8-22-2023 12:00 PM

NATO Cyber Defence, 2000-2022

Ryan J. Atkinson, *Western University*

Supervisor: Simpson, Erika, *The University of Western Ontario*

A thesis submitted in partial fulfillment of the requirements for the Doctor of Philosophy degree in Political Science

Abstract

The emergence of more devastating and organized cyber attacks by non-attributable threat actors internationally raises questions about whether classical deterrence theory in its contemporary form has assisted important military defence alliances, like the North Atlantic Treaty Organization (NATO), to adapt to the changing threat landscape. The timeline of the NATO Alliance's adaptation to external cyber threats is examined at critical historical junctures. Changes and adaptation within internal policy-making processes at NATO headquarters and its affiliated centres, think tanks, and military bases are analysed with input from informed decision-makers. The research project demonstrates that NATO policy substantively changed over the period 2000 to June 30, 2022 because the scale and measure of cyber capabilities among 30 NATO Allies (particularly during and after the COVID-19 pandemic) contributed to a two-decade pattern of increasing defensive preparations, including new technologies, extensive military exercises, and military planning intended to counter amplifying hybrid threats in the 'gray zone' of conventional warfare. NATO implemented different security solutions to cyber space challenges, demonstrating the application of contemporary deterrence theory to current policy. Critical junctures, like major international precedent-setting cyber attacks, influenced cyber defence policy developments at NATO and internal policymaking processes like NATO Summitry. Two conceptual lenses—historical institutionalism and social learning—illuminate understanding of the evolution of NATO's policy development, military exercises, and the training initiatives of affiliated NATO organizations over the period 2000-2022.

Keywords

NATO, Cyber, Policy, Deterrence, Cyber Security, Cyber Defence, North Atlantic Treaty Organization, Transatlantic, Hybrid Threats, Social Learning, Historical Institutionalism

Summary for Lay Audience

Threat actors have become more coordinated and destructive in their cyber attacks. This challenge raises questions about whether conventional deterrence theory has aided military defence alliances, including the North Atlantic Treaty Organization (NATO), in adapting to this shifting threat environment. This study looked at how NATO has dealt with cyber threats from the outside to examine how its internal policy-making procedures have changed and evolved. The chronology of NATO's policy development was analyzed in response to cyber threats by looking at significant historical events and speaking with experienced decision-makers. NATO's strategy changed dramatically between 2000 and June 30, 2022, principally due to the NATO Allies' growing cyber capabilities. The study reveals a recurring pattern of NATO's defensive preparations, including adopting new technology, military exercises, and strategic planning. In order to confront the threats posed by cyberspace, NATO has established many security measures, demonstrating how modern deterrence has been used to influence current policy. Notably, pivotal global cyberattacks have shaped NATO's internal policymaking procedures, such as NATO Summitry and cyber defence strategies. This research study illuminates how NATO has modified its processes and policies to address the growing cyber threats it confronts.

Acknowledgements

I am deeply grateful to my supervisor, Dr. Erika Simpson, for her invaluable guidance and support throughout my doctorate, which shaped the success of the research development.

I sincerely thank advisory committee members, Dr. David Armstrong and Dr. Bruce Morrison for their insightful comments and helpful criticism supporting program requirements.

To the Department of Political Science at Western University, I sincerely appreciate the stimulating academic environment and opportunities to develop scholarly expertise.

Thank you to the Ontario Graduate Scholarship and the Department of Political Science at Western University for the financial support of my dissertation research and completion of program requirements.

Thank you to the research participants for contributing time, wisdom, and perspective.

I sincerely appreciate my family's unwavering dedication, patience, and motivation. This manuscript is dedicated to my parents.

Contents

Figures

Abbreviations

4GW - Fourth Generation Warfare
ACO - NATO Allied Command Operations
ACT - NATO Allied Command Transformation
AOM - Alliance Operations and Missions
APT - Advanced Persistent Threats
C3B - Command, Control, and Communication Board
CCDCOE - Cooperative Cyber Defence Centre of Excellence
CD - Cyber Defence
CDC - Cyber Defence Committee
CDD - Cross-Domain Deterrence
CDS - Cyber Defence Section
CDMA - Cyber Defence Management Authority
CDMB - Cyber Defence Management Board
CERT - Computer Emergency Response Team
CERT-EU - Computer Emergency Response Team of the European Union
CERT.LV - Information Technology Security Incident Response Institution, Republic of Latvia
CHST - Counter Hybrid Support Team
CIRT - Computer Incident Response Team
CISA - U.S. Cybersecurity and Infrastructure Security Agency
CIICS - Cyber Information and Incident Coordination System
CIS - Communications Information Systems
CMX - Crisis Management Exercise
COE - Centre of Excellence
CSSL - Cyber Security Service Line
CyCon - International Conference on Cyber Conflict
DCB - Defence Capacity Building
DCO - Defensive Cyber Operations
DDoS - Distributed Denial of Service Attacks
EEAS - European External Action Service
ENISA - European Union Agency for Cybersecurity
ESC - Emergency Security Challenges Division at NATO HQ
EU - European Union
FOC - Full Operational Capability
FSB - Russian Federal Security Service
GRU - Russian Military Intelligence
HTTP - Hypertext Transfer Protocol
ICRC - International Committee of the Red Cross
IMS - International Military Staff
I.S. - International Staff
ITU - International Telecommunications Union
IRA - Russian Internet Research Agency
JALLC - Joint Analysis and Lessons Learned Centre

JTF-NA Task Force Noble Anvil
MC - NATO Military Committee
METU - Middle East Technical University
MISP - Malware Information Sharing Platform
MoD - Ministry of Defence
NAC - North Atlantic Council
NATO - North Atlantic Treaty Organization
NC3A - NATO Consultation, Command, and Control Agency
NCIA - NATO Communication and Information Agency
NCIRC - NATO Computer Incident Response Capability
NCIRC-FOC - NATO Computer Incident Response Capability-Full Operating Capability
NCIRC-TC - NATO Computer Incident Response Capability-Technical Centre
NCIS - NATO Communications Information Service Agency
NCSC - U.K. National Cyber Security Centre
NDPP - NATO Defence Planning Process
NIAS - NATO Information Assurance and Cyber Defence Symposium
NICP - NATO Industry Cyber Partnership
NIST - National Institute of Standards and Technology
NRF - NATO Response Force
NSA - National Security Agency
OCO - Offensive Cyber Operations
OPCW - Organization for the Prohibition of Chemical Weapons
OPS - NATO Operations Division
OPCW - Organization for the Prohibition of Chemical Weapons
PE - Persistent Engagement
PLA - People's Liberation Army, People's Republic of China
PMESII - Political, Military, Economic, Social, Infrastructural, and Informational assets
RAST - NATO Resilience Advisory Support Team
RRT - NATO Cyber Rapid Reaction Team
SACEUR - Supreme Allied Commander Europe
SACT - Supreme Allied Commander Transformation
SDSR - Strategic Defence and Security Review
SHAPE - Supreme Headquarters Allied Powers Europe
SPS - NATO Science for Peace and Security Programme
TTTP - Tools, Tactics, Techniques, and Procedures
UNIDIR - United Nations Institute for Disarmament Research
U.K. - United Kingdom
U.S. - United States
VJTF - Very High Readiness Joint Task Force
V&S - Vision and Strategy

Chapter 1: Theory and Method

1.1 – Puzzle, Question, and Approach

1.1.1 Puzzle

The emergence of threats in the cyber domain raises concerns in North America and Europe about whether classical deterrence theory adequately addresses dangers in the contemporary security environment. The North Atlantic Treaty Organization, or NATO, evolved significantly from 2000 to 2022 as an international organization adapting to a constantly changing threat landscape. NATO Allies, policymakers, and key stakeholders adopted policies and institutions for cyber threats as the Alliance changed and developed over two decades. The project focuses on NATO's changing security doctrine to analyze the extent to which classical deterrence provides the appropriate security solutions to address threats in cyberspace, compared to contemporary deterrence and other new strategic approaches beyond deterrence.

Cyber attacks increased significantly during the COVID-19 pandemic. The United States Federal Bureau of Investigation's Internet Crime Complaint Center received 2,084 reports of ransomware that amounted to $16.8M in losses - a 62-percent increase in cyber incidents in 2022 compared to 2021.[1] The FBI Center reported receiving 4,000 complaints per day, compared to 1,000 per day before the pandemic.[2] The challenge has become increasingly worse as new technologies like artificial intelligence and automated cyber capabilities demonstrate the importance of future interdisciplinary threat research.[3]

---

[1] CISA, "Ransomware Awareness for Holidays and Weekends," *CISA Cyber Security Advisory*, (February 10, 2022), https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-243a.
[2] Maggie Miller, "FBI Sees Spike in Cyber Crime Reports During Coronavirus Pandemic," *The Hill*, (April 16, 2020), https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic/.
[3] Katerina Mavrona and Raluca Csernatoni, "The Artificial Intelligence and Cybersecurity Nexus: Taking Stock of the European Union's Approach," *Carnegie Europe*, (September 15, 2022), https://carnegieeurope.eu/2022/09/15/artificial-intelligence-and-cybersecurity-nexus-taking-stock-of-european-union-s-approach-pub-87886.

The project arbitrarily segments the timeline into four chronological phases, including precedent-setting cyber attacks, significant cyber incidents, and other events. The four phases include Phase A from 2000 to 2006; Phase B from 2007 to 2013; Phase C from 2014 to 2017; and Phase D from 2018 to 2022. The Appendix summarizes all critical junctures in each of the four phases, which includes precedent-setting cyber attacks or significantly related incidents.

The increasing number of cyber attacks in recent years demonstrates that a threatening environment has become even more dangerous. Major precedent-setting cyber attacks are critical junctures which influence cyber defence policy developments at NATO during the timeline. The months and years after significant critical junctures are a major part of the analysis for further policy developments, which include cyber attacks in Kosovo in 1999, Estonia in 2007, Georgia in 2008, Stuxnet in 2010, Crimea in 2014, and Ukraine in 2015-2016, among others.

The project's title, "NATO Cyber Defence, 2000-2022," serves the dual purpose of describing the project's scope and timeline. Strict adherence to the scope and timeline was upheld to ensure the manuscript remains brief and concise. Only areas of interest within the project scope and timeline were subject to discussion related to select events. For an overview of the Author's future research agenda, see the next section, Academic Contribution and Chapter 7.

1.1.2 Academic Contribution

Cyber threats are one focus area within the larger analytic category of hybrid threats, which can include disinformation, economic coercion, energy and climate security, and other more specific areas like the geoeconomics of technological innovation and investment. Hybrid threats target strategic objectives while limiting conflict escalation from reaching conventional military capabilities. Unconventional capabilities operate in the "gray zone" of conflict between

outright war and peace. The risks posed by emerging technologies for security policy and research remain an under-analyzed sub-discipline within the Security Studies literature. These dangers are increasingly pertinent given newly emerging technologies such as artificial intelligence and automation.

The present manuscript primarily includes a descriptive history of the evolution of cyber defence policy at NATO from 2000 to 2022. Theoretical foundations and interdisciplinary methodologies develop policy-relevant approaches to analyzing real-world problems with cutting-edge solutions. The temporal scope of this study ends on June 30, 2022, with the annual NATO Summit in Madrid, Spain. The Madrid Summit Communiqué and the 2022 Strategic Concept are the final policy documents under examination. Both documents were approved by Allies at the Madrid Summit, following drafting during the spring and summer months of 2022.

Proposed future research involves closely analyzing the eight-year timeline of Russian cyber attacks on Ukraine. The project timeline includes the period from February 24 to June 30, 2022. During this period, Russia's invasion and war on Ukraine involved cyber attacks coordinated with conventional military attacks on Ukraine's critical infrastructure. All events occurring after June 30, 2022 - including but not limited to cyber-attacks, NATO policy developments, or other related incidents - are beyond the project's scope and timeline.

Russia conducted numerous precedent-setting cyber attacks on Ukraine after the project timeline. One report noted Russia's increased use of wiper malware - malicious software that erases the hard drive of an infected computer. Ukraine has been targeted by "more specimens of wiper malware than in any previous year of Russia's long-running cyber war targeting Ukraine… the growing volume of destructive code hints at a new kind of cyber war that has accompanied Russia's physical invasion of Ukraine, with a pace and diversity of cyber attacks that is

unprecedented."[4] These unprecedented cyber attacks are beyond the project scope yet remain as recent examples of critical junctures, which are yet to impact future policy-making for research beyond the current project.

1.1.3 Questions

The project analyzes adaptations and applications of deterrence to the contemporary threat landscape. To skip ahead to the Author's answers to these central and supplementary research questions, see Chapter 7.

Central Research Question

The central research question focuses on NATO as a case of an international organization evolving through time as the security environment changes immensely over twenty-two years. The project's central research question asks:

> **How does NATO's evolving strategic deterrence doctrine address contemporary security threats in the cyber domain?**

Supplementary Research Questions

Numerous supplementary research questions support the central question to address specific concerns related to the evolution of NATO cyber defence policy in the contemporary threat landscape, and are divided into three sets of questions based on the subject of focus.

Set One

The first set of supplementary research questions focuses on deterrence as an appropriate strategy to address threats in the cyber domain. Questions concern the application of defence and

[4] Andy Greenberg, "Ukraine Suffered More Data-Wiping Malware in 2022 Than Anywhere, Ever," *Wired*, (February 22, 2023), https://www.wired.com/story/ukraine-russia-wiper-malware/.

deterrence policy to the cyber domain, which requires quick adaptability. The first group of supplementary research questions asks:

> **Is deterrence an appropriate means to address threats in the cyber domain?**
>
> **What are the characteristics of contemporary deterrence that can deter cyber attacks?**
>
> **Compared to other security strategies, is contemporary deterrence the most appropriate security strategy to deter cyber attacks?**

Set Two

A second set of questions analyzes NATO's cyber defence capabilities and internal institutional dynamics. These questions ask:

> **What political and strategic considerations inform the evolution of NATO cyber defence policy?**
>
> **What benefits result from these policy developments?**
>
> **What theoretical approaches underline the implementation of these policy developments?**
>
> **What challenges remain in NATO's Approach to the cyber domain?**

Set Three

A third set of supplementary research questions focuses on NATO's ability to change as a learning organization. These questions unpack the institutional processes to adapt policy and institutional adaptation measures. These questions ask:

> **Is NATO a learning organization which facilitates the Alliance to adapt to the evolving threat landscape?**
>
> **Does NATO adapt policy in response to requirements for change?**
>
> **How do Lessons Learned protocols facilitate approaches to make change within NATO?**

Does NATO implement Lessons Learned into policy and institutional change?

Does social learning occur at NATO beyond the formal Lessons Learned procedures?

Are there affiliated organizations or informal networks to amplify social learning beyond formal Lessons Learned approaches?

NATO Adaptation

A valuable follow-up question asks how NATO's Lessons Learned procedures adapted to threats in the cyber domain through institutional and policy developments. The question asks:

Given that NATO's cyber defence policy addresses evolving threats during the timeline, what are some characteristics to define NATO's adaptation to these threats?

The first follow-up research question expands the project from simply addressing whether or not NATO made changes in response to the threat environment. Instead, the question seeks to address the kinds of changes that NATO conducted over twenty-two years. The thesis proposal defended in May 2021 proposed a descriptive and historical analysis of cyber defence policy change at NATO. The thesis proved that the Alliance evolved through unprecedented historical events influencing policy change and investment. It showed that language in NATO policy documents influences future policy and investment.

The project proved that historical analysis could map past trends and challenges for studies on long-term evolution of international institutions through time. This project demonstrates that external conjunctural events combined with internalized learning can facilitate immense adaptability even in established "legacy" international organizations. NATO provides a valuable case to exemplify that legacy international organizations can evolve. The project shows that NATO sought to adapt to the cyber threat landscape over two decades following significant critical junctures, cyber attacks, and malicious incidents. This manuscript proves that legacy

institutions have adapted to technological change, given that NATO is an established institution. However, this thesis does not claim that the lessons learned herein can be applied to other legacy institutions.

1.1.4 Approach

Security strategy remains conceptually reliant on classical deterrence theory to address contemporary cyber threats. The pressing question is whether such strategies remain appropriate to address an increasingly technologically sophisticated international security environment. The central research question is supported by supplementary research questions focusing specifically on the interrelated factors of NATO's approach to defence and deterrence in cyberspace. Internal institutional dynamics involve a network of committees which impacted the development of NATO cyber defence policy from 2000 to 2022. Future research will continue this analysis beyond the project's end date of June 30, 2022. It is too early to determine how NATO's cyber defence policy or core task of deterrence and defence will be affected by Russia's invasion and war against Ukraine.

Two conceptual lenses identify external critical junctures and other developments in NATO cyber defence policy in the months and years after precedent-setting cyber attacks and related events. The conceptual lenses include historical institutionalism and social learning. Historical institutionalism provides a conceptual lens for identifying significant external developments in the cyber threat landscape as critical junctures. Social learning provides a conceptual lens to identify learning mechanisms in institutions based on cyber defence policy decision-making. Together these two lenses supplement the theoretical approach to analyze contemporary deterrence strategies' impact on NATO cyber defence policy.

Chapters 1 and 2 outline critical concepts, debates, strategic developments, and central stakeholders from diverse state and non-state actors in the contemporary threat environment. These concepts apply to NATO cyber defence policy over more than two decades of the international organization evolving. Precedent-setting critical junctures alter, influence, and change the path dependence of NATO policy development in the cyber domain.

Chapters 3, 4, 5, and 6 analyze the development of NATO cyber defence from 2000-2022. Phases A, B, C, and D outline appropriate stakeholders and policy response measures to address threats in the cyber domain. The conceptual lenses of historical institutionalism and social learning identify challenges in bureaucratic conceptual legacy where applications of classical deterrence theory remain. These conceptual lenses analyze significant policy developments at NATO to understand the influence of critical junctures and internalized learning within an organization's cyber defence policy.

1.1.5 Argument

The following seeks to outline the central and supporting arguments within the manuscript. Note that the relevant citations from which these concepts are derived will be discussed in full detail in respective sections. The arguments are outlined as concisely as possible for clarity, and future discussion is saved for the literature review where relevant sources are discussed. The central argument is:

> Deterrence theory is challenged by external pressures best understood as critical junctures, prompted by increased cyber attacks, and guided by social learning process.

The central and supporting arguments are detailed. External threats in the cyber domain challenge applications of classical deterrence theory to related policy development. Legacy

organization like NATO can foster social learning to do more than react to critical junctures - it can learn to adapt to them to become stronger. Institutions that are path dependent are self-reinforcing and the absence of change is the status quo.

External events significantly impact the path dependence of an institution, and can cause critical junctures which effect the internal change of the formerly self-reinforcing and unchanging status quo. External events that cause critical junctures can impact the permissive conditions within an institution, to spark the potential for change in a previously unchanging institution. The specific kind of change within the institution results from productive conditions, where learning and policy can flourish by disruptions to self-reinforcing mechanisms.

Social learning can produce outcomes of internal policy development and decision making due to critical junctures ridding constraints that previously prevented change. Learning environments facilitate organizational change through new knowledge, observation, and feedback. Significant internal organizational change is observable through a study of historic critical junctures, and historical institutionalism demonstrates unprecedented external events facilitating the conditions for learning to occur within an institution.

NATO provides the unique case to study external events, critical junctures, permissive and possible conditions, and policy change facilitated by learning. The “productive conditions” of Hillel Soifer apply the “puzzling” of Peter Hall to demonstrate how social learning took place at NATO. The cyber challenge to classical deterrence depicts empirical evidence of significant gaps in security strategy and requires further examination for future research.

1.2 – Qualitative Research Method and Data Collection

1.2.1 Elite Interviews

The evolution of NATO cyber defence policy examines initial developments beginning in 2000 and depicts numerous other critical junctures up to the Summit in June 2022. A qualitative research method focuses on data from elite semi-structured interviews, archival research, and other approaches. Author and Ph.D. candidate Ryan J. Atkinson conducted the semi-structured elite interviews to garner qualitative data for the multi-phase policy analysis. Research participants include mid-level and senior-level policy officials and field experts specifically focusing on NATO cyber defence policy and related disciplines.

1.2.2 Archival Research

Archival research includes primary resources on significant cyber defence policy developments at NATO. These resources are available publicly online at the websites of each institution. The *NATO Multimedia Library and Public Archives* provide public access to key policy documents. The *Strategy and Governance Archive* of the NATO Cooperative Cyber Defence Centre of Excellence, or the CCDCOE, provides numerous public accesses to primary NATO policy documents, speeches, reports, and other documents.[5] The *Cyber Policy Portal* of the United Nations Institute for Disarmament Research provides public access to reference materials on Allies' cyber defence and other subjects.[6] The *National Cyber Security Strategies Archive* of the European Union Agency for Cybersecurity includes publicly available policy

[5] CCDCOE, "Strategy and Governance Archive," https://ccdcoe.org/library/strategy-and-governance/.
[6] UNIDIR, "Cyber Policy Portal," United Nations Institute for Disarmament Research, https://cyberpolicyportal.org/.

documents and related research reports on the developments of cyber defence by Allies.[7] Different primary sources include publicly available resources on NATO's main webpage, including Summit Documents, speeches, strategic frameworks, reports, backgrounders, fact sheets, and other related policy communications.[8]

1.2.3 Data Collection

Data collection for elite interviews on NATO cyber defence policy includes research participants at mid-level and senior-level positions, elite policymakers at NATO, and other field experts. Atkinson conducted 21 interviews between 30 minutes and 1 hour in public places like cafeterias and libraries.[9] WesternRem (WREM/formerly WREB) agreed to a list of interview questions before selecting interviewees.[10] Each research participant verbally consented to be listed by name, title, institution, date, and interview location in a collected list in the Appendix.

