haaretz.Com'. Accessed 7 August 2021. https://www.haaretz.com/.premium-idf-takes-steps-against-cyber-attacks-1.5232323.

Inbar, Efraim, and Eitan Shamir. '"Mowing the Grass": Israel's Strategy for Protracted Intractable Conflict'. *Journal of Strategic Studies* 37, no. 1 (2014): 65–90. https://doi.org/10.1080/01402390.2013.830972.

'Intellectual Overmatch Is Impossible If We Teach Only Half The Team: A Call For Professional Civilian Education'. *States News Service*. 2021.

'Iran/Israel/United Sates: Presidential Candidate: US, Israel Wary of Iran's Cyber Power'. *Asia News Monitor*. 2013.

'Israel | UNIDIR'. Accessed 25 June 2021. https://unidir.org/cpp/en/states/israel.

'Israel National Cyber Security: In Brief'. State of Israel, September 2017. https://cyber.haifa.ac.il/images/pdf/cyber_english_A5_final.pdf.

'Israel Responded to a Hamas Cyberattack with an Airstrike. That's Not Such a Big Deal. - The Washington Post'. Accessed 8 August 2021. https://www.washingtonpost.com/politics/2019/05/09/israel-responded-hamas-cyberattack-with-an-airstrike-thats-big-deal/.

'Israel Sets Precedent by Launching Air Strike against Hamas Hackers'. Accessed 25 June 2021. https://www.scmagazine.com/home/security-news/israel-sets-precedent-by-launching-air-strike-against-hamas-hackers/.

'Israel Spies Opportunity as U.S. Gives Cyber Command Major Upgrade'. *Haaretz*. 2017.

'Israel Strikes Back at Iran - the Constant Cyber Warfare Paradigm - The Jerusalem Post'. Accessed 8 August 2021. https://www.jpost.com/israel-news/israel-strikes-back-at-iran-the-constant-cyber-warfare-paradigm-628535.

'Israeli Defense Forces' Defense Doctrine - English Translation'. *Policy File*. Belfer Center for Science and International Affairs, 2016.

Israeli, Ofer. 'Israel's Nuclear Amimut Policy and Its Consequences'. *Israel Affairs* 21, no. 4 (2015): 541–58. https://doi.org/10.1080/13537121.2015.1076185.

'Japan: Cybersecurity Strategy'. Government of Japan (provisional translation), 27 July 2018. https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf.

Jervis, R. 'Some Thoughts on Deterrence in the Cyber Era'. *Journal of Information Warfare* 15, no. 2 (2016): 66–73.

Jervis, Robert. 'Deterrence Theory Revisited'. Edited by Alexander George and Richard Smoke. *World Politics* 31, no. 2 (1979): 289–324. https://doi.org/10.2307/2009945.

Johnson, David E., Rand Corporation, Project Air Force (U.S.), Arroyo Center, Inc Books24x7, United States. Army, and United States. Air Force. *Hard Fighting: Israel in Lebanon and Gaza*. Vol. MG-1085-A/AF. Book, Whole. Santa Monica, Calif: RAND, 2011. https://doi.org/10.7249/mg1085a-af.

Johnson, Jesse C., Brett Ashley Leeds, and Ahra Wu. 'Capability, Credibility, and Extended General Deterrence'. *International Interactions* 41, no. 2 (2015): 309–36. https://doi.org/10.1080/03050629.2015.982115.

Kaplan, Fred M. *Dark Territory: The Secret History of Cyber War*. First Simon&Schuster hardcover. Book, Whole. New York: Simon & Schuster, 2016.

Katz, Yaakov. 'Israel's Cyber Ambiguity'. *The Jerusalem Post*. 2012.

Kello, Lucas. *The Virtual Weapon and International Order*. New Haven: Yale University Press, 2017.

Kerr, Pauline and Australian National University. *Researching Security in East Asia: From 'strategic Culture' to 'Security Culture*. Working Paper / Australian National University, Strategic and Defence Studies Centre,0158-3751 ;No. 326. Canberra: Strategic and Defence Studies Centre, Australian National University, 1998. https://catalog.hathitrust.org/Record/007230056.

Kfir, Isaac. 'Israels Approach to Counter-Terrorism'. In *Handbook of Terrorism and Counter Terrorism Post 9/11*, 227–39. Edward Elgar Publishing, 2019. https://doi.org/10.4337/9781786438027.00026.