Each research participant verbally requested not to be directly quoted, named, or identified within the text beyond the Appendix. All interviews conducted by the Author for this study are introduced in-text as "interviews conducted for this study." Each research participant is addressed in-text as "NATO Official" followed by the number used in the interviewer's transcripts to identify the research participant (e.g., NATO Official 1). The private information of research participants is kept confidential. Each research participant is referred to by a number

[7] ENISA, “National Cyber Security Strategies - Interactive Map,” NCSS Map, European Union Agency for Cybersecurity, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.
[8] Alexander Klimburg, “National Cyber Security Framework Manual,” NATO Cooperative Cyber Defence Centre of Excellence, (2012), https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf.
[9] An alphabetized list of research participants is included in the Appendix.
[10] Interview questions are listed in the Appendix. Officials interviewed by others are cited as secondary sources in the footnotes (e.g., interviews cited in various news media sources, press releases, etc.).

assigned to them randomly. These randomized reference numbers do not correspond with the order of the alphabetized list of interviewees in the Appendix.

1.3 – Key Concepts

For twenty-two years, internal NATO cyber defence policy developed within an external evolving threat landscape. Figure 1.1 outlines the multi-level threat environment to demonstrate the interconnection between landscape segments. Figure 1.2 outlines the general differences between the capabilities of various threat levels, depending on the presence or absence of distinct categories of modern warfare. This visual depiction of the threat levels provides the ability to isolate one from the others, to support the goal of the specific research question of this project.

The present study is primarily focused on cyber threats. Distinct threat levels can be segmented to focus on the main differences in cyber, non-conventional, conventional, or nuclear challenges. Together, Figure 1.1 and Figure 1.2 demonstrate the ability to isolate concepts for analysis. Both figures isolate the cyber category specifically and demonstrate critical features within the project's scope and timeline. Key concepts listed as part of contemporary warfare in Figures 1.1 and 1.2 are defined in 1.3.1.

Figure 1.1 – Contemporary Threat Levels

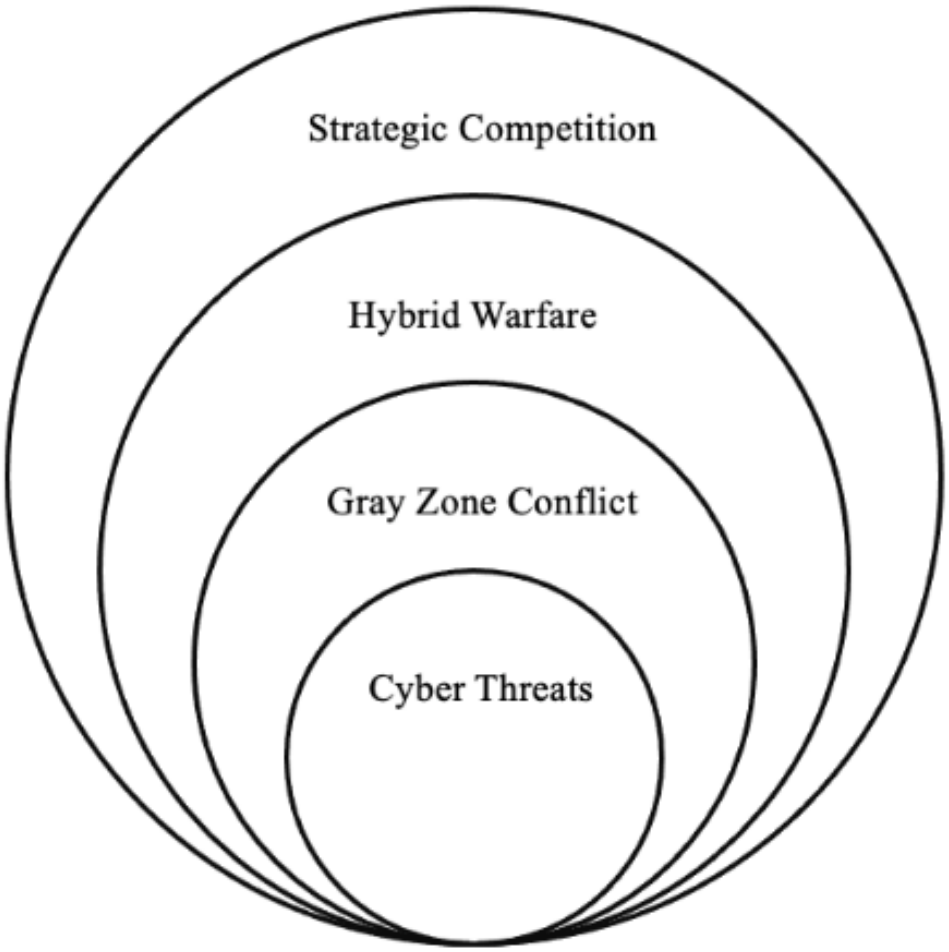


Figure 1.2 – Threat Level Capabilities

Threat Levels and Capabilities	Cyber	Non-Conventional	Conventional	Nuclear
Strategic Competition	Yes	Yes	Yes	Yes
Hybrid Warfare	Yes	Yes	Yes, but with intentions to limit escalation	No
Gray Zone Conflict	Yes	Yes	No	No
Cyber Threats	Yes	Yes	Yes	Yes

1.3.1 Cyber Threats

The increasing use of cyber attacks and malicious cyber incidents during the COVID-19 pandemic includes fraudulent phishing emails to amplify an individual's fear and panic of the coronavirus to target stolen credentials. A central motivation of cyber threat actors during the COVID-19 pandemic was "reconnaissance activity," to target research institutions to steal vaccine research and related innovations, according to Tonya Ugoretz, Deputy Assistant Director of the FBI's Cyber Division.[11] Interpol reported 907,000 spam communications, 737 malware

[11] Miller, "FBI Sees Spike in Cyber Crime Reports during Coronavirus Pandemic."

incidents, and 48,000 malicious links "all related to COVID-19" over four months, from January to April 2020.[12] These pandemic-related cases demonstrate the need for flexible, adaptable, and malleable cyber defence strategies to adapt to emerging crises as they arise.

The December 2021 edition of the NATO Standardization Office's *Glossary of Terms and Definitions* defines "cyber space" as "the global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those… which process, store or transmit data."[13] To avoid confusion, terms like "cyber domain" or "cyber space" are interchangeable to refer to the digital environment and related physical infrastructure.[14] The cyber domain includes “independent networks of information systems infrastructure… the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”[15]

Uniquely, cyber capabilities are present in all domains of military operations. The land domain includes physical infrastructure and hardware in geographical locations. The sea domain includes fibre optic cables beneath the oceans. The air and space domains include satellite telecommunication infrastructure in the sky. NATO included cyberspace as a domain of military operations at the Warsaw Summit in 2016. Cyber threats include all challenges, dangers, incidents, and attacks targeting the cyber domain. NATO defines a "cyberspace attack" as "an act or action initiated in or through cyberspace to cause harmful effects."[16] The Canadian Centre for

[12] INTERPOL, “INTERPOL Report Shows Alarming Rate of Cyberattacks during COVID-19,” INTERPOL, (August 4, 2020), https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19.
[13] NATO Standardization Office, “Cyber Space,” in *NATO Glossary of Terms and Definitions*, (Brussels, NATO, December 2021), https://standards.globalspec.com/std/14486494/AAP-06.
[14] Richard A. Clarke and Robert K. Knake, *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats* (London: Penguin Press, 2019): 15.
[15] NIST, “Cyberspace,” in *Computer Security Resource Centre*, https://csrc.nist.gov/glossary/term/cyberspace.
[16] NATO Standardization Office, “Cyber Space Attack,” in *NATO Glossary of Terms and* Definitions, (Brussels, NATO, 2021), https://standards.globalspec.com/std/14486494/AAP-06.

Cyber Security defines a "cyber threat" as a "threat actor, using the Internet, who takes advantage of a known vulnerability in a product to exploit a network and the information the network carries."[17] The Canadian Cyber Centre also refers to a "cyber attack" as the "use of electronic means to interrupt, manipulate, destroy or gain unauthorized access to a computer system, network, or device."[18]

Threats in the cyber domain are increasingly diverse in terms of the kinds of threat actors involved. Malicious low-impact cyber incidents relentlessly target Allies in extensive campaigns involving "theft or exploitation of data, disruption or denial of access or service, and destructive action… corruption, manipulation, and damage or alteration of data."[19] Threats in the cyber domain suggest more complications in the threat landscape, given increasing malicious cyber activities from an increasingly diverse set of threat actors, including states, state-sponsored proxies, and non-state groups.[20]

1.3.2 Gray Zone Conflict

Gray zone conflict involves using unconventional capabilities to operate below the threshold of conventional operations to avoid the escalation of a military response.[21] The Center for Strategic and International Studies defines gray zone conflict as "an effort or series of efforts… to advance one's security objectives at the expense of a rival... to avoid crossing a

[17] CCCS, "Cyber Threat," *Canadian Centre for Cyber Security Glossary*, (Ottawa: CCCS, July 30, 2023), https://www.cyber.gc.ca/en/glossary#c.
[18] CCCS, "Cyber Attack," *Canadian Centre for Cyber Security Glossary*, (Ottawa: CCCS, July 30, 2020), https://www.canada.ca/en/global-affairs/news/2020/07/canada-welcomes-european-unions-announcement-of-new-cyber-sanctions-listings.html.
[19] Scott Jasper, *Strategic Cyber Deterrence: The Active Cyber Defense Option,* 5.
[20] CCCS, "Cyber Threat."
[21] Lyle J. Morris et al., "Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War" (RAND Corporation, June 27, 2019): 6, https://www.rand.org/pubs/research_reports/RR2942.html.

threshold that results in open war."[22] Key features of the concept include strategies to target a competitor to attain objectives while limiting the use of military capabilities to avoid a conventional response.[23]

The cyber domain limits the sharpness of the distinction between civilian and military personnel, as the line is blurred between combatants, non-combatants, war, peace, and specific operational domains.[24] Strategic goals are achieved with “situational ambiguity” using only “low intensity” means.[25] Strategic objectives occur "below the threshold of aggressive military forces" to control escalation and strategic ambiguity such that identifiable information of gray zone operators remains hidden.[26] Gray zone conflict involves "coercive tools," including information operations, disinformation, economic coercion, and cyber capabilities.[27] The toolbox approach includes additional capabilities to attain strategic ends short of conventional war, using political and strategic objectives to blend conventional and non-conventional capabilities.

1.3.3 Hybrid Warfare

Although the Peloponnesian War, American Revolution, and Napoleonic Wars all include notable historical cases of hybrid warfare, the present study focuses on the simultaneous use of irregular fighting methods, sophisticated weapons, mixed battlefields[28], and irregular

---

[22] Kathleen H. Hicks and Melissa Dalton, “By Other Means: U.S. Priorities in the Gray Zone,” *Center for Strategic and International Studies*, (Washington, D.C.: Rowman & Littlefield, 2019): 2.
[23] Morris et al., *Gaining Competitive Advantage in the Gray Zone*, 7.
[24] William J. Lind et al., “The Changing Face of War: Into the Fourth Generation,” *Marine Corps Gazette* 73, no. 10 (1989), https://www.academia.edu/7964013/The_Changing_Face_of_War_Into_the_Fourth_Generation.
[25] Dani Belo and David Carment, “Grey Zone Conflict: Implications for Conflict Management,” *CGAI Policy Perspective*, (2019): 25, https://www.cgai.ca/grey_zone_conflict_implications_for_conflict_management.
[26] Frank G. Hoffman, “The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War,” *The Heritage Foundation*, (2016): 26.
[27] Hicks and Dalton, *By Other Means*, 2.
[28] Mixed battlefields involve a diverse set of domains which together amount collectively to the various fronts involved in the contentious dynamic. Concepts like Cross Domain Deterrence and Multi Domain Operations seek to

tactics.[29] Threat actors are increasingly diversified with cheap yet complicated capabilities paving the way for "the rise of non-state actors, information technology, and the proliferation of advanced weapons systems."[30]

Modern technology amplifies hybrid warfare beyond cyber threats to include strategic communications, information operations, disinformation, cyber-attacks, and other applications of technological innovation to collective defence.[31] Hybrid warfare is characterized by the different operational capacities which can be combined to achieve strategic goals. Coordinated decision-making combines operational in-field assets with other hybrid capabilities deployed for covert operations. Non-kinetic operations attain strategic objectives below conventional thresholds through information operations and cyber capabilities, which prevent escalation to military confrontation. Non-kinetic operations can be understood as "strategies and tactics" which use "non-lethal" or "sub-lethal… weapons not intended to be lethal."[32] D'Antonio and colleagues outline non-kinetic operations used by the United States military and include "peacekeeping, humanitarian assistance and disaster relief, national integrity operations, and military contingency operations."[33]

NATO cyber defence policy includes interrelating factors within each of the four threat levels: cyber threats, hybrid warfare, gray zone conflict, and strategic competition. NATO launched Operation Enhanced Forced Presence to respond to Russia's operations in Crimea, the

address these related challenges posed by mixed battlefields, where no one approach to a domain can achieve ultimate success alone, and numerous domains are used to tailor objectives to the competitor.
[29] Murray Williamson and Peter R. Mansoor, *Hybrid Warfare: Fighting Complex Opponents From The Ancient World To The Present,* (Cambridge: Cambridge University Press, 2012): 3.
[30] Alex Deep, "Hybrid War: Old Concept, New Techniques," *Small Wars Journal*, (February 3, 2015), https://smallwarsjournal.com/jrnl/art/hybrid-war-old-concept-new-techniques.
[31] Ibid.
[32] Collin D'Antonio, Stephanie Gower, Andrea Young, and Edward Teague, "Non-Kinetic Operations for Stabilizing Government," in *2014 Systems and Information Engineering Design Symposium*, (2014): 90–95.
[33] Ibid.

Baltics, and Eastern Europe.[34] To advance technological capabilities and enhance policy development, hybrid threats pose a fundamental challenge that NATO must overcome.[35] Russia's mixed use of conventional and non-conventional capabilities during the annexation of Crimea and the war in Donbas in 2014 brought debates about concepts like hybrid warfare back to the fore. Examples of non-conventional capabilities at work in the case of Crimea included the use of cyber attacks, targeted disinformation, covert special forces, the use of irregular forces, and conventional military operations. In practice, this amounted to cyber attacks targeting media outlets using pro-Russian media sources to promote anti-Kyiv narratives. At this time, unmarked special forces are mobilized to crucial strategic locations while maintaining a sizeable military troop presence through exercises on the border separating Ukraine from Russia.

Conventional and non-conventional approaches combine to attain strategic objectives, given that the latter alone "will not fully achieve the desired outcome."[36] Crucial differences remain between gray zone conflict and hybrid warfare despite surface-level similarities. Gray zone conflict relies on “entirely unconventional tools and tactics… propaganda campaigns, economic pressure, and the use of non-state entities, which do not cross the threshold of formalized state-level aggression.”[37] Hybrid warfare blends unconventional capabilities with conventional capabilities limiting escalation to avoid military response. Hybrid warfare includes the tools and tactics of gray zone conflict with access to conventional capabilities.

---

[34] Ryan Atkinson, “From Reassurance to Deterrence: Canada’s Contribution to NATO Operations in Central and Eastern Europe,” *NATO Association of Canada*, (February 4, 2017), https://natoassociation.ca/from-reassurance-to-deterrence-canadas-contribution-to-nato-operations-in-central-and-eastern-europe/.
[35] Ryan Atkinson and Erika Simpson, “Hybrid Warfare NATO’s Next Headache,” *London Free Press*, (February 28, 2020), https://lfpress.com/opinion/columnists/simpson-hybrid-warfare-natos-next-headache.
[36] David Carment and Dani Belo, “Gray Zone Conflict Management: Theory, Evidence, and Challenges,” *Journal of European, Middle Eastern, & African Affairs*, (2020).
[37] Ibid.

The 2021 version of the NATO Standardization Office *Glossary of Terms and Definitions* include the 2018 "hybrid threats" definition as a "type of threat that combines conventional, irregular, and asymmetric activities in time and space."[38] Irrespective of whether the phenomenon is called ‘hybrid warfare,’ ‘hybrid threats,’ or ‘hybrid challenges,’ it involves conventional and unconventional forces which achieve strategic and tactical objectives while limiting conflict escalation.[39]

Hybrid warfare involves kinetic and non-kinetic capabilities to attain strategic objectives, where kinetic capabilities use strategies to protect “critical infrastructure from adversaries, military force… against opposing forces or objectives with… lethal effects in the physical domain.”[40] Non-kinetic capabilities target the “application of [military and non-military] capabilities… to generate… non-kinetic effects in the non-physical and physical domain.”[41] State-of-the-art technology “synchronizes multiple instruments of power simultaneously to intentionally exploit creativity, ambiguity, non-linearity and the cognitive elements of warfare.”[42] Regular and irregular forces are part of a hybrid toolbox approach that is specific to features of geography, strategic objectives, and tactical opportunities.

[38] NATO Standardization Office, “Hybrid Threats,” in *NATO Glossary of Terms and Definitions,* (Brussels, NATO, 2021), https://standards.globalspec.com/std/14486494/AAP-06.
[39] Frank G. Hoffman, “Conflict in the 21st Century: The Rise of Hybrid Wars,” *Potomac Institute,* (Arlington, Potomac Institute: 2007): 8, https://potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.
[40] P. L. Ducheine, “Non-Kinetic Capabilities: Complementing the Kinetic Prevalence to Targeting,” *Amsterdam Law School Research Paper*, (July 30, 2014), https://papers.ssrn.com/abstract=2474091.
[41] Ducheine, “Non-Kinetic Capabilities.”
[42] Patrick Cullen and Erik Reichborn-Kjennerud, “Understanding Hybrid Warfare,” *Multinational Capability Development Campaign*, (2017): 8.

1.3.4 Strategic Competition

NATO approved the 2022 Strategic Concept at the Madrid Summit in Spain.[43] The concept includes language to address the challenge of "strategic competition" against the "interests, values, and democratic way of life" of NATO Allies. The concept referenced the threat of authoritarian states to:

> Interfere in democratic processes and institutions and target the security of our citizens through hybrid tactics, both directly and through proxies. Malicious activities included conduct alongside others, such as promoting disinformation campaigns, instrumentalizing migration, manipulating energy supplies, or employing economic coercion. These actors are also at the forefront of a deliberate effort to undermine multilateral norms and institutions and promote authoritarian governance models.

The comprehensive nature of the threat environment adapted the application of the concept of strategic competition to NATO's core task of deterrence and defence. Paragraph 20 states:

> While NATO is a defensive Alliance, no one should doubt our strength and resolve to defend every inch of Allied territory, preserve all Allies' sovereignty and territorial integrity and prevail against any aggressor. In an environment of strategic competition, we will enhance our global awareness and reach to deter, defend, contest and deny across all domains and directions, in line with our 360-degree Approach.

Paragraph 20 outlines that NATO's deterrence and defence are "based on an appropriate mix of nuclear, conventional and missile defence capabilities, complemented by space and cyber capabilities."[44] This sentiment demonstrates the influence of cross-domain deterrence on senior decision-makers. The threat of using force targets distinct areas with specific designs to significantly impact a competitor, irrespective of whether the response is contained within the

[43] NATO, "NATO 2022 Strategic Concept," (June 29, 2022), 3, https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf.
[44] Ibid.

same domain as the attack. The cross-domain approach applies tools available on a case-by-case basis, such that distinct domains of warfare deter a threat actor from carrying out some action.