———. 'Israel's Cyber Ecosystem: Why the Start-up Nation Eschews Doctrines and Silos When It Comes to Cybersecurity'. *Asia & The Pacific Policy Society: Policy Forum* (blog), 29 November 2018. https://www.policyforum.net/israels-cyber-ecosystem/.

Klare, Michael T. 'Why "Overmatch" Is Overkill'. *The Nation (New York, N.Y.)* 308, no. 2 (2019): 22.

Klieman, Aharon. 'Doomed to Succeed: The US–Israel Relationship from Truman to Obama'. *Israel Journal of Foreign Affairs* 10, no. 2 (3 May 2016): 305–9. https://doi.org/10.1080/23739770.2016.1197627.

Klimburg, Alexander. 'Mixed Signals: A Flawed Approach to Cyber Deterrence'. *Survival (London)* 62, no. 1 (2020): 107–30. https://doi.org/10.1080/00396338.2020.1715071.

———. 'National Cyber Security Framework Manual'. NATO CCD COE Publication, 2012. https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf.

Knapp, Kenneth J., and William R. Boulton. 'Cyber-Warfare Threatens Corporations: Expansion into Commercial Environments'. *Information Systems Management* 23, no. 2 (2006): 76–87. https://doi.org/10.1201/1078.10580530/45925.23.2.20060301/92675.8.

Kober, Avi. 'From Blitzkrieg To Attrition: Israel's Attrition Strategy and Staying Power'. *Small Wars & Insurgencies* 16, no. 2 (2005): 216–40. https://doi.org/10.1080/09592310500080005.

Landler, Mark, and Scott Shane. 'U.S. Condemns Russia for Cyberattack, Showing Split in Stance on Putin'. *The New York Times*, 16 February 2018, sec. U.S. https://www.nytimes.com/2018/02/15/us/politics/russia-cyberattack.html.

Lappin, Yaakov. 'Iran "Working Systematically to Build Serious Cyber-Attack Capabilities"'. JNS.org, 6 August 2021. https://www.jns.org/iran-is-working-systematically-to-build-serious-cyber-attack-capabilities/.

Lawson, Ewan. 'Deterrence in Cyberspace: A Silver Bullet or a Sacred Cow?' Edited by Mariarosaria Taddeo and Mariarosaria Taddeo. *Philosophy & Technology* 31, no. 3 (2018): 431–36. https://doi.org/10.1007/s13347-017-0267-1.

Lebow, Richard Ned, Janice Stein, and Canadian Institute for International Peace and Security. 'When Does Deterrence Succeed and How Do We Know?' Vol. no. 8. Ottawa: The Canadian Institute for International Peace and Security, 1990.

Leuprecht, Christian, Joseph Szeman, and David B. Skillicorn. 'The Damoclean Sword of Offensive Cyber: Policy Uncertainty and Collective Insecurity'. *Contemporary Security Policy* 40, no. 3 (2019): 382–407. https://doi.org/10.1080/13523260.2019.1590960.

Levite, Ariel. *Offense and Defense in Israeli Military Doctrine*. Book, Whole. Boulder: Westview Press, 1989.

Levy, Jack S. 'Deterrence and Coercive Diplomacy: The Contributions of Alexander George'. *Political Psychology* 29, no. 4 (2008): 537–52. https://doi.org/10.1111/j.1467-9221.2008.00648.x.

Leyden, John. 'Russia's to Blame for pro-ISIS Megahack on French TV Network'. Accessed 24 June 2021. https://www.theregister.com/2015/06/10/russian_trolls_staged_tv5monde_megahack_shocker/.

Libicki, Martin. *Cyberspace in Peace and War*. 1st ed. Naval Institute Press, 2016.

Libicki, Martin C. 'Expectations of Cyber Deterrence'. *Strategic Studies Quarterly : SSQ* 12, no. 4 (2018): 44–57.

Libicki, Martin C., Rand Corporation, Project Air Force (U.S.), United States. Air Force, and Inc Books24x7. *Cyberdeterrence and Cyberwar*. Book, Whole. Santa Monica, CA: RAND, 2009. https://doi.org/10.7249/mg877af.

Lijphart, Arend. 'Comparative Politics and the Comparative Method'. *The American Political Science Review* 65, no. 3 (1971): 682–93. https://doi.org/10.2307/1955513.