Cross-domain deterrence is applied throughout Phases A, B, C, and D as part of developing NATO's cyber defence. The 2022 Madrid Strategic Concept includes language to demonstrate the influence of cross-domain deterrence as part of the continuous evolution and development of NATO cyber defence policy. Paragraph 20 provides NATO with the means to "employ military and non-military tools in a proportionate, preferent, and integrated way to respond to all threats to our security in the manner, timing and… domain of our choosing."[45] NATO remains ambiguous about responses to significant cyber attacks against an Ally, and this requires taking added steps to ensure the perceived credibility of the response option.[46] The concept includes “economic and political values, cultural influences… rules and norms embodied in international law, agreements, practice, and… standards reflected in international institutions.”[47]

According to Michael J. Mazar, Senior Political Scientist at the RAND Corporation, competition shapes the global international system "to predominate influence over the reigning global paradigm.”[48] Mazar adds that global competition impacts the affairs of states by shaping “the surrounding geopolitical context, and indeed the larger socioeconomic environment, to their benefit, gains tremendous competitive advantage."[49] Global strategic competition achieves objectives while avoiding escalation, incorporating "geopolitical, technological, military,

[45] Ibid.
[46] Thomas Rid, “Escalation, Not Deterrence,” *Medium*, (July 2, 2014), https://medium.com/@ridt/escalation-not-deterrence-f0ddf055d4c7. A professor at Johns Hopkins School of Advanced International Studies, Dr. Thomas Rid, wrote the blog article during the 2014 NATO Wales Summit. The article provides a field expert's immediate response and perspective on NATO, including cyber defence as part of collective defence.
[47] Michael J. Mazarr, “The Essence of the Strategic Competition with China,” *PRISM* 9, no. 1 (2020): 3.
[48] Ibid.
[49] Michael J. Mazarr, “Understanding Competition: Great Power Rivalry in a Changing International Order,” *RAND Corporation*, (2022): 36, https://doi.org/10.7249/PEA1404-1.

economic, and other areas… to constrain [a] competitor's strategic options and choices."[50] The competitive dynamic of the cyber domain is described as a state of "unpeace" by Lucas Kello, Associate Professor of International Relations at Oxford University.[51] Kello argues that the "mid-spectrum rivalry" can be more "damaging than traditional peacetime activity (such as economic sanctions), but not physically violent like war."[52]

1.3.5 Merits and Limitations

During interviews for this study, NATO Officials address the merits and limitations of hybrid warfare as a concept for NATO policymaking. In an interview for this study, NATO Official 8 argues that Western concepts cannot on their own analyze Russian strategic operations. The concept of hybrid warfare limits other theoretical support to provide a history of local state military strategy. In another interview for this study, NATO Official 12 adds that there remains a need to understand the concept of hybrid warfare and the complete array of Russian military activity at every level of operations as the information becomes available.

The approach understands the unique features of the dangerous blend of kinetic and non-kinetic forces with cutting-edge technology to attain political and military objectives. In an interview for this study, NATO Official 1 argues that countermeasures to hybrid threats require deconstructing the concept of hybrid warfare. The Official adds that despite the unique mix of kinetic and non-kinetic operations in hybrid warfare, the change in physical geopolitical status quo remains highly dependent on kinetic capabilities. Unconventional operations are central to

[50] Michael Raska, "Strategic Competition for Emerging Military Technologies: Comparative Paths and Patterns," *PRISM* 8, no. 3 (2019): 67.
[51] Lucas Kello, *The Virtual Weapon and International Order* (New Haven: Yale University Press, 2017): 17.
[52] Ibid.

pre-conflict phases to shape the threat environment but remain secondary to a conventional military change in the geopolitical status quo.

1.4 – Cyber Deterrence

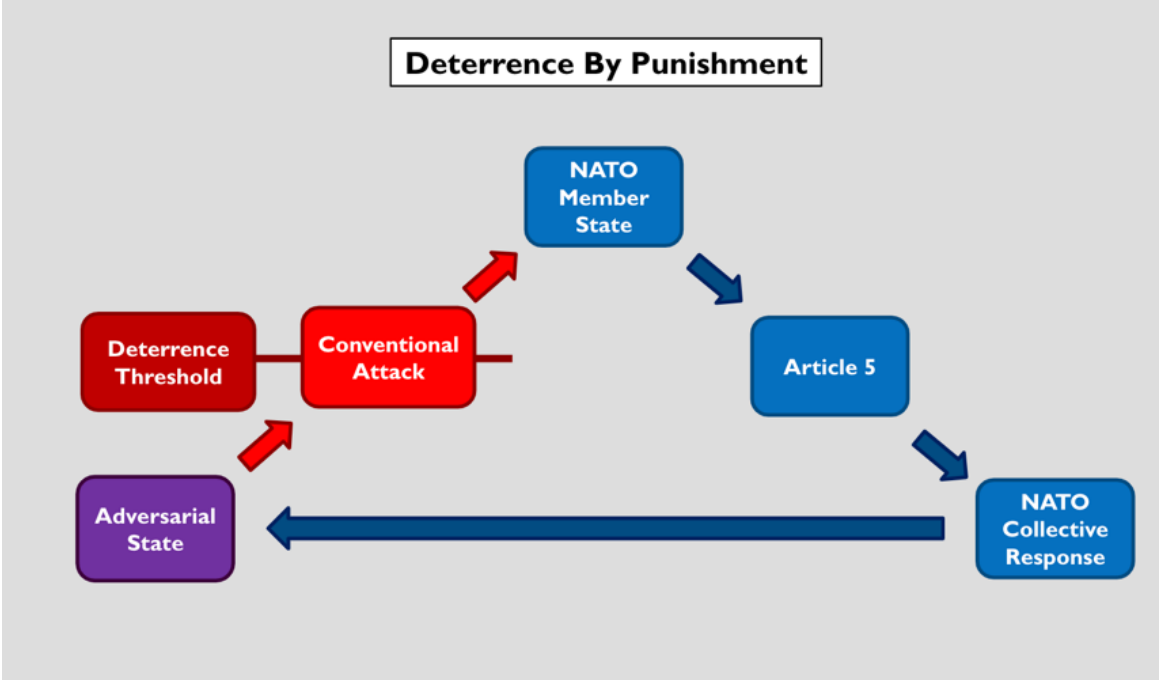
1.4.1 Deterrence By Punishment

Deterrence by punishment is a fundamental feature of classical deterrence theory. A diverse array of threat actors provides the unique challenge to deter adversary behaviour in the cyber domain, raising concerns about whether such behaviours are deterrable.[53] Threats of coercive punishment target decision-making to deter adversary behaviour in the cyber domain.[54] Figure 1.3 outlines a hypothetical set of events for the Alliance to invoke Article 5 when a conventional attack crosses the deterrence threshold.

The consensus of the North Atlantic Council at NATO Headquarters in Brussels, Belgium, decides to invoke Article 5. Over twenty-two years, broadening NATO collective defence includes attacks below conventional deterrence thresholds. Critical questions remain about whether the expansion of collective defence was appropriate to address threats in the cyber domain or whether increased bilateral and multilateral agreements strengthen the Alliance, where NATO facilitates interdisciplinary collaboration as a platform.

[53] Glenn Snyder, *Deterrence and Defense* (Princeton: Princeton University Press, 2016): 108, https://press.princeton.edu/books/hardcover/9780691652092/deterrence-and-defense.
[54] Keisuke Nakao, "Modeling Deterrence by Denial and Punishment," *SSRN Electronic Journal* (2019), https://doi.org/10.2139/ssrn.3419332.

Figure 1.3 – Deterrence By Punishment

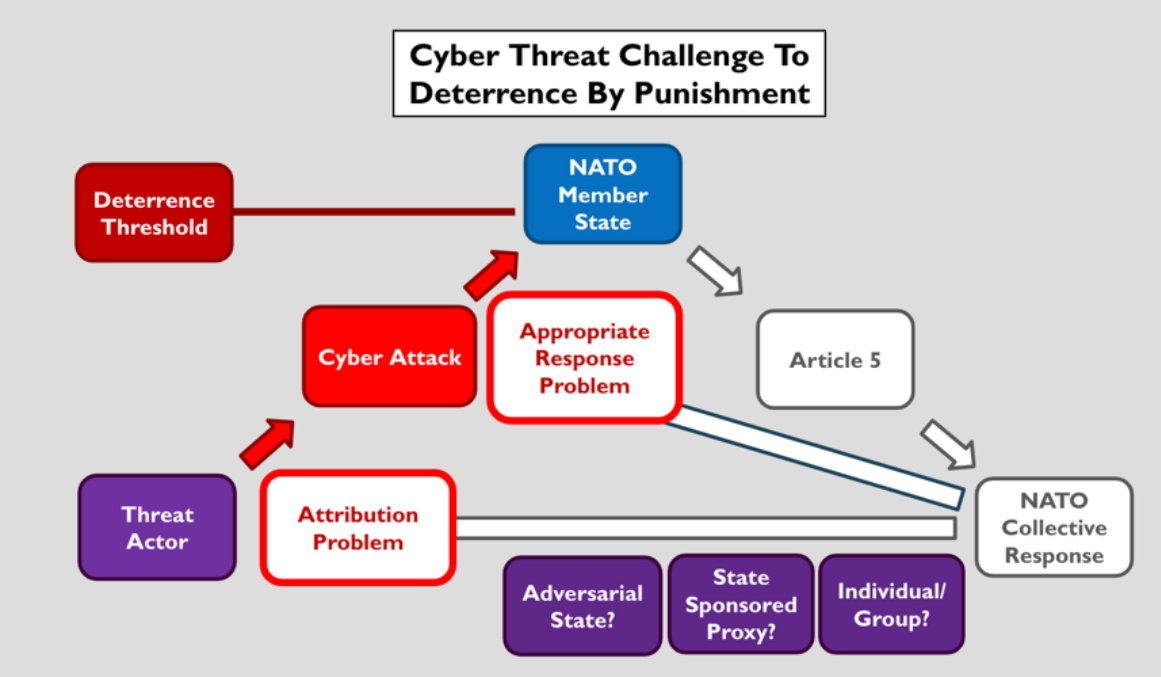


Policy officials face challenges by cyber criminals threatening the avoidance of justice for prolonged periods. Cyber criminals often live in a country without an extradition treaty with the indicting state. Such circumstances suggest legal action is unlikely and will not provide an effective deterrent because a lack of an extradition treaty limits the ability for indictments to bring offenders to justice.[55] It remains to be seen whether cyber criminals remaining in countries without extradition treaties will be held responsible for cyber attacks to deter future actors or

[55] Forrest Hare, "The Significance of Attribution to Cyberspace Coercion: A Political Perspective," *The 4th International Conference on Cyber Conflict*, (Tallinn, NATO CCDCOE, 2012): 127, https://ccdcoe.org/uploads/2012/01/2_5_Hare_TheSignificanceOfAttribution.pdf.

actions.[56] Alternatively, such states become safe havens for organized crime by aligning with the state not to harm state interests.

Figure 1.4 – Cyber Threat Challenge to Deterrence By Punishment



There remain immense challenges to applying deterrence in the cyber domain. Figure 1.4 outlines the attribution problem and appropriate response problem. Both problems complicate the application of deterrence by punishment to the cyber domain. To reach a consensus, the North Atlantic Council must agree to attribute threat actors to design appropriate countermeasures to the circumstances. The credibility of threats provides significant challenges for policy in the cyber domain.

[56] Sandeep Baliga, Ethan Bueno De Mesquita, and Alexander Wolitzky, "Deterrence with Imperfect Attribution," *American Political Science Review* 114, no. 4 (November 2020): 1164.

Attackers can prevent identification to "mask the point of origin behind… several remote servers, which can be located in a variety of jurisdictions… [to] use non-state actors as proxies."[57] Threat actors operate with the lessened likelihood of being identified and penalized, eradicating the fear that may otherwise deter them from launching a cyber attack.[58] The attribution problem challenges the identification of attackers to hold them accountable. The appropriate response problem determines the best countermeasures to cause the target the most harm.

1.4.2 Deterrence By Denial

Deterrence by denial seeks to persuade an adversary not to launch an attack based on signals that the defending organization is too strong and resilient for the attack to be worth the effort. An organization is resilient when it can return to operational functioning quickly while ensuring continuity of governance and operations.[59] Cyber resilience increases costs and decreases benefits for threat actors by adopting a deterrence-by-denial approach to "assure that cyber and non-cyber military response options are available for retaliation."[60] An organization can take crucial yet manageable steps to become more resilient by enhancing capabilities to detect and respond to cyber threats.

Strengthening cyber resilience requires the Alliance and member states to increase investment and political will. Defensive measures deny adversaries the ability to establish a

[57] Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (January 2017): 50, https://doi.org/10.1162/ISEC_a_00266.
[58] Nye, "Deterrence and Dissuasion in Cyberspace," 50.
[59] Mike Gallagher, "The State of Deterrence by Denial," *The Washington Quarterly* 42, no. 2 (2019): 35.
[60] Aaron F. Brantly, "The Cyber Deterrence Problem," in *10th International Conference on Cyber Conflict,* (Tallinn, IEEE, 2018): 46.

foothold, using threat hunting to conduct aggressive network defence.[61] A 2019 IBM study found "the average time to identify a [cyber] breach… was 206 days, and the average time to contain a breach was 73 days, for a total of 279 days."[62] Note that it is over nine months of unrestricted access to an organization's network without removal. If someone gained access to a network in June 2023, the IBM average suggests threat actors would be removed from the network in March 2024.

The IBM study includes a whole-of-society scope, including civil society, the private sector, and political-military organizations. Good threat-hunting and network defence capabilities allow organizations to deter malicious threats on a network. Threat actors can use the time to their advantage without being kicked off the network due to a lack of threat hunting and network defence. With these crucial tools, an organization can detect and deter malicious threat actors from remaining on the network without detection or removal.

Cyber resilience applies to the cyber domain as deterrence by denial increases costs and decrease benefits for threat actors seeking to force access to a network with significant time, resources, and motivation. Cyber resilience develops capabilities for an organization to become highly resilient with cutting-edge technology from private industry. Capability development requires investment to hunt for threats on a network, observe unusual or unknown network traffic, and remove authorization or access as soon as it is detected. The more prudent strategy assumes threat actors already have access to the network. Proactive measures seek to find threats before they gain a foothold on a network, to remain undetected for an unknown time. An organization becomes more cyber resilient by increasing costs, decreasing benefits, and funding

[61] Nye, "Deterrence and Dissuasion in Cyberspace," 51.
[62] IBM, "2019 Cost of a Data Breach Report," *IBM Security,* (2019), https://www.ibm.com/downloads/cas/RDEQK07R#:~:text=The%20lifecycle%20of%20a%20data%20breach%20is%20getting%20longer.

resources for threat hunting to deny an adversary the means to establish a foothold within a network.

1.4.3 Deterrence By Entanglement

Deterrence by entanglement relies on establishing interdependent norms and other relations between states to deter threat actors from taking specific actions. Interdependence encourages various actors to become mutually reliant on one another, and the interrelation of interests ensures that any harm for one party affects all parties.[63] The Approach extends deterrence "to third parties to maintain reputation and prevent losses and benefits," which shifts strategic calculations away from costs to mutual benefits.[64] Self-deterrence contains otherwise strategic calculations not to harm the gains from the cooperative dynamics of entanglement.[65] A challenge for entanglement is that states can manipulate the leverage gained from asymmetries in resource dependencies. A state with a monopoly on a specific resource that other states rely on can use this uneven power imbalance to its advantage. Different approaches to deterrence by entanglement explore normative developments and international law.

1.5 – Cyber Challenge to Classical Deterrence

The “cyber security dilemma” involves the inability to decipher the motivation of cyber behaviour on a network.[66] Dual-use cyber capabilities are notoriously difficult to differentiate between offensive and defensive behaviour in cyberspace. For example, unrecognized traffic on

[63] Nye, “Deterrence and Dissuasion,” 49.
[64] Aaron Brantly, “Conceptualizing Cyber Deterrence by Entanglement,” *SSRN Scholarly Paper* (Rochester, SSRN, 2018): 10, https://doi.org/10.2139/ssrn.2624926.
[65] Brantly, “Conceptualizing Cyber Deterrence by Entanglement,” 49.
[66] Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations* (Oxford: Oxford University Press, 2016): 17.

an organization's network could be a threat actor collecting reconnaissance for espionage purposes or laying the groundwork for a large-scale cyber attack. In interviews for this study, various NATO Officials outline what they believe to be a better strategy, which involves assuming that an adversary is already on the network. Appropriate measures ensure such behaviour is limited in time and access, including intense threat hunting to remove adversaries from networks quickly. Threat hunting is one Approach which requires the appropriate tools, staff, and resources to protect NATO's networks.

The diversity of cyber threat actors complicates the strategic logic of deterrence, given that decision-makers must account for states, state-sponsored proxies, non-state hacking groups, private firms, individuals, and others dangers.[67] The cyber domain uniquely demonstrates the challenge of applying both deterrence by punishment and denial in the cyber domain.[68] Cyber threats pose a complex set of challenges to applying classical deterrence theory.[69]

1.5.1 Cyber Deterrence at NATO

Recall this project's central research question, how NATO's evolving strategic deterrence doctrine addresses contemporary security threats in the cyber domain. In the 2017 book *Strategic Cyber Deterrence*, Scott Jasper outlines four focus areas to address questions about the various forms of cyber deterrence, including punishment, denial, engagement, and proactive approaches like active cyber defence.[70] Jasper uses these focus areas to analyze the "sufficiency of strategic

[67] Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge: Cambridge University Press, 2018): 8, https://doi.org/10.1017/9781316422724.
[68] Irène Couzigou, "Securing Cyber Space: The Obligation of States to Prevent Harmful International Cyber Operations," *International Review of Law, Computers & Technology* 32, no. 1 (2018): 42, https://doi.org/10.1080/13600869.2018.1417763.
[69] Amir Lupovici, "Cyber Warfare and Deterrence: Trends and Challenges in Research," *Military and Strategic Affairs*, no. 3, vol. 3, (2011): 51, https://www.inss.org.il/wp-content/uploads/2017/02/FILE1333533336-1.pdf.
[70] Jasper, *Strategic Cyber Deterrence*, 13.

cyber deterrence options… to alter malicious actor behaviour in cyberspace." These four focus areas frame the analysis of how deterrence applies to address cyber threats, focusing specifically on deterrence by punishment, denial, entanglement, in addition to the distinct proactive strategic focus of active cyber defence.

Jasper notes that the attribution problem and the appropriate response problem directly challenge the application of deterrence by punishment in the cyber domain. Deterrence by punishment uses "all necessary means… in response to hostile acts in cyberspace."[71] Jasper adds that deterrence by denial questions the degree to which "proactive measures improve security networks and systems to deny adversaries the benefit of attack."[72] Deterrence by entanglement involves using "cooperative measures… based on mutual interests," Jasper adds, to effectively restrain behaviour, which otherwise involves "conducting, endorsing, or allowing malicious cyber activity."[73] Political will remains crucial, requiring additional resources to fund training and recruit personnel.

Asymmetric dependencies involve disproportionate state reliance on others for resources and dependencies, extorted by states to influence the dependent's decision-making. Phase A-D provides a structure for this analysis on cyber deterrence to study NATO cyber defence policy in Chapters 3-6. Classical deterrence theory and contemporary deterrence theory apply policy countermeasures against threats in the cyber domain. Persistent engagement provides a distinct strategic logic to the strategies related to the present analysis. Future research will provide a comparative assessment of cyber deterrence and persistent engagement.

[71] Ibid.
[72] Ibid.
[73] Ibid.

1.5.2 Classical Deterrence at NATO

NATO defines "deterrence*"* as "convincing a potential aggressor that the consequences of coercion or armed conflict outweigh the potential gains. Such consequences require credible military capabilities and a strategy with the clear political will to act."[74] The NATO definition of "deterrence" in the December 2021 edition of the NATO Office of Standardization *Glossary of Terms and Definitions* has remained unchanged in the glossary since the January 1996 edition. The 1996 definition was "developed and approved by various tasking authorities" to attain the status of "NATO Agreed."[75] Classical deterrence continues to influence NATO's understanding of deterrence for contemporary challenges. The critical question is how these classical definitions are applied to countermeasures against contemporary hybrid and cyber threats.

Questions remain about how classical deterrence adequately applies to other areas of the Alliance's adaptation to new challenges. The essence of classical deterrence is that "one party prevents another from doing something the first party does not want by threatening to harm the other party seriously if it does."[76] Retaliatory threats of punishment and resilient denial of capabilities signal significant challenges to threat actors to deter their actions from achieving objectives.[77] Credibility and reputation depend on other states' perceptions to understand how an opponent sees the world.[78] Deterrence relies on not misinterpreting behaviour, which could otherwise have catastrophic consequences.[79]

---

[74] NATO Standardization Office, "Deterrence," in *NATO Glossary of Terms and Definitions*, (Brussels, NATO, 2021), https://standards.globalspec.com/std/14486494/AAP-06.
[75] NATO Standardization Office, "Deterrence."
[76] Patrick M. Morgan, *Deterrence Now*. (Cambridge: Cambridge University Press, 2003): 1, https://www.cambridge.org/core/books/deterrence-now/7890EF6476 6FFF2A54D0011A097FA9AF.
[77] Glenn Snyder, "Deterrence: A Theoretical Introduction," in *Theories of Peace and Security: A Reader in Contemporary Strategic Thought*, edited by John Garnett (London: Palgrave Macmillan UK, 1970): 108, https://doi.org/10.1007/978-1-349-15376-3_6.
[78] Robert Jervis, "Deterrence and Perception," *International Security* 7, no. 3 (1982): 6, https://doi.org/10.2307/2538549.
[79] Ibid.

NATO was founded on the principle of collective defence outlined in the North Atlantic Treaty signed on April 4, 1949. Article 5 of the Treaty stated that "an armed attack against one or more" of the members of the Alliance would be "considered an attack against them all."[80] Collective defence is central to NATO's deterrence strategy to ensure the Alliance agrees to military solidarity, such that any act of violence against a member is treated as an "armed attack against all members." Allies agree to take all actions necessary "to assist the Ally attacked," such that the support is designed to deter an adversary's actions from harming the Alliance.[81]

1.6 – Contemporary Deterrence at NATO

In recent decades, contemporary threats like cyber attacks have challenged the applicability of collective defence provided by classical deterrence.[82] In recent years, new multi-domain challenges have included gray zone conflict, hybrid warfare, and cyber threats. Targets below the threshold of military response options attain strategic goals without escalation to conventional warfare. The application of Article 5 over the past decade expands collective defence to apply to cyber-attacks and hybrid threats on a case-by-case basis.