Lim, Gil Baram, Kevjn. 'Israel and Iran Just Showed Us the Future of Cyberwar With Their Unusual Attacks'. *Foreign Policy* (blog). Accessed 8 August 2021. https://foreignpolicy.com/2020/06/05/israel-and-iran-just-showed-us-the-future-of-cyberwar-with-their-unusual-attacks/.

Limnéll, Jarno. 'The Cyber Arms Race Is Accelerating - What Are the Consequences?' *Journal of Cyber Policy* 1, no. 1 (2016): 50–60. https://doi.org/10.1080/23738871.2016.1158304.

Lin, Herbert. 'Attribution of Malicious Cyber Incidents: From Soup to Nuts'. *Journal of International Affairs (New York)* 70, no. 1 (2016): 75–137.

Lin, Herbert, and Jaclyn Kerr. 'On Cyber-Enabled Information Warfare and Information Operations'. *Oxford Handbook of Cybersecurity*, 23 May 2019, 29.

Lindsay, Jon R. 'Stuxnet and the Limits of Cyber Warfare'. *Security Studies* 22, no. 3 (2013): 365–404. https://doi.org/10.1080/09636412.2013.816122.

———. 'Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack'. *Journal of Cybersecurity (Oxford)* 1, no. 1 (2015): 53–67. https://doi.org/10.1093/cybsec/tyv003.

Lobel, Oved. 'Israel and Iran: "Cyber Winter Is Coming"'. *The ASPI Strategist [BLOG]*, no. Generic (2020).

Lonsdale, David J. 'Warfighting for Cyber Deterrence: A Strategic and Moral Imperative'. Edited by Mariarosaria Taddeo and Mariarosaria Taddeo. *Philosophy & Technology* 31, no. 3 (2018): 409–29. https://doi.org/10.1007/s13347-017-0252-8.

Lupovici, Amir. *The Power of Deterrence: Emotions, Identity and American and Israeli Wars of Resolve*. Book, Whole, 2016. https://doi.org/10.1017/CBO9781316534540.

———. 'Toward a Securitization Theory of Deterrence'. *International Studies Quarterly* 63, no. 1 (2019): 177–86. https://doi.org/10.1093/isq/sqy045.

Lynn, William J. 'Defending a New Domain: The Pentagon's Cyberstrategy'. *Foreign Affairs (New York, N.Y.)* 89, no. 5 (2010): 97–108.

Malka, Amos. 'Israel and Asymmetrical Deterrence'. *Comparative Strategy* 27, no. 1 (2008): 1–19. https://doi.org/10.1080/01495930701839613.

Maoz, Zeev. 'Evaluating Israel's Strategy of Low-Intensity Warfare, 1949-2006'. *Security Studies* 16, no. 3 (2007): 319–49. https://doi.org/10.1080/09636410701547782.

Mastriano, Douglas. 'Putin - the Masked Nemesis of the Strategy of Ambiguity'. *Defense and Security Analysis* 33, no. 1 (20 January 2017): 68–76.

Matania, Eviatar, Lior Yoffe, and Michael Mashkautsan. 'A Three-Layer Framework for a Comprehensive National Cyber-Security Strategy'. *Georgetown Journal of International Affairs* 17, no. 3 (2016): 77–84. https://doi.org/10.1353/gia.2016.0038.

Mearsheimer, John J. *Conventional Deterrence*. Book, Whole. Ithaca: Cornell University Press, 1983.

'Meet "Flame," The Massive Spy Malware Infiltrating Iranian Computers | WIRED'. Accessed 25 June 2021. https://www.wired.com/2012/05/flame/.

Mekelberg, Yossi. 'Cyberspace: The New Frontier in the Israeli-Iranian Battleground'. *Arab News*. 2020.

Mitchell, Charlie. 'U.S. Indictment of Russian Intelligence Officers Reflects First Culpability for Devastating "NotPetya" Attack'. *Inside Cybersecurity*, 20 October 2020. http://www.proquest.com/docview/2452445958/citation/D6F7A8A9FD224FAFPQ/1.

'Modernization Gives Army Overmatch, Deterrence | AUSA'. Accessed 24 June 2021. https://www.ausa.org/news/modernization-gives-army-overmatch-deterrence.

Morgan, Patrick M. *Deterrence: A Conceptual Analysis*. Book, Whole. Beverly Hills, Calif: Sage Publications, 1977.

———. *Deterrence Now*. Vol. 89. Book, Whole. Cambridge [England];New York; Cambridge University Press, 2003. https://doi.org/10.1017/CBO9780511491573.

Nakasone, GEN Paul M. 'Command Vision for US Cyber Command: Achieve and Maintain Cyberspace Superiority'. United States Cyber Command, April 2018. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf.

'Nakasone_03-01-18.Pdf'. Accessed 25 June 2021. https://www.armed-services.senate.gov/imo/media/doc/Nakasone_03-01-18.pdf.

'National Cyber Security Strategy 2016-2021'. Her Majesty's Government, 2016. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

'National Cyber Strategy of the United States of America'. The White House, September 2018. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

'National Cybercrime Policy of Papua New Guinea'. Government of Papua New Guinea, July 2014. file:///C:/Users/u4499315/Downloads/National-Cybercrime-Policy-2014.pdf.

'National Cybersecurity Strategy'. Republic of Korea: National Secuirty Office, n.d.

'National Infrastructure Protection Plan: 2006'. U.S. Department of Homeland Security, 2006. https://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf.

Nelson, Steven. 'White House Accuses Russia of NotPetya Cyberattack, Threatens Unspecified "Consequences"'. *Washington Examiner*. 15 February 2018, sec. Politics. http://www.proquest.com/docview/2002763227/citation/C885AA93B8254452PQ/1.

Netanyahu, Benjamin. 'Advancing the National Preparedness for Cyber Security: Government Resolution No. 2444'. The State of Israel: The Government Secretary, n.d. https://ccdcoe.org/uploads/2019/06/Government-Resolution-No-2444-Advancing-the-National-Preparedness-for-Cyber-Security.pdf.

Iran International. 'Netanyahu: Iran Attempts "Daily" Cyber Attacks on Israeli Infrastructure', 29 January 2019. https://iranintl.com/en/world/netanyahu-iran-attempts-daily-cyber-attacks-israeli-infrastructure.

The Jerusalem Post | JPost.com. 'Netanyahu: Iran behind Cyber Attacks on Israel'. Accessed 24 June 2021. https://www.jpost.com/israel-news/watch-live-netanyahu-addresses-cyber-security-conference-375290.

Netolicka, Veronika, and Miroslav Mares. 'Arms Race "in Cyberspace" - A Case Study of Iran and Israel'. *Comparative Strategy* 37, no. 5 (2018): 414–29. https://doi.org/10.1080/01495933.2018.1526568.

Neville, Liam, and Zoe Hawkins. 'Deterrence in Cyberspace: Different Domain, Different Rules'. *Australian Strategic Policy Institute: The Strategist*, 27 July 2016. https://www.aspistrategist.org.au/deterrence-cyberspace-different-domain-different-rules/.

'New Zealand's Cyber Security 2019'. Department of the Prime Minister and Cabinet, 2019. https://dpmc.govt.nz/publications/new-zealands-cyber-security-strategy-2019.

Nye, Joseph S. 'Deterrence in Cyberspace'. *The ASPI Strategist [BLOG]*, no. Generic (2019).

Obama, Barack. 'International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World: (688502011-001)'. American Psychological Association, 2011. https://doi.org/10.1037/e688502011-001.

———. 'National Security Strategy'. President of the United States of America, May 2010. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

———. 'National Security Strategy'. White House, United States of America, February 2015. https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf.

———. 'The Comprehensive National Cybersecurity Initiative'. The White House, May 2009. https://obamawhitehouse.archives.gov/sites/default/files/cybersecurity.pdf.

Ojserkis, Raymond P. *Beginnings of the Cold War Arms Race: The Truman Administration and the U.S. Arms Build-Up*. Vol. 1. Book, Whole. Westport, Conn: Praeger, 2003.

O'Neil, Andrew. 'Australia and the "Five Eyes" Intelligence Network: The Perils of an Asymmetric Alliance'. *Australian Journal of International Affairs* 71, no. 5 (3 September 2017): 529–43. https://doi.org/10.1080/10357718.2017.1342763.

Opall-Rome, Barbara. 'US-Israel Sign Cyber Defense Declaration'. *DEFENSE NEWS INTERNATIONAL* 31, no. 23 (2016).