The ambiguous application of deterrence limits threat actors from knowing precisely where the threshold for specific response options is designed. The NATO Glossary defined "hybrid threats" as combining "conventional, irregular, and asymmetric activities in time and space."[83] Notably, this definition includes the combined features that blend different combat forces. A crucial feature of contemporary deterrence is the need to counter hybrid warfare, gray

[80] NATO, "The North Atlantic Treaty," NATO, (April 4, 1949), https://www.nato.int/cps/en/natohq/official_texts_17120.htm.
[81] Ibid.
[82] Kęstutis Paulauskas, "On Deterrence," *NATO Review*, (August 5, 2016), https://www.nato.int/docu/review/articles/2016/08/05/on-deterrence/index.html.
[83] NATO Standardization Office, "Hybrid Threats."

zone conflict, and cyber threats to limit conflict escalation below conventional domains of warfare.

1.6.1 Cross-Domain Deterrence

Cross-domain deterrence uses various tools across operational domains of land, sea, air, space, and cyber to deter attackers from targeting one domain based on the threat of coercive measures in other domains.[84] Deterrence expands beyond the cyber domain to create interoperable cooperation, such that threats are in "some combination of different types… [to] dissuade a target from taking actions of another type."[85] Examples include targeted economic sanctions to punish cyber intrusion.[86] Alternatively, "name and shame" strategic communication initiatives publicly attribute a threat actor for breaking cyber norms or international law.[87]

When cyber-attacks and malicious cyber campaigns target Allies, countermeasures remain on a case-by-case basis, including Article 5. In an interview for this study, NATO Official 6 describes the value of flexible response options to provide countermeasures on a case-by-case basis in the cyber domain. The Official argues that a toolbox approach provides response options to other domains beyond cyber, such that various countermeasures can be applied and combined based on coordinated efforts to deter actions.

---

[84] Erik Gartzke and Jon R. Lindsay, *Cross-Domain Deterrence: Strategy in an Era of Complexity* (New York, NY: Oxford University Press, 2019): 6.
[85] Gartzke and Lindsay, "Cross-Domain Deterrence:" 6.
[86] Mark Peters, "Cyber Enhanced Sanction Strategies: Do Options Exist?" *Journal of Law & Cyber Warfare* 6, no. 1 (2017): 110.
[87] Global Affairs Canada, "Canada Welcomes European Union's Announcement of New Cyber Sanctions Listings," (July 30, 2020), https://www.canada.ca/en/global-affairs/news/2020/07/canada-welcomes-european-unions-announcement-of-new-cyber-sanctions-listings.html.

1.6.2 Tailored Deterrence

Tailored deterrence prevents an adversary from acting in a specific way, such that threats target what a competitor values the most. Cross-domain deterrence is most robust when practitioners tailor countermeasures to target an adversary's weaknesses specifically. In an interview for this study, NATO Official 15 notes that tailored deterrence was a key motivator to develop a comprehensive approach for preventative response options to counter hybrid threats. The official added that innovative thinking was required to apply and amplify the toolbox approach to form a list of response options dependent on the specific contextual circumstances.

1.7 – New Strategic Approaches

1.7.1 Active Cyber Defence

Active cyber defence is a proactive approach to enhance deterrence by punishment and denial. Defences make "it harder to carry out a cyber attack and support retaliation… providing more options to inflict punishment."[88] Malicious cyber activity targets networks and combines "internal systemic resilience to halt malicious cyber activity." Active cyber defence involves "real-time detection, analysis, and mitigation of network security breaches combined with the aggressive use of legal countermeasures beyond network and state territorial boundaries."[89] The value of cyber operations to shape the threat environment is "unmistakable," according to Ben Buchanan, Senior Faculty Fellow at Georgetown's Center for Security and Emerging Technology.[90] Active cyber defence strategically shapes the threat environment.

---

[88] Jasper, *Strategic Cyber Deterrence*, 10-11.
[89] Ibid.
[90] Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Cambridge, Massachusetts: Harvard University Press, 2020): 3.

Revelations of state secrets in any domain are immensely damaging. The secrecy surrounding state cyber capabilities comes with added damage that "revealing the capability diminishes it" to no longer have the cyber effect in the real world.[91] Once the vulnerability is known, defenders can patch the network before attackers can exploit it to their advantage. A zero-sum game between attackers, defenders, and victims includes tools to shape the "expectations and behaviours of others… through the power of ideas or superior capabilities."[92] Threats in the cyber domain challenge the core tenets of classical deterrence and contemporary deterrence. A new strategic approach requires proactive alternatives to address these challenges. Contemporary deterrence must be equipped to handle these cyber threats without further emphasizing proactive strategic alternatives.

1.7.2 Persistent Engagement

Deterrence provides the main strategic logic that is analyzed to counter threats in the cyber domain. Constant engagement outlines a different approach with a distinct strategic logic, which is herein introduced to demonstrate other strategies beyond deterrence. Cyber persistence theory applies to the threat environment with persistent engagement to operate "more effectively below the level of armed conflict… [to] influence the calculations of our adversaries, deter aggression, and clarify the distinction between acceptable and unacceptable behaviour in cyberspace."[93] The approach will "degrade and neutralize adversary capabilities themselves" rather than "influencing [the] cost-benefit analysis of opponents as deterrence aims to do."[94] To operate persistently in cyberspace is constantly engaging adversaries in the cyber domain.

---

[91] Ibid., 39.
[92] Jasper, *Strategic Cyber Deterrence,* 93.
[93] Ibid.
[94] Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation," *The Cyber Defence Review*, no. Special Issue (2019): 270.

Deterrence seeks to prevent future undesirable actions by threatening punishment, denying access, or entangling interests. Persistence requires direct engagement with adversaries to prevent future malicious cyber threats proactively. This distinct strategic logic of persistent engagement, provided by the theoretical foundation of cyber persistence theory, outlines key features of the threat environment. Cyber persistence theory argues:

> States act persistently in and through cyberspace rather than engage in episodic hacking or breaching of devices, systems, and networks. The dominant State behaviour in cyberspace is exploitation rather than coercion… Competitive interaction is the dominant dynamic.[95]

Fischerkeller, Goldman, and Harknett argue that "States act persistently in and through cyber space rather than engage in episodic hacking or breaching of devices, systems, and networks."[96] A crucial difference between persistent and episodic hacking relates to "dominant state behaviour in cyberspace as exploitation rather than coercion." This crucial difference needs to be unpacked, given that persistence theory grants the possibility for competition in cyber space, which can be exploitative and coercive. It is essential to understand the threat environment where "competitive interaction is the dominant dynamic" yet, remains "exploitative rather than coercive," as the authors claim. There remains a need to study persistence to develop strong countermeasures and understand competitor behaviour in cyberspace. When combined with accumulation theory, persistence theory emphasizes that many small impact events, such as minor cyber attacks, can have significant strategic effects over time when combined as targeted campaigns.

The NATO Standardization Office's Glossary of Terms and Definitions includes "defensive cyberspace operations" as "actions in or through cyberspace to preserve… freedom of

[95] Ibid., 58.
[96] Ibid., 58.

action in cyberspace."[97] The same glossary defines "offensive cyberspace operations" as "actions in or through cyberspace that create effects to achieve military objectives."[98] Some Allies are hesitant to adopt persistent engagement over criticisms that it can seem "overly aggressive" or raise concerns over state sovereignty to keep networks free from foreign intrusion.[99]

Allies lacking cyber capabilities to take part in hunt forward operations can rely on other Allies with these capabilities to support them. The challenge is that Allies may be less open to value cyber operations, given little inclination to support what they cannot themselves directly take part in.[100] Alternatively, such an ecosystem fosters the incentive for Allies with strong cyber capabilities to help strengthen less mature cyber Allies. NATO functions as a leadership platform to foster bilateral and multilateral agreements.

Allies view these strategic advancements favourably, with some even contracting the United States Cyber Command to conduct hunt forward operations within the requesting Ally's territory. These alternative approaches practice cyber persistence theory across the Alliance, such that NATO can function as a platform to facilitate ongoing coordination. United States Air Force Lieutenant General Charles Moore noted that the United States had conducted 24 hunt forward operations across 14 countries since 2018.[101] The United States reportedly deployed a hunt-

[97] NATO Standardization Office, "Offensive Cyberspace Operation," in *NATO Glossary of Terms and Definitions*, (Brussels, NATO, 2021), https://standards.globalspec.com/std/14486494/AAP-06.
[98] NATO Standardization Office, "Defensive Cyberspace Operation," in *NATO Glossary of Terms and Definitions,* (Brussels, NATO, 2021), https://standards.globalspec.com/std/14486494/AAP-06.
[99] Max Smeets, Robert Chesney, and Monica Kaminska, "The Transatlantic Dialogue on Military Cyber Operations-Amsterdam," *Lawfare*, (December 5, 2019), https://www.lawfareblog.com/workshop-report-transatlantic-dialogue-military-cyber-operations-amsterdam.
[100] Max Smeets, "NATO Members' Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis," in *2019 11th International Conference on Cyber Conflict*, vol. 900, (2019): 4, https://doi.org/10.23919/CYCON.2019.8756634.
[101] Brad D. Williams, "CYBERCOM Has Conducted 'hunt-Forward' Ops in 14 Countries, Deputy Says," *Breaking Defense*, (November 10, 2021), https://breakingdefense.com/2021/11/cybercoms-no-2-discusses-hunt-forward-space-cybersecurity-china/.

forward team to Ukraine in 2021.[102] In 2022, various Heads of State of NATO Allies invited the United States to deploy hunt-forward operations, including Lithuania, in May 2022.[103] And Croatia in August 2022.[104]

1.8 Chapter Outline

Chapter 1 has introduced the project and outlines the research puzzle, questions, theoretical and conceptual lenses, and methodology. Chapter 2 explains vital conceptual lenses and critical debates throughout Phases A, B, C, and D. Chapter 3 provides an overview of NATO as an international organization to outline key related policy developments throughout its history. Chapter 3 Section 3.3 focuses on the first critical juncture: cyber incidents during NATO's Operation Allied Force in Kosovo in 1999. These cyber incidents were instrumental in founding NATO cyber defence policy in Phase A, which included related developments between 2000 and 2006.

Phase A is a model for the other timelines in Phases B, C, and D in Chapters 4, 5, and 6, respectively. Each phase details critical junctures, significant cyber incidents, and other events in the cyber threat landscape and NATO defence policy. Chapter 4 focuses on Phase B between 2007 and 2013 to outline critical junctures and policy developments. Chapter 5 focuses on Phase C between 2014 and 2017. Chapter 6 focuses on Phase D between 2018 and 2022. Chapter 7 revisits the project's central research questions to discuss key findings from Phases A, B, C, and D.

---

[102] Suzanne Smalley, "Nakasone Says Cyber Command Did Nine 'Hunt Forward' Ops Last Year, Including in Ukraine," *CyberScoop*, (May 4, 2022), https://www.cyberscoop.com/nakasone-persistent-engagement-hunt-forward-nine-teams-ukraine/.
[103] Ines Kagubare, "U.S. Deployed Cyber 'Hunt Forward' Team to Croatia," *The Hill*, (August 19, 2022), https://thehill.com/policy/cybersecurity/3608312-us-deployed-cyber-hunt-forward-team-to-croatia/.
[104] Ibid.

Chapter 2: Theorizing the Threat Landscape

2.1 - Cross-Level Analysis of International Institutions

This project's level of analysis is the international organization. One international organization can be distinguished from another to provide analytically rich conclusions. The analytic distinction between states and international organizations also applies as a cross-level distinction between international institutions. Formal international institutions are distinguished based on functions, purposes, systems, rules, and other roles.

Some theoretical approaches are more valuable to apply to some institutions over others when considering the specific research agenda and analytic scope. This cross-level analysis approach distinguishes between international institutions based on distinct focus areas. For example, distinguishing a project focused on the study of international institutions dedicated to global peace and security with a case study set within the United Nations is distinct from one focused on regional collective defence of Allies within NATO.

The cross-level analysis approach distinguishes between international institutions to focus on the individual entity as a closed-box system. Different institutions have distinct scopes which justify a specific application of cyber conflict and international relations theory. The international relations theory literature is applied to NATO policy evolution in response to cyber threats. NATO is an international institution with a regional scope focused on the collective defence of the transatlantic Alliance. The United Nations is an international institution focused on international peace and security in the context of international law, governance, and norms. A project designed to address the evolution of cyber norms is best suited to address the cyber diplomacy literature related to norms focused on the United Nations.

The present focus on cyber defence within the deterrence literature focuses on the evolution of NATO policy. This project uses historical institutionalism and social learning to explain outcomes as a hybrid approach. This hybrid approach seeks to overcome challenges to differentiate between international organizations as distinct institutions with specific focus areas. These approaches are used to attend to these nuances and understand the historic legacies focused on a single institutional entity over two decades.

The present project opted for a hybrid methodology to incorporate elements of various theories of international relations applied to the cyber conflict literature, but only as applicable to questions of cyber deterrence and NATO. The present approach seeks to understand how cyber policy has evolved to benefit future adaptation to new threats. The following section provides a literature review on related cyber International Relations theory applied to the project. Generally, the cyber diplomacy work is beyond the project scope of cyber resilience, defence, and deterrence.

2.2 International Relations Theory, Cyber Conflict Studies, and NATO

International Relations theory is briefly surveyed to demonstrate minimal applicability to the NATO cyber defence project as it currently stands. The International Relations theories of Realism, Liberalism, Constructivism, and Feminism are briefly introduced to survey International Relations theory projects beyond the present scope. Each International Relations theory emphasizes specific characteristics of the international system. Discussion of these International Relations theories applied to the NATO cyber defence project will be expanded in Chapter 7.

2.2.1 Realism

Realists emphasize the power and self-interest of states seeking to maximize capabilities to ensure survival. A realist interpretation of International Relations focuses on the anarchic character of the international system absent a central authority. State and non-state actors pursue power, competitive advantage, and capability amassment to ensure survival. Classical realists argued that the laws of human nature govern international politics.[105] Neorealism expanded this approach to focus on state competition due to the anarchic nature of the international system, without a greater international power to prevent states from amassing capabilities.[106] States must strategically acquire as much power as possible to achieve hegemony, even by revisionist means.[107] From this context, a state develops cyber capabilities for survival to maintain dominance within the international system. Game theoretical approaches are also appropriate as a means to understand the dangers of strategy from a single strategist's point of view.[108]

2.2.2 Liberalism

The liberal approach to International Relations emphasizes the importance of institutions and cooperation to maintain peace and avoid conflict. Formal and informal conventions, rules, principles, and laws regulate government collaboration and competition in international affairs. The state-centric approach of realism is challenged by a focus on international organizations to facilitate state collaboration. Liberalism argues that promoting collaboration among states and international organizations lessens the chances of conflict. The liberal challenge to the state-

[105] Hans J Morgenthau, *Politics Among Nations: The Struggle for Power and Peace* (New York: Knopf, 1948).
[106] Kenneth N Waltz, *Theory of International Politics* (Addison-Wesley, 1979).
[107] John J Mearsheimer, *The Tragedy of Great Power Politics* (Norton, 2001).
[108] Erika Simpson, "Game Theory and Peace Research: Professor Anatol Rapoport's Contributions," *In Factis Pax 12, no. 1 (2018): 38-58.*

centric approach of neorealism shows how institutions impact international dynamics between states.[109]

The domestic, state and international levels of analysis are used to move beyond analyzing the state as a closed-box system to assess power dynamics and influence between states and international institutions.[110] A rationalist perspective to studying institutions emphasizes formal organizations and regimes, where cooperative dynamics are influenced by competition and scarcity.[111] A reflectivist perspective focuses on the sociological dynamics within an institution that stresses flexible preferences to analyze cultural differences in values, norms, and practices.[112] Crucial distinctions between realism and liberalism will be addressed related to the limitations of theoretical applications in the present case focused on NATO.

The liberal institutionalist argues that institutions may change state preferences through the encouragement of the advantages of cooperation to deter self-interest. Unique institutional differences demonstrate the appropriate approaches to specific focus areas when applied to certain institutions and less appropriate when applied to others. NATO policy includes language on cyber diplomacy, international law, and cyber-related norms at the United Nations.

2.2.3 Constructivism

Constructivists emphasize norm development and socialization to shape state behaviour. The constructivist interpretation of international relations emphasizes the importance of norms, ideas, and identities. The goal of the approach is to understand the role of state adherence to

[109] Andrew Moravcsik, "Taking Preferences Seriously: A Liberal Theory of International Politics," *International Organization* 51, no. 4 (1997): 513–53, https://doi.org/10.1162/002081897550447.
[110] Andreas Hasenclever, Peter Mayer, and Volker Rittberger, "Integrating Theories of International Regimes," *Review of International Studies* 26, no. 1 (2000): 3–33.
[111] Robert O Keohane, "International Institutions: Two Approaches," *International Studies Quarterly* 32, no. 4 (1988): 379–96, https://doi.org/10.2307/2600589.
[112] Robert O Keohane, "International Institutions."

international norms to reduce tensions and prevent conflict escalation. The Constructivist approach focuses on how ideational factors influence the diffusion and socialization of ideas and beliefs within the institution. Constructivism holds the "middle ground" between rationalist and relativist perspectives in International Relations theory, with the view that human interaction shapes the dynamics and interpretations of the material world.[113]

The concept of "cognitive evolution" involves the innovation, diffusion, and institutionalization of ideas to shape state governance practices at the level of international organizations.[114] A Constructivist research agenda focused on cyber norm diffusion among states focused on the change in cognitive evolution in an institution to help explain the role of "epistemic communities" in preventing conflict.[115] This approach is focused on the interaction between international organizations and states. The Constructivist approach focuses on how ideational factors influence ideas and beliefs to understand how norms spread and socialize.

Norm socialization involves states adopting certain behaviours and identities proliferated through interactions amongst each other in the international community.[116] Such an approach involves the interrelation between levels of analysis to study the spread of norms from the international organization to socialize among the states. Here, the focus is on the developments within an international institution as a closed-box system rather than any focus on the organization's interactions with other states. The present project focuses on NATO as a closed-box system to identify how contemporary deterrence theory adapted policy to cyber threats within this institution. The project is not concerned with how policy translates from NATO to

[113] Emanuel Adler, "Seizing the Middle Ground: Constructivism in World Politics, 1997," *European Journal of International Affairs* 3, no. 3 (1997), https://journals.sagepub.com/doi/abs/10.1177/1354066197003003003.
[114] Adler, "Seizing the Middle Ground."
[115] Ibid.
[116] Jeffrey T Checkel, "The Constructivist Turn in International Relations Theory," ed. Martha Finnemore, Peter Katzenstein, and Audie Klotz, *World Politics* 50, no. 2 (1998): 324–48.

individual states, and the scope focuses solely on the international institution as the level of analysis.

A Constructivist approach examines deterrence theory in the context of the cyber conflict literature. For deterrence to be successful, threats need to be seen as credible and involve a psychological component.[117] The credibility of threats is based on perceptions of state reputations to understand how states come to understand the world. A state can draw reputational conclusions about commitments to past behaviour to make conclusions about future state behaviour. Credibility is a component of the deterrent effectiveness to understand how states treat credible deterrence based on how credible a state's threats are perceived.[118]

It is entirely appropriate to examine the diffusion of norms, their impact on state behaviour, and whether credible deterrence works among the international community. The specific focus here is that this extensive literature applies to the world of NATO cyber defence. The merit of applying Constructivism to the present project is an analytic reach, given that it forces a NATO-centric project to become more focused on international cyber diplomacy, which is more appropriately focused on a case study of the United Nations.

NATO does acknowledge the importance of cyber norms. However, when cyber norms are discussed, it is in the context of the Alliance either acknowledging the United Nations Charter or specific norms developed within the more extensive cyber diplomacy literature. For example, the Vilnius Summit Communiqué cited the United Nations Charter and acknowledged the "voluntary norms of responsible state behaviour in cyberspace."[119] This norm has been

[117] Robert Jervis, "Deterrence and Perception," *International Security* 7, no. 3 (1982): 3–30.
[118] Paul K Huth, "Deterrence and International Conflict: Empirical Findings and Theoretical Debates," *Annual Review of Political Science* 2, no. 1 (June 1999): 25–48, https://doi.org/10.1146/annurev.polisci.2.1.25.
[119] NATO, "Vilnius Summit Communiqué Issued by NATO Heads of State and Government (2023)," NATO, July 11, 2023, https://www.nato.int/cps/en/natohq/official_texts_217320.htm.

developed extensively within the cyber diplomacy literature and United Nations setting. Understanding cyber norm diffusion within NATO requires first understanding how norms were developed and then examining how they spread within the context of distinct international organizations.

Most initial work and development on these cyber norms occurred at the United Nations or within specific states or groups of states at the international level. Even the language on cyber norms within NATO documentation directly cites the work of the United Nations. For example, the 2023 NATO Vilnius Summit Communiqué stated that the Alliance was "committed to act under international law, including the United Nations Charter, international humanitarian law, and international human rights law as applicable."[120] Any project focused on cyber norm diffusion within any institution, including NATO, must first outline the cyber diplomacy literature focused on developing cyber norms, primarily at the United Nations, to build a foundational solid project.