Osawa, Jun. 'The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?' *Asia-Pacific Review* 24, no. 2 (2017): 113–31. https://doi.org/10.1080/13439006.2017.1406703.

Painter, Chris. 'Deterrence in Cyberspace', n.d., 16.

Pasley, James F. 'Chicken Pax Atomica: The Cold War Stability of Nuclear Deterrence'. *Journal of International and Area Studies* 15, no. 2 (2008): 21–39.

Payne, Keith B. *The Fallacies of Cold War Deterrence and a New Direction*. Book, Whole. Lexington: University Press of Kentucky, 2001.

Perlroth, Nicole, and Scott Shane 'How Israel Caught Russian Hackers Scouring the World for U.S. Secrets'. *New York Times (Online)*. 2017.

'PM Netanyahu: Cyber Security Is a Serious Business Matter for Israel: ISRAEL CYBER SECURITY'. *EFE News Service*. 2017.

Powell, Robert. *Nuclear Deterrence Theory: The Search for Credibility*. Book, Whole. Cambridge: Cambridge University Press, 2008.

‘Presidential Policy Directive -- United States Cyber Incident Coordination’. The White House, 26 July 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

‘Quadrennial Defense Review Report 2010’. United States Department of Defense, February 2010. https://history.defense.gov/Portals/70/Documents/quadrennial/QDR2010.pdf?ver=vVJYRVwNdnGb_00ixF0UfQ%3d%3d.

Quester, George H. *The Future of Nuclear Deterrence*. Book, Whole. Lexington, Mass: Lexington Books, 1986.

Raska, Michael. ‘Confronting Cybersecurity Challenges: Israel’s Evolving Cyber Defence Strategy’. *Policy File*. S. Rajaratnam School of International Studies, 2015.

Reich, Bernard, and Gershon R. Kieval. *Israeli National Security Policy: Political Actors and Perspectives*. Vol. no. 210. Book, Whole. New York: Greenwood Press, 1988.

U.S. Department of Defense. ‘Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City’. Accessed 24 June 2021. https://content.govdelivery.com/accounts/USDOD/bulletins/571813.

Renshon, Stanley Allen. *National Security in the Obama Administration: Reassessing the Bush Doctrine*. Book, Whole. Milton Park, Abingdon, Oxon;New York; Routledge, 2010. https://doi.org/10.4324/9780203874516.

Reveron, Derek S. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Book, Whole, 2012.

Rid, Thomas. ‘Deterrence beyond the State: The Israeli Experience’. *Contemporary Security Policy* 33, no. 1 (2012): 124–47. https://doi.org/10.1080/13523260.2012.659593.

Rid, Thomas, and Ben Buchanan. ‘Attributing Cyber Attacks’. *Journal of Strategic Studies* 38, no. 1–2 (2 January 2015): 4–37. https://doi.org/10.1080/01402390.2014.977382.

Riordan, Shaun. ‘Cyberdiplomacy: Managing Security and Governance Online’, no. Generic (2019).

Rowley, Charles K., and Jennis Taylor. ‘The Israel and Palestine Land Settlement Problem, 1948-2005: An Analytical History’. *Public Choice* 128, no. 1/2 (2006): 77–90. https://doi.org/10.1007/s11127-006-9045-9.

Samaan, Jean-Loup. ‘From War to Deterrence? Israel-Hezbollah Conflict Since 2006’: Fort Belvoir, VA: Defense Technical Information Center, 1 May 2014. https://doi.org/10.21236/ADA601846.

Sanger, David E. *Confront and Conceal: Obama’s Secret Wars and Surprising Use of American Power*. 1st ed. Book, Whole. New York: Crown Publishers, 2012. ui-

Sanger, David E., and Nicole Perlroth. ‘U.S. Said to Find North Korea Ordered Cyberattack on Sony’. *The New York TImes*, 17 December 2014. https://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html.

Schelling, Thomas C. *Arms and Influence*. Book, Whole. Yale University Press, 2008.

‘Shin Bet Deputy Chief R: Mossad, Shin Bet, IDF Borders May Need Redo - The Jerusalem Post’. Accessed 24 June 2021. https://www.jpost.com/israel-news/shin-bet-deputy-chief-r-mossad-shin-bet-idf-borders-may-need-redo-664571.

Sicker, Martin. *Israel’s Quest for Security*. Book, Whole. New York: Praeger, 1989.