Norms can influence government decision-making depending on whether they successfully socialize within the specific community before becoming institutionalized. A norm cascade involves norm leaders engaging in "dynamic imitation" to "socialize other states to become norm followers."[121] A norm cascade occurs when norm leaders engage in "dynamic imitation" to "socialize other states to become norm followers."[122] A "tipping point" is reached when "norm entrepreneurs have persuaded a critical mass of states to become norm leaders and adopt new norms."[123] When a sufficient number of states accept and support a standard, a new

[120] NATO, "Vilnius Summit Communiqué."
[121] Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," *International Organization* 52, no. 4 (1998): 887–917.
[122] Finnemore and Sikkink, "International Norm Dynamics and Political Change."
[123] Ibid.

normative framework is created, establishing new mechanisms of behaviour as part of a state's identity.

A norm is a "standard of appropriate behaviour for actions with a given identity."[124] Understanding how the cyber norms that NATO cites developed first requires focusing on the cyber norm development at the United Nations. Unlike NATO, the United Nations provides the ability to track what individual states say at committee meetings, granting the ability to track norm socialization at the United Nations. Therefore, early on in the research process, this research project was stymied from studying norm development at the United Nations, and it could not study norm development at NATO. A Constructivist approach to norm diffusion could provide an alternative explanation for cyber policy development at NATO, but due to a lack of relevant documentation available to the public due to institutional design, such processes cannot be appropriately studied.

The NATO case is challenged to track norm socialization because it is necessary to see how norms diffuse among states through state communications during committee meetings. Given that these committee meetings in the NATO context are not available publicly, it limits the researcher's approach to this case. Norm diffusion or socialization cannot be tracked in the NATO context. However, the United Nations is a different institutional design and norms can be tracked within this context. Committee meeting notes can be used to track norm diffusion based on how international cyber norms spread at the United Nations to identify what different states said about them.

Publicly available United Nations committee reports provide a potent means for researchers to study the socialization of norms based on how individual states speak about

[124] Ibid.

specific norms. However, when the same approach is attempted within the NATO context, it is not possible in the same way that it is possible at the United Nations because of the distinct institutional design. The NATO cyber defence project focused on publicly available documents, which are the product of consensus-based agreements among Allies. Given the unique institutional structures, there is no way to gauge distinct Ally perspectives to track norm diffusion. Instead, the present project focused on cyber defence policy documents that the Allies agreed upon by consensus.

Differences in institutional design determine whether norm diffusion and socialization are methodologically possible. A project that seeks to study international cyber norm diffusion is better to focus on the United Nations, given that committee documents are publicly available and can be studied to see how individual states spoke about specific norms to track spread. The United Nations has a solid approach to tracking norm socialization by focusing on what individual states say at relevant meetings. Even if a project seeks to understand how norms diffuse or socialize at NATO, there remains a crucial flaw to this methodology requiring the institutional ability to identify how norms developed within a specific institution and how individual states respond to the norm proliferation.

NATO is not directly involved in initial norm development. Instead, NATO directly cites norms developed in the United Nations cyber diplomatic context. A project focused on cyber norms must be a multi-institutional project involving a case on cyber norm development and diffusion. A multi-institutional project requires understanding how norms are developed in the context of the United Nations, focusing on how they diffuse at NATO. The analysis of how the norms spread to NATO must first focus on how cyber norms developed at the United Nations.

The additional United Nations focus is a foundational case required to focus on cyber norm socialization at NATO.

The United Nations is better suited for a project focused on cyber norm diffusion and socialization because committee documentation is publicly available and allows for the direct study of norm socialization among states within an institution. The scope of a project focused on cyber norm diffusion and socialization necessitates a case focused on cyber diplomacy at the United Nations to understand how the norms first came into being before examining how they proliferated from the United Nations to NATO. Further challenges related to the seeming inability to track norm socialization among states at NATO, where committee meetings are not publicly available, compared to tracking norm socialization among states at the United Nations, where such meetings are publicly available.

The project briefly discussed cyber diplomacy, international law, rules, and norms applied to cyberspace. The focus on international law is vital to understanding the proliferation of cyber norms. It fundamentally requires that states are central to understanding how different states are influenced by norms spread through international institutions. In contrast, a more cyber diplomatic approach would expand beyond the project's focus on norms, including further considerations of the moral, ethical, and legal implications of international cyber conflict and cybercrime, with interrelated focus areas on privacy, human rights, and ethics.[125] For example, promoting responsible state behaviour in cyberspace demonstrates development within national and international conversations, norms, regulations, and international law. [126] Further initiatives

[125] Lucie Angers, "Combating Cyber-Crime: National Legislation as a Pre-Requisite to International Cooperation," in *Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research*, ed. Ernesto U. Savona (Dordrecht: Springer Netherlands, 2004), 39–54, https://doi.org/10.1007/978-1-4020-2924-0_4.
[126] Michael N Schmitt and Liis Vihul, "Respect for Sovereignty in Cyberspace," SSRN Scholarly Paper (Rochester, NY, November 3, 2017), https://papers.ssrn.com/abstract=3180669.

are designed to increase international collaboration to establish support for worldwide cyber security agreements.[127]

The evolution of cyber norms builds upon other international normative developments related to non-interference and responsible state behaviour. International legal and normative developments related to the Tallinn Manual discussed in this volume are essential. However, the Tallinn Manual remains an academic, peer-reviewed document, not an official NATO document agreed upon by consensus.[128] The most significant developments in cyber diplomacy, international law, and norms include the dynamic in recent years between the United Nations Group of Government Experts and the Open-Ended Working Group.[129] Both groups are introduced in the section on cyber diplomacy to provide a brief introduction to these developments in the context of the United Nations.

A Constructivist approach focuses on norm diffusion and socialization to spread cyber norms throughout the international system by tracking the spread from the international organization developing the norm which spreads among states. A Constructivist approach can address how norms diffuse through the international system, primarily through state socialization. The Constructivist interpretation is less practical when the analytic focus is on documents that are the product of consensus, where the black box of decision-making prevents an understanding of how consensus was reached.

---

[127] Michael N Schmitt, "Taming the Lawless Void: Tracking the Evolution of International Law Rules for Cyberspace," *Texas National Security Review* 3, no. 3 (Autumn 2020): 32–47.
[128] Michael N Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. (Cambridge: Cambridge University Press, 2017), https://doi.org/10.1017/9781316822524.
[129] Michael N Schmitt and Liis Vihul, "International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms," Just Security, June 30, 2017, https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/.

Vital institutional differences prevent understanding how norms socialize among states within NATO. There is no way to understand how individual states adopted or spread the cyber norms in question because there are no publicly available committee documents to track norm diffusion and socialization at NATO. The United Nations is ideal for examining cyber norm diffusion both because the analysis can identify initial norm development within the United Nations and how norms socialize among the international community. United Nations committee meetings have publicly available documents that can be used to study norm diffusion, and this line of inquiry is continued in the relevant section on constructivist International Relations theory.

2.2.4 Feminism

The feminist approach to International Relations theory takes a gendered approach to focus on inclusivity and representation, which emphasizes diverse perspectives in global affairs to examine the disproportionate effect of women and marginalized communities. A Women, Peace, and Security agenda focuses on protecting women and girls globally in conflict and post-conflict environments to address gender-based violence and inequality.[130] This agenda includes promoting women's participation in decision-making.

When combined with Poststructuralism, Feminist International Relations theory provides important conclusions that identify the impact of linguistic constructs to maintain power structures between opposing ideas related to gender in International Relations. This approach has been applied to technostrategic language structures to discuss how language familiarization on nuclear weapons excludes people unfamiliar with the concepts from criticizing decision-making

[130] Anwar Mhajne, Luna K. C., and Crystal Whetstone, "A Call for Feminist Analysis in Cybersecurity: Highlighting the Relevance of the Women, Peace and Security Agenda," *Women, Peace and Security*, September 17, 2021.

practices.[131] The gendered language of metaphors and euphemisms is used to limit criticism and curtail debate.

When the Feminist critical approach is applied to the International Relations literature, gender dynamics and power relations can understand how strategy formulation is affected. A focus on gender disparities in cybersecurity highlights significant gaps in representation, which otherwise allow diverse perspectives to share a voice in policy development. The Feminist approach scrutinizes power dynamics and emphasizes the intersectional study of gender with other identity markers like race and class.

This thesis does not examine NATO cyber policy from a Feminist perspective and, instead, briefly discusses the literature as challenging and illuminating but beyond the scope of the project as it currently stands. Numerous International Relations theories briefly touched upon in this chapter demonstrated minimal applicability to the current research project because they focused only on specific facets of NATO's policy that proved to be less explanatory and persuasive.

This project ultimately used Historical Institutionalism and Social Learning to explain outcomes. Such a hybrid model helped overcome challenges in studying one international organization, namely NATO, as a specific focus area. While other International Relations theories are persuasive and explanatory, in the process of conducting the interviews and collecting data, it was found that two concepts – namely Historical Institutionalism and Social Learning – could be melded in a new methodological approach that helps illuminate and clarify NATO's evolutionary approach to deterring threats in the cyber domain.

[131] Carol Cohn, "Sex and Death in the Rational World of Defense Intellectuals," *Signs* 12, no. 4 (1987): 687–718.

Similarly, a Feminist approach that is simultaneously Constructivist might focus on uncovering gender inequalities within decision-making and policy outcomes. Such an approach can be appropriately nestled within the purview of the NATO Cyber Defence Pledge. State commitments to develop voluntary cyber capabilities include focusing on how Allies can further acknowledge and act on commitments to gendered approaches to international relations.[132] The 2023 NATO Vilnius Communiqué includes at least two paragraphs focused on the Women, Peace, and Security agenda "across all [NATO] core tasks," which include deterrence and defence, crisis prevention and management, and cooperative security.[133] A critical International Relations theoretical approach loosely applies to the present project focused on studying developments in NATO cyber defence policy over twenty-two years. Despite providing valuable insights into the specific perspective of the International Relations theory in question, such an approach is less analytically valuable when compared to the hybrid approach of this project.

2.3 Cyber Conflict Studies and Contemporary Threats

The vastness of the cyber conflict literature has grown significantly in the last decade as malicious cyber activities and other cyber threats continue to intensify. In the first quarter of 2023, weekly cyber assaults rose 7% compared to the same time in 2022.[134] Between the first quarter of 2022 and 2023, cyberattacks targeting the education and research sectors rose by

[132] NATO, "Cyber Defence Pledge," NATO, July 8, 2016, https://www.nato.int/cps/en/natohq/official_texts_133177.htm.
[133] NATO, "Vilnius Summit Communiqué."
[134] Check Point, "Global Cyberattacks Continue to Rise with Africa and APAC Suffering Most," *Check Point Highlight Report*, April 27, 2023, https://blog.checkpoint.com/research/global-cyberattacks-continue-to-rise/.

15%.[135] Persistent threat actors provide increasing obstacles for cyber defenders and proactive approaches are required to address strategic competition in the threat landscape.[136]

A descriptive historical project focused on the case of NATO outlines the evolution of security policy challenging cyber threats to contemporary deterrence.[137] NATO is a unique international institution which evolved cyber defence policy as part of its approach to deterrence doctrine in the contemporary threat landscape. This approach demonstrates the unique challenges that cyber policy faces to adapt to specific cases. Due to the persistence and constant contact with competitors, states conduct offensive and defensive operations to obstruct, disrupt, and destroy cyberspace.[138]

2.4 Multidisciplinary Approach to Emerging Threats

The following section briefly focuses on critical emerging threats to demonstrate crucial challenges for cyber defence policy. These future challenges place immense pressure on future adaptations of cyber policy required for contemporary deterrence theory to adapt to cyber threats. Despite the state-centric focus of these sub-areas, they are each discussed to demonstrate the strategic value of NATO policy development.

Proactive measures address the cumulative nature of cyber threats where reconnaissance gains network access, escalates privileges, and maps essential infrastructure to target crown jewels.[139] In recent years, many countries have established military cyber commands, and the

[135] Check Point, "Global Cyberattacks Continue to Rise."
[136] Stéphane Taillat, "Disrupt and Restraint: The Evolution of Cyber Conflict and the Implications for Collective Security," *Contemporary Security Policy* 40, no. 3 (July 3, 2019): 368–81.
[137] Sandeep Baliga, Ethan Bueno De Mesquita, and Alexander Wolitzky, "Deterrence with Imperfect Attribution," *American Political Science Review* 114, no. 4 (November 2020): 1155–78.
[138] Michael P Fischerkeller and Richard J Harknett, "Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation," *The Cyber Defence Review*, no. Special Issue (2019): 267–87.
[139] CISA, "Critical Infrastructure Sectors," 2022, https://www.cisa.gov/critical-infrastructure-sectors?stream=top.

exponential rise includes the capabilities to conduct offensive cyber operations.[140] In addition to developing specific cyber defence policies in many cases, since 2018, NATO nations have increasingly established military cyber commands to conduct offensive cyber operations.[141]

Critical infrastructure is a national challenge within NATO's cyber resilience and defence initiatives. Allies agreed to the NATO Cyber Defence Pledge 2016 to provide an excellent understanding of developing sovereign cyber capabilities, including protecting critical infrastructure.[142] National defence plans heavily rely on creating cyber capabilities and rules to safeguard military and civilian networks, critical infrastructure, and individual information.[143] A better cyber security posture includes managing risks, assessments, and incident response. Nevertheless, concerns remain about how cyber challenges for national defence and security stem from the influence of evolving technologies on strategic planning.[144] Promoting cyber norms, regulations, and laws involves diplomatic activities and new technologies to defend against generated vulnerabilities that use faults in security infrastructure.[145]

Critical national infrastructure in North America and Europe is severely threatened by ransomware as threat actors become increasingly more active.[146] To advance security measures, national standards and legislation hold organizations and governments to monitor the evolution

[140] Max Smeets, *No Shortcuts: Why States Struggle to Develop Military Cyber-Force* (Oxford University and Press, 2022).
[141] Max Smeets, "NATO Members' Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis," in *2019 11th International Conference on Cyber Conflict (CyCon)*, vol. 900, 2019, 1–15.
[142] NATO, "Cyber Defence Pledge," NATO, July 8, 2016, https://www.nato.int/cps/en/natohq/official_texts_133177.htm.
[143] Jason Healey and Klara Tothova Jordan, "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow" (Atlantic Council, September 1, 2014), https://www.jstor.org/stable/resrep03426.
[144] James Kotsias, Atif Ahmad, and Rens Scheepers, "Adopting and Integrating Cyber-Threat Intelligence in a Commercial Organisation," *European Journal of Information Systems* 32, no. 1 (January 2, 2023): 35–51.
[145] Erica Borghard and Shawn Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies* 26 (July 3, 2017): 452–81, https://doi.org/10.1080/09636412.2017.1306396.
[146] Sean Collins and Stephen McCombie, "Stuxnet: The Emergence of a New Cyber Weapon and Its Implications," *Journal of Policing, Intelligence and Counter Terrorism* 7, no. 1 (April 1, 2012): 80–91.

of threats.[147] Advanced measures cooperate public-private partnerships between necessary organizations and significant stakeholders towards enhanced specialization of crucial infrastructure by national entities to link defence and security authorities and cybersecurity professionals.[148] The heavy reliance on critical infrastructure is a significant challenge to national cyber resilience and requires the interrelated efforts of law enforcement and cyber defenders. Cyber-criminal organizations are used as a stand-in for state-sponsored threat actors.[149] This section and the next aim to demonstrate how different areas of cyber conflict studies directly apply to the project. In contrast, other areas within the rich discipline are less relevant and beyond the project's scope.

An ongoing debate in the cyber conflict literature considers the threat landscape as an intelligence contest.[150] This assumption is dangerous because it assumes foreign cyber capabilities are only used for competitive intelligence and espionage when discovered on a network. This assumption is challenged by the complexity of the cyber threat landscape and the prevalence of non-state actors to hide and deceive on true intentions. One challenge involves discerning between espionage and reconnaissance actions to provide the groundwork for more significant future disruptive or destructive assaults.[151] Defending forward and persistent engagement allows for more ongoing and proactive cyber operations.

---

[147] National Institute of Standards and Technology Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1" (Gaithersburg, MD: National Institute of Standards and Technology, April 16, 2018), https://doi.org/10.6028/NIST.CSWP.04162018.
[148] Vitalii Kruhlov et al., "Public-Private Partnership in Cybersecurity," 2020, https://ceur-ws.org/Vol-2654/paper48.pdf.
[149] Yuan Stevens, Stephanie Tran, and Ryan Atkinson, "See Something, Say Something? Coordinating the Disclosure of Security Vulnerabilities in Canada's Infrastructure," in *2021 IEEE International Symposium on Technology and Society (ISTAS)*, 2021, 1–5, https://doi.org/10.1109/ISTAS52410.2021.9629214.
[150] Max Smeets and Robert Chesney, *Deter, Disrupt, or Deceive: Assessing Cyber Conflict as an Intelligence Contest* (Washington, DC: Georgetown University Pre
[151] Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations* (Oxford University Press, 2016).

An active approach to cyber defence includes internal tactics to increase the expenses and decrease the benefits for attackers. Developments in network defence, threat hunting, incident response, and defensive cyber operations are a few examples of this. Additionally, while exploiting cyber capabilities and impacts for strategic aims, offensive cyber operations stress responsible behaviour and under-acknowledged norms for responsible state behaviour.[152] As defined and enforced by responsible cyber behaviour, reconciling state sovereignty and holding irresponsible cyber actions accountable is still tricky.[153]

The key issues and debates in contemporary cyber conflict studies directly address persistent and combative threat actors that benefit from the malleability and flexibility of the threat landscape. The most active and creative uses of cyber capabilities to target Allies are advanced persistent threats, including cybercriminals and state-sponsored threat actors to enable government plausible deniability.[154] A discussion on the optimal courses of action is necessary due to this anonymity, which undermines the consensus on political attribution.[155] In international situations, political attribution has taken the form of statements of NATO.[156]

The current and upcoming use of new technology will provide significant challenges for cyber risks. Today's technology poses threats in the form of 5G, cloud computing, spyware, backdoors in consumer electronics, the propagation of false information on social media

[152] Perri Adams, Dave Aitel, David Perkovitch, JD Work, "Responsible Cyber Offense," Lawfare, August 2, 2021, https://www.lawfareblog.com/responsible-cyber-offense.
[153] Valentin Weber, "The Illusion of 'Responsible' Cyber Offense," German Council on Foreign Relations, October 27, 2021, https://dgap.org/en/research/publications/illusion-responsible-cyber-offense.
[154] Qi Wu et al., "Exploring the Vulnerability in the Inference Phase of Advanced Persistent Threats," *International Journal of Distributed Sensor Networks* 18, no. 3 (March 1, 2022), https://doi.org/10.1177/15501329221080417.
[155] Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1–2 (January 2, 2015): 4–37, https://doi.org/10.1080/01402390.2014.977382.
[156] NATO, "Statement by the North Atlantic Council in Solidarity with Those Affected by Recent Malicious Cyber Activities Including the Microsoft Exchange Server Compromise," NATO, July 19, 2021.

platforms, and other problems.[157] In the next ten years, security policy must keep up with many technological developments, including the Internet of Things, brain-computer interfaces, blockchain applications, extended reality, additive manufacturing, artificial intelligence and machine learning applications, and low-orbit satellites.[158]

2.5 – Conceptual Lenses

NATO is a case of an international organization evolving in a changing global threat landscape. The central theoretical contribution of this manuscript is to analyze deterrence theory in the contemporary threat landscape in the case of NATO's evolution for more than two decades. Two conceptual lenses - historical institutionalism and social learning - provide tools to analyze NATO's institutional cyber defence policy development, illuminating internal and external influences on the Alliance's policy-making procedures.[159]

The analysis outlines the value of conceptual lenses to answer the central research question related to the policymaking dynamics within NATO cyber defence throughout the project timeline. Historical institutionalism provides analytic tools to identify, change, and observe the evolution between precedent-setting cyber attacks, related events, and structural institutional processes. Social learning provides analytic tools to identify learning processes within an organizational design. NATO's internal Lessons Learned protocols are but one example to demonstrates the institutionalization of internal learning and development processes.

---

[157] Michael Raska, "Strategic Competition for Emerging Military Technologies: Comparative Paths and Patterns," *PRISM* 8, no. 3 (2019): 64–81.
[158] Alex Wilner and Casey Babb, "New Technologies and Deterrence: Artificial Intelligence and Adversarial Behaviour," in *NL ARMS Netherlands Annual Review of Military Studies 2020: Deterrence in the 21st Century—Insights from Theory and Practice*, ed. Frans Osinga and Tim Sweijs, NL ARMS (The Hague: T.M.C. Asser Press, 2021), 401–17, https://doi.org/10.1007/978-94-6265-419-8_21.
[159] Gianna Reggio, "Entities: An Institution for Dynamic Systems," in *Recent Trends in Data Type Specification*, eds. H. Ehrig et al., vol. 534, "Lecture Notes in Computer Science," (Berlin, Heidelberg: Springer Berlin Heidelberg, 1991), 246–65.

Conceptual lenses can borrow vital concepts from historical institutionalism and social learning to analyze NATO cyber defence policy. These lenses can help address traditional and contemporary deterrence from a fresh analytic perspective, challenging deterrence theory and addressing the unique character of threats in the cyber domain. Such perspectives help us understand the extent that deterrence theory was altered, abandoned, or otherwise changed in response to cyber challenges. The following two sections outline historical institutionalism and social learning more clearly to outline central concepts and clear causal mechanisms.

2.5.1 Historical Institutionalism

The historical intuitionalist expects to find path dependence within an organization where the status quo is expected rather than change. Self-reinforcing dynamics perpetuate the environment, making small-scale change harder to obtain without larger-scale events external to the institution. Paul Pierson adds that past decisions can lead to self-reinforcing feedback loops, which can be immensely challenging to break once created.[160] Arrangements and practices ingrained within institutions are analyzed using tools from historical institutionalism, such as those outlined by Kathleen Thelen.[161] An institution's future outcomes are limited over time by ingrained path dependence, until a significant event triggers critical junctures and the opportunity for change.[162]

A path-dependent institution is one with internal dynamics that are self-reinforcing and maintain an unchanging status quo. Path dependence involves expecting continuity to remain

[160] Paul Pierson, "Increasing Returns, Path Dependence, and the Study of Politics," *The American Political Science Review* 94, no. 2 (2000): 251–67.
[161] Kathleen Thelen, "Historical Institutionalism in Comparative Politics," *Annual Review of Political Science* 2, no. 1 (1999): 369–404.
[162] Paul Pierson, "Increasing Returns, Path Dependence, and the Study of Politics."

within an organization rather than change. The presence of anything beyond the unchanging status quo is enough to problematize the concept. Path dependence emphasizes the influence of historical sequences of events on an organization's development to impact critical junctures and be considered "qualitatively different from the normal historical development of the institutional setting of interest."[163] The historical institutionalist expects little policy or institutional change in self-reinforcing patterns where change is not expected.

External events can cause critical junctures to impact the previously unchanging status quo. Change becomes possible in the institution due to critical junctures that incite distinct institutional changes.[164] Decisions made within an institution result from possible choices, such that specific events intersect with "cumulative causal logics" to impact outcomes.[165] Historical institutionalism identifies mechanisms of influence which impact cyber defence policy development at NATO.[166]

Building on the research of Magnus Lundgren and colleagues to apply punctuated equilibrium theory to the study of international organizations, to examine the impact of external events to disrupt institutional path dependence. Researchers can identify "policy agendas characterized by periods of stability when there are little or no chance, and periodic punctuations, marked by rapid dramatic changes."[167] This account provides a solid case to analyze cyber attacks that have targeted NATO, to clarify old strategies that are no longer utterly functional against cyber threats. Critical junctures are grounded in external phenomena strong enough to

[163] Giovanni Capoccia and R. Daniel Kelemen, "The Study of Critical Junctures: Theory, Narrative, and Counterfactuals in Historical Institutionalism," *World Politics* 59, no. 3, (April 2007): 341–69.
[164] James Mahoney, "Path Dependence in Historical Sociology," *Theory and Society* 29, no. 4 (2000): 523.
[165] Thomas Rixen, Lora Anne Viola, and Michael Zurn, eds., *Historical Institutionalism and International Relations: Explaining Institutional Development in World Politics* (Oxford: Oxford University Press, 2016).
[166] Jacob S. Hacker and Paul Pierson, "After the 'Master Theory': Downs, Schattschneider, and the Rebirth of Policy-Focused Analysis," *Perspectives on Politics* 12, no. 3 (September 2014): 653.
[167] Magnus Lundgren, Theresa Squatrito, and Jonas Tallberg, "Stability and Change in International Policy-Making: A Punctuated Equilibrium Approach," *Review of International Organizations* 13, no. 4 (2018): 547–72.

disrupt an institution's path dependence, creating opportunities for plasticity and fresh ideas to redirect from the established path.

Critical junctures are the result of events that are external to the institution. External cyber attacks in Kosovo in 1999, Estonia in 2007, Georgia in 2008, and Stuxnet in 2010 stand as critical junctures in this analysis which provided the permissive conditions for change. These cases are of external events capable of disrupting processes of institutional self-reinforcement and allow for internal change to the pattern of policy development. Hillel Soifer outlines two distinct causal mechanisms involved to understand how critical junctures impact an institution and open the possibility for it to change.[168] First, "permissive conditions" describe when change is possible within an institution, and "represent the easing of the constraints of structure and make change possible."[169] The second change mechanism is "productive conditions," which involve the specific kind of change that occurs, dependent on the permissive conditions being present, to represent "the outcome or range of outcomes that are then reproduced after the permissive conditions disappear and the juncture comes to a close."[170] Permissive conditions are necessary at present, given that they provide the means for critical junctures to instigate internal change. The productive conditions are discussed in a different section related to internal learning protocols within NATO.

When applied to NATO, change was enabled by the events during Phases A and B, which amounted to critical junctures strong enough to result in permissive conditions that led to internal policy developments and institutional changes, such as the 2010 Strategic Concept. The initial cyber policy language within these NATO documents outlines the first public depiction of

[168] Hillel Soifer, "The Causal Logic of Critical Junctures," *Comparative Political Studies* 45, no. 12 (2012): 1572–97.
[169] Ibid.
[170] Ibid.

the Alliance's stance on deterrence and defence in the cyber domain. Initial policy language and the subsequent inclusion of terminology on cyber threats in related documents demonstrates an Alliance that is invested in developing cyber defence capabilities.

Further policy language added to NATO Summitry documents facilitated stronger political will to deal with cyber threats. Policy language encouraged further policy development and investment in then-new sectors of cyber defence. In this regard, NATO policy documents helped to provide arguments to leverage and promote further increases in defence policy, innovation, and investment among NATO nations. For example, the 2010 Strategic Concept included initial language on cyber defence that officials used to justify further policy and investment in 2011 and 2012.

2.5.2 Social Learning

A social learning approach analyzes the impact of ideas on institutional developments. The institutionalization of learning processes at NATO was often formalized into NATO's Lessons Learned procedures and exercises. Alternative modes of social learning have impacted NATO's cyber defence policy, as demonstrated by closely examining the Lessons Learned from various military exercises and operations. Social learning views NATO as a learning organization with standardization approaches to train decision-makers on situational awareness. The formalization of NATO's internal approach to social learning through Lessons Learned facilitates NATO's Joint Analysis and Lessons Learned Centre, or JALLC. The Centre works with other NATO entities on cases where Lessons Learned focuses on cyber defence at NATO.

Social learning holds that new ideas are crucial for policies to evolve. In an interview for this study, NATO Official 3 spoke of the competition of policy ideas in the diplomatic

marketplace. The official notes that one of NATO's unique strengths as an international organization is the frequency of conversations through meetings at the ministerial level, roughly every two or three months. These meetings provide the environment for ongoing policy competition and debate, fuelling learning. Pursuing specific ideas over others demonstrates these ideas have more influence on policy-makers.[171] The comparison of the overall attractiveness of a specific policy relative to others can establish whether it contains positive or negative emotional qualities of high or low intensity as a "valence" of ideas.[172] High-valence ideas tend to be those with highly positive emotional qualities with more influence on policy change, compared to negative emotional qualities with low valence and intensity.[173]

Social learning is used along with historical institutionalism as a different "conceptual lens" because it contributes vital concepts to help analyze how NATO evolved its cyber defence strategy amidst a changing threat landscape that challenges contemporary deterrence immensely. Social learning involves acquiring new knowledge and skills within organized environments to encourage learning through observation, interaction, and communication.[174] Social learning differs from historical institutionalism in that it encourages the acquisition of new knowledge and skills development far beyond historical tradition. A legacy institution like NATO that fosters social learning is doing more than reacting to critical junctures – it is learning to adapt. Therefore, although these two lenses – historical institutionalism and social learning—may seem similar, they are not. These lenses are used compatibly to both understand how external historical

[171] Frank R. Baumgartner, Christoffer Green-Pedersen, and Bryan D. Jones, "Comparative Studies of Policy Agendas," *Journal of European Public Policy* 13, no. 7 (September 1, 2006): 964, https://doi.org/10.1080/13501760600923805.
[172] Robert H. Cox and Daniel Béland, "Valence, Policy Ideas, and the Rise of Sustainability," *Governance* 26, no. 2 (2013): 318, https://doi.org/10.1111/gove.12003.
[173] Ibid.
[174] Albert Bandura, "Social Learning Theory," *Social Learning Theory* (Oxford, England: Prentice-Hall, 1977).

forces impact internal decision making, and to learn more about the character of the internal learning itself. The manuscript identifies both formalized internal learning protocols within NATO, and informalized affiliated learning engagements through cyber exercises conducted by the CCDCOE or cyber centre of excellence in Tallinn.

Critical concepts borrowed from social learning will assist this analysis in understanding NATO's cyber defence strategy. “Cognitive apprenticeships” are a social learning concept emphasizing learning through imitation, observation, and guided practice through expert direction.[175] Additional observations that suggest social learning has occurred in an organization include enhanced learning activities along with knowledge and skill development.[176] NATO Centres of Excellence encourage the exchange of knowledge and expertise, with procedures to participate in methods that make learning accessible. For example, many NATO Centres of Excellence include a unique blend of field expert reports and military defence exercises. Cyber exercises organized by the Coordinated Cyber Defence Centre of Excellence (including Locked Shields and Crossed Swords) involve communities of practices and cognitive apprenticeships to share knowledge.[177] Such initiatives provide tools for evaluating learning organizations based on knowledge enhancement and skills exchange.[178] In other words, they are examples of social learning at a more profound and broader level.

---

[175] Allan Collins, John Seely Brown, and Susan E. Newman, “Cognitive Apprenticeship: Teaching the Crafts of Reading, Writing, and Mathematics,” in *Knowing, Learning, and Instruction*, ed. Lauren B. Resnick, 1st ed. (Routledge, 2018), 453–94, https://doi.org/10.4324/9781315044408-14.
[176] Etienne Wenger, “Communities of Practice: Learning, Meaning, and Identity,” *Higher Education from Cambridge University Press* (Cambridge University Press, July 27, 1998), https://doi.org/10.1017/CBO9780511803932.
[177] Jean Lave and Etienne Wenger, *Situated Learning: Legitimate Peripheral Participation*, 1st ed. (Cambridge University Press, 1991), https://doi.org/10.1017/CBO9780511815355.
[178] Amy Edmondson and Bertrand Moingeon, “From Organizational Learning to the Learning Organization,” *Management Learning* 29, no. 1 (March 1, 1998): 5–20, https://doi.org/10.1177/1350507698291001.

In collaboration with the CCDCOE and other organizations, cognitive apprenticeships at NATO promote cyber defence cooperation and knowledge-sharing to unite NATO Allies and representatives. An example of such an initiative includes reports co-published by NATO's Allied Command Transformation (ACT) headquartered in Norfolk, Virginia, and the NATO CCDCOE in Tallinn, Estonia. One example includes the CCDCOE-ACT workshop "Cyberspace Strategic Outlook 2030" in the Fall of 2021, which included discussions among policy officials, academics, and field experts.[179] The workshop included representatives from NATO ACT, CCDCOE, and other individuals from other institutions indicating that the concept of cognitive apprenticeships at NATO is proof of social learning.

The workshop example illustrates NATO and Allies facilitating the exchange of best practices and lessons to develop training, education, and exercise programs. NATO involves communities of practice that clarify cyber defence strategy, bringing together specialists from member nations to facilitate information exchanges, help understand the cyber threat landscape, and create efficient risk reduction.[180] NATO's Cyber Defence Committee is the central platform for the Alliance to debate and plan joint cyber defence efforts among allies and NATO's political-military International Staff.[181]

Public-private partnerships are crucial for knowledge sharing at NATO, with the development of cyber defence fostering collaboration among sectors, including communities of business, academia, and other experts, to facilitate knowledge and skills exchange.[182] NATO includes many initiatives to work with industry; for example, NATO's Science for Peace

[179] CCDCOE. *CCDCOE-ACT Workshop 2021: Cyberspace Strategic Outlook 2030 – Doctrinal Thinking and Tactics*, 2021, https://www.youtube.com/watch?v=eMQm5EGhNK4.
[180] Etienne Wenger, "Communities of Practice: Learning, Meaning, and Identity"
[181] Jamie Shea, "How Is NATO Meeting the Challenge of Cyberspace," *PRISM* 7, no. 2 (December 21, 2017), https://cco.ndu.edu/PRISM-7-2/Article/1401835/how-is-nato-meeting-the-challenge-of-cyberspace/.
[182] Vitalii Kruhlov et al., "Public-Private Partnership in Cybersecurity," (2020).

Programme involves numerous engagements related to training, education, and cyber defence capacity building. NATO functions as a learning organization when dedicated to lifelong learning, creating policies, and providing financial support for cyber defence, training, and educating initiatives to advance the capabilities of the Alliance. Social learning assists policymakers in providing insights for collaborations on knowledge exchange between stakeholders.[183]

In short, social learning is needed as a conceptual lens to support predictions that learning environments facilitate organizations to be dedicated to change in light of knowledge, observation, and reaction to feedback loops. Substantial and efficient change is in response to historical-critical juncture threats, proving that historical institutionalism demonstrates the unprecedented external events that necessitate policy change and can act as the crux for emergency-based required fast-paced learning and training.

Historical institutionalism and social learning are used to comprehend social and organizational development. Key concepts from both theories are used to analyze organizational change, focusing specifically on learning mechanisms, temporal perspective, and level of analysis. From the perspective of learning mechanisms, social learning emphasizes individual and group learning to shape organizational transformation. Such initiatives include learning new skills through observing, copying, and adapting behaviours and practices from other organizations or actors.[184] Historical institutionalism focuses on how institutions function and the historical evolution influencing organizational transformation.[185] Institutions provide the

[183] Johanna Lahtinen, "Local Social Knowledge Management: A Case Study of Social Learning and Knowledge Sharing Across Organizational Boundaries," *Journal of Information Science*, 39, no. 5 (2013): 661-675.
[184] Albert Bandura. "Social Learning Theory."
[185] James G. March and Johan P. Olsen, "The New Institutionalism: Organizational Factors in Political Life," *American Political Science Review* 78, no. 3 (1984): 734–749.

guidelines, customs, and practices to control organizational behaviour over time. To apply this distinction, a social learning perspective might examine organizational change by focusing on a competitor's success. In contrast, a historical institutionalism perspective examines how the institutional rules, norms, and protocols impact such change.

From a temporal perspective, social learning adopted an immediate, process-oriented viewpoint to stress the direct influence learning has on an organization and to emphasize the dynamic interactions and feedback loops between actors over a brief time.[186] Institutionalism examines historical developments and long-standing organizational arrangements to shape structure and decision-making processes. Cumulative impacts are emphasized such that historical processes have the stability of institutions over the long term. A social learning approach applied to an organization could concentrate on individual learning and information sharing to examine the impact of changes in procedures and conduct. A historical institutionalism approach applied to an organization could focus on the dependence on an organization that is moulded to historical legacies.[187]

When considered through a specific level of analysis, social learning focuses on how individuals and groups learn through the spread of practices at various focus levels. Focusing on micro-level organizational processes highlights the importance of cognitive functioning, social networks, and knowledge acquisition.[188] Historical institutionalism focuses on how larger social institutions and structures influence organizational behaviour at the macro-level to highlight political, economic and social factors that affect institutions and organizations.[189] A social

[186] Chris Argyris and Donald A. Schön, *Organizational Learning: A Theory of Action Perspective*. (New York, NY: Addison-Wesley, 1978).
[187] Paul Pierson, *Politics in Time: History, Institutions, and Social Analysis*, (Princeton University Press, 2004).
[188] Barbara Levitt and James G. March, "Organizational Learning," *Annual Review of Sociology* 14 (1988): 319-340.
[189] Kathleen Thelen and James Mahoney, *Explaining Institutional Change: Ambiguity, Agency, and Power*, (Cambridge: Cambridge University Press, 2010).

learning perspective could study organizational change by examining how individuals or teams exchange information. A historical institutionalism perspective could examine how social norms or laws have affected an organization's decisions, strategies, and operational procedures.

Historical institutionalism and social learning are used to complementary ends to function as conceptual lenses. The project borrows critical concepts from each theory to better understand what cyber defence policy changes occurred at NATO. More significant conclusions are drawn about the limitations these observations present for contemporary deterrence that can then be applied to the cyber domain. Social learning and historical institutionalism borrow vital concepts to help identify and list developing policies to deter cyber threats in the cyber domain. NATO is demonstrated through Chapters 3 to 6 as a learning organization, given those social learning mechanisms are ingrained within internal, external, and affiliated learning procedures. The present manuscript will determine whether social learning better explains cyber defence policy development than historical institutionalism or whether using a mix of key concepts from both for the present analysis makes more sense.

The following applies social learning to explain internal policy developments. Rather than focus solely on how NATO creates learning opportunities, social learning is applied to explain internal policy developments resulting from the many internal procedures that NATO uses to facilitate internal social learning in the form of meetings, exercises, and other learning initiatives. Peter Hall discusses three orders of change which are applicable as levels of learning in the present discussion on international institutions.[190] The first order of change involves how policy tools are set or calibrated, leaving the broad outlines of policy untouched. The second

[190] Peter A. Hall, "Policy Paradigms, Social Learning, and the State: The Case of Economic Policy-making in Britain," *Comparative Politics* 25, no. 3 (1993): 275–96.

order involves reworking the tools themselves to change the instruments, such that policy tools are transformed based on the idea that the instruments were misguided. The third order involves a complete paradigm shift leading to the opportunity for new policy ideas to flourish.

Initial research assumptions understood cyber deterrence as a paradigm shift away from classical deterrence theory. However, in retrospect it does not make sense to consider the kind of cyber defence policy change at NATO as a paradigm change in the form of Hall's third order of change. Rather, it appears that institutional tools and instruments must be adapted to adhere to the contemporary threat landscape, such that there remains a need to change and sharpen the tools themselves to address contemporary threats. Hall's second order of change is more appropriate to understand observable change at NATO, such that cyber defence policy amounts to the recalibration of policy tools rather than dealing with a complete overhaul represented by a paradigm shift. Added features beyond deterrence may be found to be more appropriate to deal with cyber threats than other threats concerning multi-domain operations.

Learning opportunities cultivated social learning at NATO through the regularity of meetings, exercises, discourse, and other training; all contributing to the social learning of the group. Hall identifies that change within institutions results from internal actors "puzzling," rather than solely being based on politics based on exercises of power.[191] In the NATO context, Allies and other key stakeholders have actively "puzzled" over contemporary problems to develop new tools and techniques. Numerous empirical examples are included throughout the timeline, and were also depicted in interviews with research participants.

Puzzling over policy observably led to learning about new concepts which can be used to supplement deterrence theory with new strategic approaches. Returning to Hillel Soifer to apply

[191] Ibid.

the concept of "productive conditions" to understand how internal deliberations within NATO resulted in specific policies.[192] Recall that permissive conditions are where critical junctures can impact the previously unchanging status quo. Productive conditions are used to understand the specific kinds of change that occur when internal learning mechanisms within NATO facilitate new ideas of opportunities to build consensus. The "productive conditions" of Soifer apply the "puzzling" of Hall to demonstrate social learning through interactive character at NATO. The cyber challenge to classical deterrence depicts empirical evidence of significant gaps in security strategy which requires further examination to develop measures to fill these gaps.

2.6 – Theoretical Approaches

2.6.1 Deterrence Theory

Chapter 1 provided a detailed breakdown of the numerous concepts within deterrence theory and the related security studies literature on emerging technologies and hybrid threats. The present section seeks to demonstrate how these concepts are used to address the evolution of deterrence theory from classical to contemporary forms and to understand the evolution of security policy with newly emerging technologies. Risks posed by modern technologies, including cyber threats, have forced deterrence theory to evolve from its classical roots to a contemporary stance. Thus, contemporary deterrence reacts to these hybrid threats, using unconventional means to signal desired inaction and credibility to take action.

Strategic innovations include combining offensive and defensive strategies within a cyber deterrence framework. Offensive strategies seek to cause network disruption with warnings that

[192] Hillel Soifer, "The Causal Logic of Critical Junctures," *Comparative Political Studies* 45, no. 12 (2012): 1572–97.

cyber attacks will be responded to with cyber effects.[193] Cyber deterrence can achieve objectives through offensive and defensive preparations. Concerns remain over when such an approach becomes cyber coercion, risking the dangers of escalation calculation and pre-emptive targeting. Furthermore, coordinated operations using diplomatic, economic, military, and legal powers raise concerns about the ability of deterrence to combat such contemporary threats.[194]

Contemporary deterrence is challenged to operate in the cyber domain by numerous concerns. For example, the anonymity of the adversary makes attribution difficult and in light of asymmetric power shifts, small groups or individuals can significantly impact the cyber realm.[195] Anonymity breeds the challenge of attributing threat actors, with dangers for unintentional escalation and little consensus on countermeasures.[196] Strategic approaches to active cyber defence, forward defence, and persistent engagement operate beyond an organization's cyber defence posture to withstand such attacks and rapidly resume normal operations. The reliance of today's cyber defence on resilience and collaboration provides essential foundation characteristics. Further cyber fortification through defence capacity building and contingency plans are among other preventative defensive actions.