Smeets, Max. ‘Integrating Offensive Cyber Capabilities: Meaning, Dilemmas, and Assessment’. *Defence Studies* 18, no. 4 (2018): 395–410. https://doi.org/10.1080/14702436.2018.1508349.

Smith, Hugh. *On Clausewitz : A Study of Military and Political Ideas*. Book, Whole. New York: Palgrave Macmillan, 2005. https://doi.org/10.1057/9780230513679.

Smoke, Richard, and Alexander George. ‘Theory for Policy in International Affairs’. *Policy Sciences* 4, no. 4 (1973): 387–413. https://doi.org/10.1007/BF01728468.

‘Statement by President Donald J. Trump on the Elevation of Cyber Command – The White House’. Accessed 24 June 2021. https://trumpwhitehouse.archives.gov/briefings-statements/statement-president-donald-j-trump-elevation-cyber-command/.

Sterner, Eric. ‘Retaliatory Deterrence in Cyberspace’. *Strategic Studies Quarterly : SSQ* 5, no. 1 (2011): 62–80.

Stevens, Tim. ‘A Cyberwar of Ideas? Deterrence and Norms in Cyberspace’. *Contemporary Security Policy* 33, no. 1 (2012): 148–70. https://doi.org/10.1080/13523260.2012.659597.

‘Summary of the 2018 National Defense Strategy of The United States of America: Sharpening the American Military’s Competitive Edge’. Department of Defense, 2018. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

Tabansky, Lior. ‘Israel Defense Forces and National Cyber Defense’. *Connections. The Quarterly Journal (English Ed.)* 19, no. 1 (2020): 45–62. https://doi.org/10.11610/Connections.19.1.05.

———. ‘Israel’s Cyber Security Policy: Local Response to the Global Cybersecurity Risk’. In *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications*, 1125–45, 2018. https://doi.org/10.4018/978-1-5225-5634-3.ch054.

———. ‘Towards a Theory of Cyber Power: The Israeli Experience with Innovation and Strategy’. In *International Conference on Cyber Conflict, CYCON*, 2016-:51–63, 2016. https://doi.org/10.1109/CYCON.2016.7529426.

Taddeo, Mariarosaria. ‘The Limits of Deterrence Theory in Cyberspace’. Edited by Mariarosaria Taddeo and Mariarosaria Taddeo. *Philosophy & Technology* 31, no. 3 (2018): 339–55. https://doi.org/10.1007/s13347-017-0290-2.

Tal, Israel, and Martin Kett. *National Security: The Israeli Experience*. Book, Whole. Westport, Conn: Praeger, 2000.

Tamkin, Emily. ‘10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?’ *Foriegn Policy*, 27 April 2017. https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/.

‘The Arab-Israeli Wars’. Accessed 7 August 2021. https://www.mfa.gov.il/mfa/aboutisrael/history/pages/the%20arab-israeli%20wars.aspx.

'The National Military Strategy For Cyberspace Operations'. United States, Department of Defense, December 2006. file:///C:/Users/u4499315/Downloads/35693%20(1).pdf.

'The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World'. Cabinet Office, Whitehall, November 2011. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

'Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe', 17 February 2021. https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and.

Tor, Uri. '"Cumulative Deterrence" as a New Paradigm for Cyber Deterrence'. *Journal of Strategic Studies* 40, no. 1–2 (2 January 2017): 92–117. https://doi.org/10.1080/01402390.2015.1115975.

Tritten, James John, and Paul Stockton. *Reconstituting America's Defense: The New U.S. National Security Strategy*. Book, Whole. New York: Praeger, 1992.

Trump, Donald J. 'National Security Strategy Of the United States of America'. White House, United States of America, December 2017. https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

'Two Eyes for an Eye; Israel's Military Strategy'. *The Economist (London)* 390, no. 8613 (2009): 23.

'UNIDIR Cyber Policy Portal: Collation of State's Cyber Security Policies', n.d. https://unidir.org/cpp/en/.

'U.S. Cyber Command - U.S. Strategic Command', 16 April 2014. https://web.archive.org/web/20140416192156/http:/www.stratcom.mil/factsheets/2/Cyber_Command/.

'U.S. Department Of Homeland Security Cybersecurity Strategy'. U.S. Department of Homeland Security, 15 May 2018. https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf.