Many cyber frameworks uphold strict standards and regulations, including the National Institute of Standards and Technology in the United States.[197] Active cyber defence includes actively seeking threat actors to stop them before they can do damage. These relationships

[193] Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (April 3, 2015): 316–48, https://doi.org/10.1080/09636412.2015.1038188.
[194] David M. Harold and Susan J. Martin, "Cyber Deterrence and Its Limitations," in *Handbook of Cyber Security*, eds. Liming Chen, Sushil Jajodia, and X. Sean Wang, (Springer, 2014), 111–134.
[195] Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (April 3, 2015): 316–48, https://doi.org/10.1080/09636412.2015.1038188.
[196] Erica Borghard and Shawn Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies* 26 (July 3, 2017): 452–81, https://doi.org/10.1080/09636412.2017.1306396.
[197] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1" (Gaithersburg, MD: National Institute of Standards and Technology, April 16, 2018), https://doi.org/10.6028/NIST.CSWP.04162018.

between individual states, national standards, and regulations are explored in the Tallinn Manual, currently developing Version 3.0, as an account of comprehensive cyber capabilities within international law.[198] Further, multilateral relationships explore intelligence sharing, joint cyber defence collaboration, international cooperation, and formalized agreements.

2.6.2 Cyber Persistence Theory and Accumulation Theory

Defending forward is a proactive strategy developed by the United States Department of Defense to thwart threats before they reach their intended targets.[199] Threat hunters look for dangers in the early stages to disable threat actor efforts before they can be successful. Cyber persistence theory illustrates the difficulty posed by threats to accumulate and grow over time. Cumulative cyber campaigns of small-scale cyber attacks can build, and limited initial access can lead to a massive breach, compromise, or attack. Accumulation theory adds that minor cyber attacks can serve threat actors to launch more significant attacks later. Initial access escalates privileges through internal lateral movements on an organization's network. NATO's Brussels Summit Communiqué of 2021 states that "cumulative cyber attacks" may be sufficient to invoke Article 5 on a "case by case basis."[200] This approach calls for a significant shift in thinking away from complete deterrence by denial to increasing costs and lowering benefits.

Adopting internal network threat hunting provides the added benefit of actively looking for threats on an organization's networks to remove unwanted traffic.[201] Advanced persistent

---

[198] Michael N Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. (Cambridge: Cambridge University Press, 2017), https://doi.org/10.1017/9781316822524.
[199] US Department of Defense, "Summary of the 2018 Department of Defense Cyber Strategy: Defending Forward and Persistent Engagement" (US Department of Defense, 2018), https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.
[200] NATO, "Brussels Summit Communiqué," NATO, (June 14, 2021), https://www.nato.int/cps/en/natohq/news_185000.htm.
[201] Ryan Tate and Chad Bates, "Deterrence Thru Transparent Offensive Cyber Persistence," *The Cyber Defense Review* 7, no. 4 (2022): 227–46.

threats (APT) are among the most challenging cyber threat actors because they target campaigns against specific networks and specialize in specific tactics. Increasingly professional organized cyber criminals add to the array of highly resourced adversaries that a state can call on to carry out national business while officials remain able to plausibly deny any involvement.

2.7 – General Theoretical Considerations

Chapter 1 detailed various kinds of contemporary deterrence to outline critical concepts as part of the literature to understand how deterrence has evolved from its classical origins to its contemporary iteration. These concepts are featured within the recent introduction of the theoretical approaches of deterrence, persistence, and accumulation theories. These theoretical approaches are combined with the critical concepts borrowed from conceptual lenses of historical institutionalism and social learning.

Critical dynamics are identified during the evolution of NATO cyber defence policy over twenty-two years, with a significant focus on how external historical events impacted internal policy developments. Formal and informal learning procedures facilitated an organizational use that was apt to change while remaining unified. Deterrence is less effective in the cyber domain, where contemporary approaches show promise. However, it remains to be seen whether more coercive approaches related to defending forward and persistent engagement are more appropriate to deter threats in the cyber domain.

2.7.1 – Revolution or Evolution

Rapid technological change in the threat environment challenges Allies to innovate policy in response to global strategic competition. It is important to differentiate whether

institutional policy change results from a revolution or evolution, which depends on the pace and extent of the change. Revolutions involve relatively quick fundamental changes in the threat landscape. Evolutions involve gradual changes that can be fundamental but are drawn out over time. The hybrid warfare concept is indebted to a rich literature on technology applications to non-conventional military strategies.

The first modern study of hybrid warfare demonstrates the decentralization of mobilization strategies during the Second Chechen War beginning in 1999 to complement conventional tactics using technology to attain strategic objectives.[202] Hezbollah's use of hybrid warfare in the 2006 Lebanon War provides an example of the use of hybrid capabilities to embody "political, social, diplomatic, and informational components," from years of "humanitarian aid, building physical infrastructure, … [and] serving as medical providers."[203] This example demonstrates operations requiring the synchronization of components between strategic and tactic levels, including: "conventional capabilities, irregular tactics and formations,… indiscriminate violence,… coercion, and criminal disorder."[204]

A central goal of hybrid warfare is to control "the support of the combat zone's indigenous population,… the home front of the intervening nations, and the support of the international community."[205] The coordination of conventional and non-conventional forces "in conjunction with psychological, economic, [and] political… assaults," occurs between all levels

[202] William J. Nemeth, "Future War and Chechnya: A Case for Hybrid Warfare," *Naval Postgraduate School*, (2002), https://core.ac.uk/download/pdf/36699567.pdf.
[203] Russell W. Glenn, "Thoughts on 'Hybrid' Conflict," *Small Wars Journal*, (February 3, 2009), https://smallwarsjournal.com/jrnl/art/thoughts-on-hybrid-conflict.
[204] Hoffman, "Conflict in the 21st Century," 29.
[205] John J. McCuen, "Hybrid Wars" *Joint Special Operations University Report 13-4*, (Tampa, Joint Special Operations University, 2013): 108, https://www.hsdl.org/?view&did=744761.

of operation.[206] The convergence of operations across threat levels amounts to the increasing "synthesis of technological progress," which contributes significantly to military success.[207]

2.7.2 American and Russian Contemporary Warfare

Debates on the hybrid warfare concept increasingly rely on conceptual lineages, including debates over eight years since Russia's annexation of Crimea in 2014. American and Russian concepts of contemporary warfare apply to the current discussion. American Fourth Generation Warfare acknowledges that states have lost the "monopoly on war," given the increasing blend of force capabilities, including fighters, non-combatants, and non-state actors.[208] Joint operations achieve strategic objectives by the "most effective" means, which blur the lines "between responsibility and missions."[209] Non-traditional areas of competition continue to blur distinctions between military, civilians, war, and peace.

Russian New Generation Warfare involves tailoring hybrid threats to target "adversaries' decision cycles… designed around the weaknesses of Russian adversaries."[210] A 2013 article by Russian Federation Chief of the General Staff, General Valery Gerasimov, provides insight into the Russian military's interpretations of warfare in the 21st Century.[211] Past distinctions between war and peace remain blurry such that "wars are no longer declared, and when they begin, they

---

[206] Joshua Ball, "What Is Hybrid Warfare? Non-Linear Combat in the 21st Century," *Global Security Review*, (August 1, 2018), https://globalsecurityreview.com/hybrid-and-non-linear-warfare-systematically-erases-the-divide-between-war-peace/.
[207] Albertas Kondrotas, "Private Armies Throughout the Generations of Warfare: Pitfalls and Prospects," *National Defense Academy of Estonia,* (Tallinn, National Defense Academy of Estonia, 2010): 16-17.
[208] Lind et al., "The Changing Face of War," 88.
[209] Ibid.
[210] John Chambers, "Countering Gray-Zone Hybrid Threats: An Analysis of Russia's New Generation Warfare and Implications for the US Army," *West Point Modern War Institute*, (October 18, 2016), https://mwi.usma.edu/wp-content/uploads/2016/10/Countering-Gray-Zone-Hybrid-Threats.pdf.
[211] Valery Gerasimov, "The Value of Science Is in the Foresight," *Military Review*, (February 2016), 24.

do not follow the pattern that we are accustomed to."[212] Strategic objectives target political, economic, informational, humanitarian, and non-military focus areas, requiring substantial cooperation across strategic, operational, and tactical levels. For Gerasimov, the characteristics of contemporary warfare include flexible, non-static strategic logic to tailor tactics to operations.

2.7.3 From Crisis to Policy

Crisis can justify a unity of effort to establish political will, which starts the policy-making process against cyber threats at NATO. The project timeline includes many unprecedented cyber attacks as critical junctures involving various NATO countermeasures toward policy development and institutional investments in years to come. In various interviews with research participants, NATO Officials cited Estonia in 2007, Georgia in 2008, and Crimea in 2014 as prime examples of cases where security policy did not initially account for technological change. Significant precedent-setting cyber attacks require political will to take the necessary measures to survive a crisis. Procurement decisions for policy investment occur after precedent-setting cyber attacks. Allies agree to invest in cyber defence capabilities in the years that follow various critical junctures - including the 2010 Strategic Concept.

Allies agreed that significant policy developments at the Lisbon Summit necessitated more investment in NATO cyber defence. NATO's 2010 Strategic Concept and other significant policy documents included new language, which led to institutional policy change caused by increased political will and proposed investment in cyber defence. The institutional and policy developments provided language for policymakers to heighten momentum to develop policy and investments in 2011. The NATO Lisbon Summit Communiqué demonstrated a gradual increase

[212] Ibid., 28.

in language on cyber defence over ten years between 2000 and 2010. The inclusion of more language on cyber defence in these crucial policy documents - the 2010 Strategic Concept and Lisbon Summit Communiqué - led to more cyber defence policy initiatives and additional funding.

2.7.4 Cyber Norms and International Law

A normative approach to cyber deterrence focuses on the impact of norms, values, and other constructions of knowledge on security strategy.[213] Major cyber attacks restrain actors from escalating conflict to higher levels of contention.[214] Collective restraint prevents actors from targeting critical infrastructure out of fear of "retaliation and escalation of conflict beyond control."[215] Escalation limits conventional thresholds as targets remain in the cyber domain to cause significant disruption, devastation, and destruction.[216]

Some argue that cyber space requires new international laws to address the "complexity, dynamism, and novelty of the strategic cyber environment."[217] In 2017, Microsoft President Brad Smith spoke of the private sector's role in the cyber domain "as a neutral Digital Switzerland that assists customers everywhere and retains the world's trust."[218] Smith noted the function of the private sector is similar to the Red Cross's role in helping to formulate the Fourth Geneva Convention in 1949.

---

[213] Amir Lupovici, "The Emerging Fourth Wave of Deterrence Theory—Toward a New Research Agenda," *International Studies Quarterly* 54, no. 3 (2010): 722.
[214] Erica D. Borghard and Shawn W. Lonergan, "Cyber Operations as Imperfect Tools of Escalation," *Strategic Studies Quarterly*, (2019, no. 3): 133.
[215] Nye, "Deterrence and Dissuasion," 51.
[216] Jason Healey and Robert Jervis, "The Escalation Inversion and Other Oddities of Situational Cyber Stability," (2020), https://doi.org/10.26153/TSW/10962.
[217] Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, *Cyber Persistence Theory: Redefining National Security in Cyberspace* (New York: Oxford University Press, 2022): 92.
[218] Brad Smith, "The Need for a Digital Geneva Convention," *Microsoft On the Issues*, (February 14, 2017), https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

Proponents have criticized calls to create new international cyber laws, arguing that international law already applies to new technologies and includes the cyber domain. In an interview for this study, NATO Official 6 states that the pursuit of new international law in the cyber domain misunderstands that international law is agnostic and can apply to the cyber domain just as it can apply to changes in other domains. The official argues there is no need for a new convention or treaty to deal with threats in cyberspace, given that international law currently applies to threats in cyber space.

2.7.5 Tallinn Manual

The release of the Tallinn Manual in February 2013 provides details on how the international law of armed conflict applies to threats in the cyber domain. The Tallinn Manual's Director, Michael Schmitt, also Director of International Law at the United States Naval War College, emphasizes the dangers of "war without understanding what law applies and how it applies… in an era when cyber operations are central to armed conflict."[219] Article 36 of the First Additional Protocol to the Geneva Conventions justifies the application of the Law of Armed Conflict to cyberspace, according to International Committee of the Red Cross Legal Advisor Laurent Gisel. The article requires states to "apply the law of armed conflict to new military technologies or means of waging war."[220] Concepts such as the "use of force" and the "right to self-defence" in the United Nations Charter remain central to deliberations of the Tallinn Manual drafters, given the subject matter of these concepts.

[219] Spencer Kimball, "NATO Moves to Apply Armed Conflict Law to Cyber Warfare," *Deutsche Welle,* (July 2, 2014), https://www.dw.com/en/nato-moves-to-apply-armed-conflict-law-to-cyber-warfare/a-17754359.
[220] Kimball, "NATO Moves to Apply Armed Conflict Law to Cyber Warfare."

The influence of the Tallinn Manual on NATO policymaking is demonstrable through indirect means, given the document is not explicitly a NATO agreed-upon document. The Manual nonetheless provides senior policymakers and field experts valuable insights into the specific international law cases that apply to the cyber domain. A similar learning pattern is observable, with exercises run by the Cooperative Cyber Defence Centre of Excellence in Tallinn, which continues to provide unique resources for future exercises.

2.8 – Cyber Diplomacy, International Law, and Norms

2.8.1 Group of Government Experts

NATO reaffirms its commitment to applying international law in cyberspace, including in Summit Communiqués and the 2022 Strategic Concept.[221] NATO Summit Communiqués, Strategic Concepts, and other policy documents reference the United Nations' international legal developments in cyberspace. The Group of Government Experts began in 2004 to study "the threats posed by the use of Information Communication Technologies… in the context of international security and how these threats should be addressed."[222] The 2013 report of the Group of Government Experts outlines recommendations on “norms, rules and principles” of responsible state behaviour, such that “international law, and… the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible [digital] environment.”[223] Each report by the New Group of

[221] NATO, “Madrid Summit Declaration,” NATO, (June 29, 2022), https://www.nato.int/cps/en/natohq/official_texts_196951.htm.
[222] United Nations Officer of Disarmament Affairs (UNODA), “Developments in the Field of Information and Telecommunications in the Context of International Security,” *United Nations Officer of Disarmament Affairs*, (New York, UNODA) n.d., https://www.un.org/disarmament/ict-security/.
[223] United Nations General Assembly (UNGA), “Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,” (New York: United Nations General Assembly, June 24, 2013), https://undocs.org/A/68/98.

Experts builds upon the recommendations of the last. The 2015 Group built off the recommendations of the 2013 report, the latter of which outlines the "voluntary, non-binding norms, rules, or principles of responsible behaviour of States aiming to promote an open, secure, stable, accessible and peaceful ICT environment."[224]

In 2017, the Group of Experts failed to agree to include fundamental international legal concepts of self-defence and international humanitarian law. The 2017 iteration of the Group of Experts "collapsed" when a few states-including Russia, China, and Cuba - rejected "the final report's proposed text."[225] These states "signalled their acceptance of both self-defence and humanitarian law" in the 2015 report.[226] The failure of the 2017 Group of Experts resulted from "international politicization in the cyber context of well-accepted international law norms."[227] It remains to be seen how these international legal developments will continue given an observable divergence between these institutional approaches.

2.8.2 Open-Ended Working Group

In December 2018, the United Nations General Assembly established the Open-Ended Working Group through resolution 73/27.[228] The United Nations encouraged all member states

[224] United Nations General Assembly (UNGA), "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security" (United Nations General Assembly, July 22, 2015), https://undocs.org/A/70/174.
[225] Michael N. Schmitt and Liis Vihul, "International Cyber Law Politicized: The UNGGE's Failure to Advance Cyber Norms," *Just Security*, (June 30, 2017), https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/.
[226] Michael N. Schmitt, "Taming the Lawless Void: Tracking the Evolution of International Law Rules for Cyberspace," *Texas National Security Review* 3, no. 3 (Autumn 2020): 33.
[227] Schmitt and Vihul, "International Cyber Law Politicized."
[228] United Nations Office of Disarmament Affairs (UNODA), "Open-Ended Working Group," (New York: UNODA, 2018), https://www.un.org/disarmament/open-ended-working-group/.

to participate in "consultative meetings with industry, civil society, and academia."[229] The formation of the Open-Ended Working Group led to two separate resolutions: a document "sponsored by Russia," and another document with the United States' sponsorship to "further" the Group's 2015 framework.[230] Both the Group of Experts and Working Group presented reports in 2021.

The Working Group's report includes 193 state participants, while the Group of Experts includes 25 state participants.[231] Institutional dialogue provides viable options, yet all parties left "equally unhappy" given that decisions seemed "new without bringing much new."[232] The 2021 Group of Experts report provides "a substantive step forward" yet remains challenged to get individual states "to make voluntary national contributions… on the subject of how international law applies to" state use of cyber capabilities.[233]

2.8.3 Challenges to Normative Approaches

Cyber norms and international law are challenged in the cyber domain by limitations that impose costs on threat actors for breaking norms and international law. In an interview for this study, NATO Official 20 argues that there remains the challenge to appear to take international law and norms seriously. The official notes that some states vocally uphold cyber norms while actively breaking the same norms in practice and limiting the credibility of the norm as an agreement in word but not deed. The Group of Governmental Experts vocalized support for

[229] United Nations Office of Disarmament Affairs (UNODA), "Developments in the Field of Information and Telecommunications in the Context of International Security," *United Nations Officer of Disarmament Affairs*, https://www.un.org/disarmament/ict-security/.
[230] Fischerkeller, Goldman, and Harknett, *Cyber Persistence Theory, 93*.
[231] Ibid.
[232] Pavlina Ittelson, "What's New with Cybersecurity Negotiations? UN Cyber OEWG Final Report Analysis," *Diplomacy*, (March 19, 2021), https://www.diplomacy.edu/blog/whats-new-cybersecurity-negotiations-un-cyber-oewg-final-report-analysis/.
[233] Fischerkeller, Goldman, and Harknett, *Cyber Persistence Theory,* 94.

norm 13(f), such that a "state should not conduct or knowingly support [cyber] activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public."[234]

The challenge is when states use cyber operations to target critical infrastructure, to "damage… or otherwise impair [its] use," while simultaneously upholding the report by the Group of Experts.[235] Developing cyber norms and related international law will take time to establish. Competitors challenge NATO and require immediate approaches.[236] Responsible offensive cyber operations provide a means to respond to threats in the cyber domain that overcome the power vacuum left by inaction. Deterrence by entanglement relies on normative approaches to apply international law to cyberspace, and numerous entanglement-related challenges limit the availability of prudent response options.[237]

2.8.4 Restraint and Adventurism

The United States Department of Defense released *a Cyber Strategy* in April 2015.[238] The strategy characterized a "Doctrine of Restraint" that operated within "the parameters of Cold War security paradigms that relied on nuclear threats to deter war… [and] coincided with adversarial adventurism and led to strategic losses."[239] Policy debates and developments on cyber norms and international law challenge the unprecedented social reliance on digital

[234] UNGA, "Group of Governmental Experts, 2015."
[235] Ibid.
[236] Weber, "The Illusion of 'Responsible' Cyber Offense."
[237] Adams, Aitel, Perkovitch, and Work, "Responsible Cyber Offense."
[238] United States Department of Defense, "The Department of Defense Cyber Strategy," *United States Department of Defense,* (Washington, DC, USDOD, 2015).
[239] Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, "Persistent Engagement in Cyberspace Is a Strategic Imperative," *The National Interest*, (July 6, 2022), https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/persistent-engagement-cyberspace.

infrastructure to establish, apply, and enforce the rule of law in cyberspace. These important developments require pervasive innovation for digital infrastructure to establish the foundations to build solid cyber norms and related international law.

This period of cyber restraint involves developments establishing cyber norms and applying international law in cyberspace. Nevertheless, without practical applications of these developments, threat actors took advantage of the power vacuum to participate in adventurism between 2000 and the release of the United States Department of Defense's 2015 policy.[240] While Allies debate cyber norms and international law, adversaries experiment with using cyber space as "a new competitive environment where strategic gains could be achieved through continuous activity below the threshold at which deterrence functions effectively."[241] This period of restraint provides adversaries time to experiment with new tactics, techniques, and procedures in cyber space with little direct challenge.

The transformation of the United States' cyber doctrine between 2015 and 2018 included the release of Cyber Command's new vision statement. Contemporary threats in the cyber domain involve sophisticated adversaries "increasingly capable of contesting and disrupting America's society, economy, and military."[242] The threat landscape came to involve the vast interconnection of "direct continuous operations" to conduct the "activities against our allies… in campaigns short of open warfare to achieve competitive advantage and impeded [United States] interests."[243]

---

[240] Ibid.
[241] Ibid.
[242] United States Cyber Command, "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," United States Cyber Command, (April 2018), https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.
[243] Ibid.

Chapter 3: Founding NATO Cyber Defence

3.1 – Opening Remarks

Recall this project's central research question on NATO's evolving strategic deterrence doctrine to address contemporary security threats in the cyber domain. The project presents a descriptive analysis of the evolution of NATO cyber defence policy after major precedent-setting cyber incidents. Complementary research questions approach political and strategic considerations to inform cyber defence policy at NATO. Moreover, three conceptual lenses analyze the implementation of cyber defence policy during NATO's evolution over the two-decade timeline in Chapter 2. Key findings are found at the end of the four phases in Chapters 3, 4, 5, and 6.