'US, Israel Set up Team to Combat Cybersecurity Threat'. *The Times of Israel*. 2017.

'U.S. Mulls Putting N. Korea Back on Terror Sponsor List [UPDATE1]'. *Kyodo News Service*. 2017.

'U.S. Strategic Command, The Cyber Warfare Lexicon: A Language to Support the Development, Testing, Planning and Employment of Cyber Weapons and Other Modern Warfare Capabilities, January 5, 2009. Unclassified/For Official Use Only. | National Security Archive'. Accessed 10 September 2021. https://nsarchive.gwu.edu/document/21360-document-1.

'USCYBERCOM Vision April 2018.Pdf'. Accessed 24 June 2021. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf.

Uz Zaman, Rashed. 'Strategic Culture: A "Cultural" Understanding of War'. *Comparative Strategy* 28, no. 1 (18 February 2009): 68–88. https://doi.org/10.1080/01495930802679785.

Van Maanen, John, Ed. 'Reclaiming Qualitative Methods for Organizational Research: A Preface'. Edited by John Van Maanen. *Administrative Science Quarterly* 24, no. 4 (1979): 520–26. https://doi.org/10.2307/2392358.

Walsh, Joe. 'Here Are Some Of The Major Hacks The U.S. Blamed On Russia In The Last Year'. Forbes. Accessed 24 June 2021. https://www.forbes.com/sites/joewalsh/2021/06/01/here-are-some-of-the-major-hacks-the-us-blamed-on-russia-in-the-last-year/.

Walt, Stephen M. 'Is the Cyber Threat Overblown?' *Foriegn Policy*, 30 March 2010. https://foreignpolicy.com/2010/03/30/is-the-cyber-threat-overblown/.

Waltz, Kenneth. 'The Spread of Nuclear Weapons: More May Be Better'. *International Institute for Strategic Studies*, Adelphi Papers, 171 (1981). https://www.mtholyoke.edu/acad/intrel/waltz1.htm.

'What Israel's Strike on Hamas Hackers Means For Cyberwar | WIRED'. Accessed 25 June 2021. https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/.

'Why "Overmatch" Is Overkill | The Nation'. Accessed 24 June 2021. https://www.thenation.com/article/archive/overmatch-pentagon-military-budget-strategy/.

Williams, Brad D. 'US Urges "Like-Minded" Countries To Collaborate On Cyber Deterrence'. *Breaking Defense* (blog), 24 April 2019. https://breakingdefense.sites.breakingmedia.com/2019/04/us-urging-likeminded-countries-to-collaborate-on-cyber-deterrence/.

Williams, Paul. *Security Studies: An Introduction*. Book, Whole. London;New York; Routledge, 2008.

Willis, Ben. 'The Advantages and Limitations of Single Case Study Analysis'. *International Relations*, n.d., 7.

Wilner, Alex S. 'US Cyber Deterrence: Practice Guiding Theory'. *Journal of Strategic Studies* 43, no. 2 (2019 2020): 245–80. https://doi.org/10.1080/01402390.2018.1563779.

Woodside, Arch G. *Case Study Research: Theory, Methods, Practice*. Emerald Group Publishing, 2010.

Wong, Alex Seven Questions: Richard Clarke on the Next Cyber Pearl Harbor, Foreign Policy, April 2 2008, https://foreignpolicy.com/2008/04/02/seven-questions-richard-clarke-on-the-next-cyber-pearl-harbor/

Yin, Robert K. *Case Study Research and Applications: Design and Methods*. 6th ed. Los Angeles: Sage Publications, 2018.

———. *Case Study Research: Design and Methods*. 4th ed. Vol. 5. Book, Whole. Los Angeles, Calif: Sage Publications, 2009.

Zahav, Sally. 'Middle East and Terrorism: IDF Blog: The Attack against Israel You Haven't Heard About'. *Middle East and Terrorism* (blog), 27 August 2014. http://israelagainstterror.blogspot.com/2014/08/idf-blog-attack-against-israel-you.html.

Zurkus, Kacy. 'Netanyahu Boasts of Israel's Cyber Intelligence'. Infosecurity Magazine, 26 June 2019. https://www.infosecurity-magazine.com/news/netanyahu-boasts-of-israels-cyber-1/.

Appendices

Appendix A: Research Participants

Available to examiners only.