3.2 – An Overview of NATO Pre-2000

3.2.1 NATO's Founding

NATO is a political-military Alliance among the governments of 28 European nations and two North American nations. NATO formed with the signing of the Washington Treaty in Washington, DC, on April 4, 1949. The twelve founding members were Belgium, Canada, Denmark, France, Iceland, Italy, Luxembourg, Netherlands, Norway, Portugal, the United Kingdom, and the United States. NATO was formed after World War II on the agreement to abide by the collective defence and defend each other from external threats, which at the time was conceived primarily against the Soviet Union during the Cold War. Alliance members shared a dedication to promoting democratic values and peaceful conflict resolution in the Euro-Atlantic region.

NATO membership expanded to include many new Allies from the 1950s to now. Greece and Türkiye joined NATO in 1952, Germany in 1955, and Spain in 1982. In 1999, the Czech Republic, Hungary, and Poland joined NATO. In 2004, Bulgaria, Estonia, Latvia, Lithuania, Romania, Slovakia, and Slovenia joined NATO. In 2009, Albania and Croatia joined NATO. The Alliance's newest members - Montenegro and North Macedonia - joined NATO in 2017 and 2020, respectively. At the NATO Madrid Summit in June 2022, Finland and Sweden were invited to become members of NATO and signed the Accession Protocols.[244] The NATO Parliamentary Assembly outlined the following:

> These protocols are, in effect, amendments or additions to the treaty, which, once signed and ratified by the Allies, become an integral part of the treaty itself and permit the invited countries to become parties to the treaty. From the moment the Accession Protocols are signed, NATO invites representatives of the invited countries to attend meetings of the North Atlantic Council as observers.[245]

Following the accession, NATO Allies began to ratify the protocols, and as of October 2022, all member states except Hungary and Türkiye had completed this requirement. Hungary ratified Finland on March 27, 2023, and Türkiye ratified Finland on March 31, 2023. Finland was welcomed into NATO on April 4, 2023.[246] Once all Allies have completed the ratification process, the Secretary-General will invite Sweden to accede to the North Atlantic Treaty.[247]

[244] NATO, "Madrid Summit Declaration."
[245] NATO Parliamentary Assembly, "Ratification of Finland and Sweden's Accession to NATO," Finland and Sweden Accession, (Brussels, NATO Parliamentary Assembly), March 27, 2023.
[246] Reuters, "Turkish Parliament Ratifies Finland's NATO Accession as Sweden Kept Waiting," *Reuters,* (March 31, 2023), https://www.reuters.com/world/europe/turkish-parliament-approves-finlands-nato-accession-2023-03-30/.
[247] NATO Parliamentary Assembly. "Ratification of Finland and Sweden's Accession to NATO."

3.2.2 NATO Enlargement

NATO enlargement stems from its open-door policy to grant other states membership if they meet specific requirements.[248] The North Atlantic Council decides to invite a country to join NATO.[249] Article 10 of the North Atlantic Treaty outlined the opportunity for membership, such that Allies may "by unanimous agreement, invite any other European States in a position to further the principles of the Treaty to contribute to the security of the North Atlantic."[250] NATO's Membership Action Plan helped states meet the requirements to become members with practical assistance and training initiatives.[251]

3.2.3 The Council and Network of Committees

NATO Headquarters is in Brussels, Belgium, to enable permanent consultations on short notice with political oversight held by the Heads of State of Allies. Article 9 of the North Atlantic Treaty established that the North Atlantic Council represented each member nation with the ability to "meet promptly at any time," to set up "subsidiary bodies as may be necessary," and recommend the implementation of other articles of the North Atlantic Treaty."[252] The Council is the highest decision-making body at NATO and oversees all political and military decisions made through consensus agreement by Allies.

---

[248] NATO, "Enlargement and Article 10," NATO, (July 10, 2022), https://www.nato.int/cps/en/natohq/topics_49212.htm.
[249] NATO, "Member Countries," NATO, (September 14, 2022), https://www.nato.int/cps/en/natohq/topics_52044.htm.
[250] NATO, "The North Atlantic Treaty."
[251] NATO, "Membership Action Plan," NATO, (March 23, 2020), https://web.archive.org/web/20220227230934/https:/www.nato.int/cps/en/natolive/topics_37356.htm.
[252] NATO, "The North Atlantic Treaty."

Military representatives from the Military Committee included Allied Command Operations, with headquarters in Mons, Belgium, and Allied Command Transformation, with headquarters in Norfolk, United States. The various headquarters provided the primary sources of military advice for NATO senior decision-makers. NATO Headquarters in Brussels, Belgium, hosted a multitude of focused committees which completed the day-to-day initiatives involved in reporting to NATO senior decision-makers. NATO's Cyber Defence Committee, where all cyber defence-related committee discussions occur at NATO, is operated by the Cyber and Hybrid Policy Section in the Emerging Security Challenges Division. NATO International Staff, International Military Staff, and other Allied representatives collaborated to agree on a policy passed up to the North Atlantic Council for approval. Allies hold sole executive power in NATO. The International and International Military Staff facilitate the work to draft policies, reports, and documents required to undergird debates in Council sessions.

3.2.4 North Atlantic Treaty

Article 3

Multiple Articles of the North Atlantic Treaty are directly related to the present research project. Article 3 stated that Allies "separately and jointly, through continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack."[253] Part of these developments included commitments to spend a minimum of 2% of GDP on defence as outlined in 2006.[254] Allies reiterated the sentiment at the 2014 Wales

[253] Ibid.
[254] James Appathurai, "NATO Speech: Briefing by NATO Spokesman," *NATO*, (June 6, 2006), https://www.nato.int/docu/speech/2006/s060608m.htm.

Summit, and member states that still needed to meet the 2% guideline voluntarily committed to doing so within a decade by 2024.[255]

Russia's annexation of Crimea in 2014 brought even more attention to Article 3. For example, the resilience baselines were released at the 2016 Warsaw Summit to "improve civil preparedness… continuity of government, continuity of essential services, security of critical civilian infrastructure, and support to military forces with civilian means."[256] These increased resilience commitments aligned with the Cyber Defence Pledge, another initiative established at the 2016 NATO Warsaw Summit focused specifically on the cyber defence commitments of Allies. The Pledge and baselines overlapped on crucial areas that kept cyber networks online and directly involved keeping the societies that depend on them online too.

Article 4

Article 4 outlined the process for Allies to request meetings to discuss pressing issues to "consult together whenever… the territorial integrity, political independence or security of any of the Parties [is] threatened."[257] Article 4 functioned as a starting point for many NATO operations to consult on military matters officially to decide the next steps. The Report of the Committee of Three on Non-Military Cooperation in NATO outlined the procedures involved with Article 4, released on December 13, 1956. Processes were outlined such that:

> Special attention must be paid… to matters of urgent and immediate importance to the members of NATO, and to "emergency" situations where it may be necessary to consult closely on national lines of conduct affecting the interests of members of NATO as a whole… While members of NATO are responsible for consulting with their

[255] NATO, "Wales Summit Declaration," *NATO*, (September 5, 2014), https://www.nato.int/cps/en/natohq/official_texts_112964.htm.
[256] NATO, "Warsaw Summit Communiqué," *NATO*, (July 9, 2016), https://www.nato.int/cps/en/natohq/official_texts_133169.htm.
[257] NATO, "The North Atlantic Treaty."

> partners on relevant matters, a large share of responsibility for such consultation necessarily rests on the more powerful members of the Community.[258]

Article 4 has been invoked seven times in NATO's history. Türkiye invoked Article 4 five times concerning its border with Iraq and Syria between 2003 and 2020. The present study focused on the other two times Article 4 was invoked, given its relevance to this project. First, Latvia, Lithuania, and Poland invoked Article 4 in March 2014 in response to Russia's annexation of Crimea.[259] NATO deployed forces to the Black Sea and imposed sanctions on key Russian officials, and the North Atlantic Council released a statement condemning the "serious breach of international law and a major challenge to Euro-Atlantic security."[260] Allies agreed on NATO Enhanced Forward Presence at the Warsaw Summit 2016, which deployed NATO defence and deterrence forces to Ally-led battlegroups in Estonia, Latvia, Lithuania, and Poland.[261] These battlegroups demonstrated the significant response that NATO gathered two years after Russia's annexation of Crimea in 2014.

Article 4 was invoked again by Bulgaria, Czech Republic, Estonia, Latvia, Lithuania, Poland, Romania, and Slovakia in February 2022 in response to Russia's invasion and full-scale war on Ukraine. NATO deployed forces to its eastern flank, and the Allies provided material support to Ukraine.[262] The NATO Response Force and the Very High Readiness Joint Task

---

[258] NATO, "Report of the Committee of Three on Non-Military Cooperation in NATO," *NATO*, (December 13, 1956), https://www.nato.int/cps/en/natohq/official_texts_17481.htm.
[259] NATO, "Press Conference by NATO Secretary General Jens Stoltenberg Following the Meeting of the NATO-Ukraine Commission," *NATO*, (November 26, 2018), http://www.nato.int/cps/en/natohq/opinions_160789.htm.
[260] NATO, "Statement by the North Atlantic Council on Crimea," NATO, (March 18, 2019), https://www.nato.int/cps/en/natohq/news_164656.htm.
[261] NATO, "NATO's Military Presence in the East of the Alliance," *NATO*, (July 8, 2022), https://www.nato.int/cps/en/natohq/topics_136388.htm.
[262] NATO, "Statement by the North Atlantic Council on Russia's Attack on Ukraine," *NATO*, (February 24, 2022), https://www.nato.int/cps/en/natohq/official_texts_192404.htm

Force activated for the first time in Alliance history in February 2022, previously only used for disaster relief or high-profile security events.[263]

Article 5

NATO's primary commitment to collective defence is encapsulated by Article 5. If one member state is attacked, all other Allies will respond to provide military support. Article 5 has only ever been invoked in NATO's history in response to the terrorist attacks on the United States on September 11, 2001. Article 5 states:

> The Parties agree that an armed attack against one or more in Europe or North America shall be considered an attack against them all. Consequently, they agree that if such an armed attack occurs, each of them, in the exercise of the right of individual or collective self-defence recognized by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of Armed Forces, to restore and maintain the security of the North Atlantic area... Any armed attack and all measures taken shall be immediately reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security.[264]

After the fall of the Berlin Wall in 1989, NATO developed partnerships with former Soviet Union states. Many of these partnerships became part of NATO's enlargement in the 1990s. NATO's first crisis management operation was in 1995 in Bosnia and Herzegovina. The following section will begin with NATO in Kosovo in 1999. This case will depict the threat environment that shaped the development of cyber capabilities and information operations in the late 1990s.

---

[263] Associated Press, "NATO Response Force Is Being Activated, Stoltenberg Reveals; Its Numbers Can Grow to 40,000," *Associated Press*, (February 25, 2022), https://www.msn.com/en-us/news/world/nato-response-force-is-being-activated-stoltenberg-reveals-its-numbers-can-grow-to-40000/ar-AAUjgJZ.
[264] NATO, "The North Atlantic Treaty."

3.3 – NATO Operation Allied Force, 1999

Cyber capabilities provided NATO immense value for operations yet gave adversaries an avenue to target the Alliance. NATO's Operation Allied Force in Kosovo in 1999 represented the first critical juncture the Alliance experienced relevant to this project's timeline. This first critical juncture led to the founding of NATO cyber defence policy at the 2002 NATO Summit in Prague, Czech Republic. NATO operations in Kosovo 1999 demonstrated the need to develop cyber capabilities and led to related policy developments at the Summit.

3.3.1 Cyber Attacks During Operations in Kosovo

In 1999, significant cyber attacks occurred during NATO's Operation Allied Force. Jason Healey, Director of the Cyber Statecraft Initiative at the Atlantic Council, outlines "a flurry of cyber incidents against NATO and member governments and militaries, including a defacement of the webpage of Supreme Headquarters Allies Powers in Europe. In 1999, defacements against the [US] Department of Defence tripled."[265] NATO websites were targeted with defacement and disruption, temporarily taking them offline, but no corresponding data breaches or obstructions to NATO operations were reported.[266] NATO supplemented air capabilities with cyber attacks that targeted “Serbian computers and Serbian financial holdings outside the country.”[267] These malicious cyber activities are minor by current standards but set new precedents for the time. This critical juncture influenced decision-makers to formulate a firm NATO cyber defence

[265] Jason Healey, “Cyber Attacks Against NATO, Then and Now,” *Atlantic Council*, (September 6, 2011), https://www.atlanticcouncil.org/blogs/new-atlanticist/cyber-attacks-against-nato-then-and-now/
[266] Ibid.
[267] John Tirpak, “Washington Watch: Victory in Kosovo,” *Air & Space Forces Magazine*, (July 1, 1999), https://www.airandspaceforces.com/article/0799watch/.

policy. Several examples demonstrated that operations in Kosovo set new precedents for cyber warfare.

NATO conducted operations during the Kosovo War against the Federal Republic of Yugoslavia between March 24 and June 10, 1999. A diverse array of threat actors used cyber capabilities to attain strategic objectives during the NATO operation. Pro-Serbian forces targeted NATO, among other Serbian-Albanian non-state actors. NATO's operations in Kosovo involved unprecedented defensive capabilities because numerous cyber attacks targeted the Alliance operation in March 1999.

On March 31, 1999, NATO Spokesperson Jamie Shea addressed cyber attacks that had targeted NATO, stating that:

> Since March 28, the service from our Internet homepage has been erratic… it seems that we have been dealing with some hackers in Belgrade who have hacked into our website and caused line saturation of the server by using a bombardment strategy… our email system has also been saturated by one individual who is currently sending us 2,000 emails a day. Furthermore, we are dealing with macro viruses from Yugoslavia in the email system.[268]

NATO took steps to upgrade all server processing power by disabling all Internet services except Hypertext Transfer Protocol and email to make it harder to overwhelm servers with sudden website traffic surges.[269] These disruptive cyber attacks demonstrated to NATO policy-makers that NATO needed to upgrade its cyber capabilities immediately.

For NATO's Head of Integrated Data Service, Chris Scheurweghs, the attacks demonstrated the need to "identify alternative procedures to lessen the burden" on his staff of

[268] Jamie Shea, "NATO Press Conference: NATO's Role in Kosovo," *NATO*, (March 31, 1999), https://www.nato.int/kosovo/press/p990331a.htm.
[269] Dan Verton, "Serbs Launch Cyberattack on NATO," *FCW*, (April 4, 1999), https://fcw.com/1999/04/serbs-launch-cyberattack-on-nato/195288/.

two.[270] Scheurweghs added that this attack had a central lesson for NATO and its members: "We will have to invest much more in security, and the Internet is no longer just a side issue."[271] The influx of cyber attacks during the Operation in Kosovo demonstrates that further policy development requires increased funding for cyber defence at NATO.

On April 4, 1999, Serbian hackers conducted distributed denial of service attacks on the "server supporting the public affairs apparatus of the United States-led NATO operation in Kosovo, rendering the server virtually inoperable for several days."[272] In May 1999, NATO accidentally bombed the Chinese embassy in Belgrade. Hackers sabotaged United States government websites, including the Department of Energy, the Interior Department, and the National Park Service. The Department of Energy's webpage was defaced with the message:

> Protest USA's Nazi action! Protest NATO's brutal action! We are Chinese hackers who take no cares [sic] about politics. Nevertheless, we cannot stand by seeing our Chinese reporters being killed, which you might have known [sic]. Whatever the purpose is, NATO, led by the USA, must take responsibility. We will not stop attacking until the war stops! You have owed Chinese people a bloody debt which you must pay for.[273]

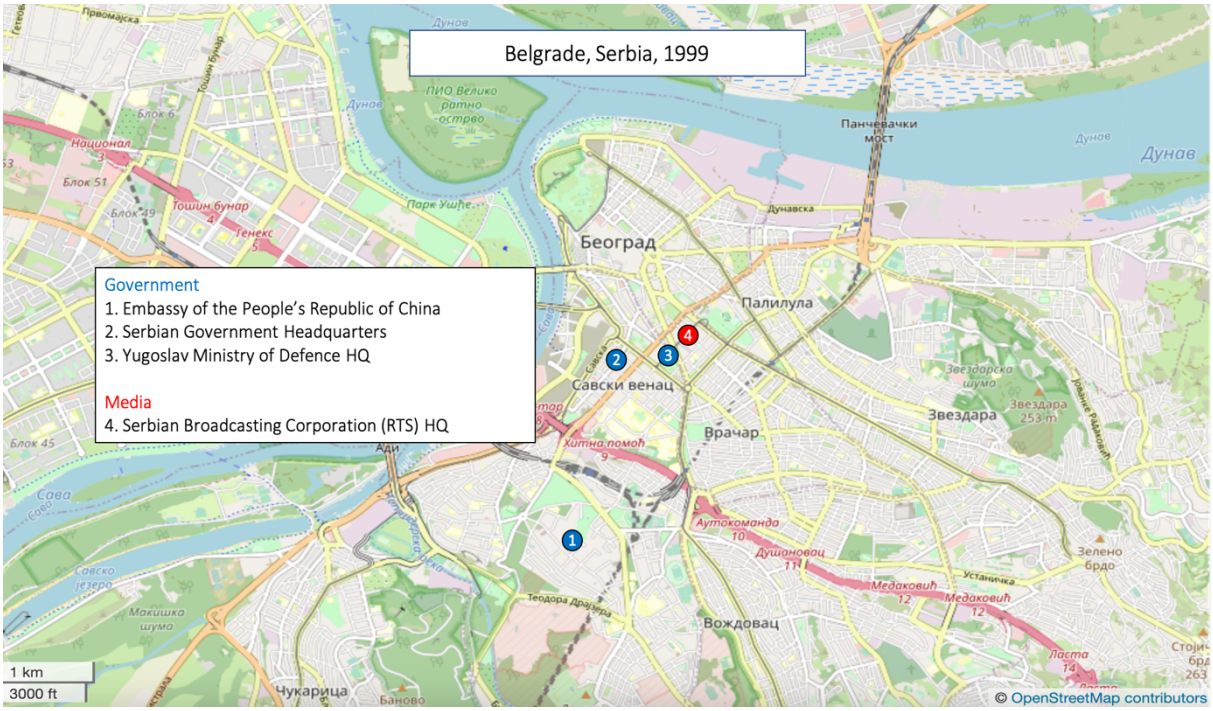
In response to these developments, the North Atlantic Council met in Brussels on April 12, 1999, to discuss Kosovo. Meeting objectives included an end to the military violence of the Milosevic government, a withdrawal of forces from Kosovo to establish a United Nations Peacekeeping presence, and the safe return of refugees to establish further political frameworks.[274]

---

[270] Ibid.
[271] Ibid.
[272] Ibid.
[273] Stephen Barr, "Anti-NATO Hackers Sabotage 3 Web Sites," *Washington Post*, (May 12, 1999), https://www.washingtonpost.com/wp-srv/inatl/longterm/balkans/stories/hackers051299.htm.
[274] NATO, "The Situation In and Around Kosovo," *NATO Press Release*, (June 29, 2011), https://web.archive.org/web/20110629141056/http://www.nato.int/docu/pr/1999/p99-051e.htm.

On April 30, 1999, hackers in the United States wrote anti-NATO messages and took the website "recreation.gov" offline for days.[275] They also posted the message “stop the war… NATO has screwed up… [Milosevic] does not give a damn about his people. He could not care less if they are dead or alive.”[276] Pro-NATO hackers were active within the borders of the Allies. In late April and early May 1999, a Dutch group called "Dutchthreat" replaced anti-NATO messages with pro-Kosovo messages, like "Help Kosovo… NATO is not out for blood, but for peace."[277] Servers of NATO and the United States were taken offline with allegations that Chinese and Russian attackers were responsible.[278]

Figure 3.1 – Cyber Attacks in Belgrade, Serbia, 1999



© Ryan J. Atkinson, 2023*

[275] Ellen Messmer, "Kosovo Cyber-War Intensifies: Chinese Hackers Targeting US Sites, Government Says," *CNN*, (May 12, 1999), http://edition.cnn.com/TECH/computing/9905/12/cyberwar.idg/.
[276] Ibid.
[277] Ibid.
[278] Mohan B Gazula, “Cyber Warfare Conflict Analysis and Case Studies,” *MIT Sloan School Working Paper*, (May 2017): 37.

*Note that the author developed all the maps in Microsoft PowerPoint, using screenshots of the location maps provided by ©OpenStreetMap via an open-source licence. See https://www.openstreetmap.org/copyright and the Appendix for the copyright information.

3.3.2 Precedent Setting Features of Operations in Kosovo

United States Joint Task Force Noble Anvil was the American cyber contributor to NATO Operation Allied Force. The Commander of United States Naval Forces Europe, James Elliss, noted that information operations and cyber capabilities were used to "great success" during operations in Kosovo.[279] A United States Naval Forces Europe spokesperson described the mission's information operations to include destroying adversary networks, infrastructure, and communications, including radar jamming.[280] The spokesperson added:

> [The American cyber contribution to Allied Forces] was the first time a Joint Task Force staff was organized with an information operations cell, which was composed of military personnel with expertise in various facets of [Information Operations]... actions taken to affect adversary information systems while defending one's own information and information systems… Offensive [Information Operations] included a wide range of actions, from destroying an enemy's information infrastructure to more traditional electronic warfare attacks, such as jamming an enemy's radar and attacking computer networks.[281]

On November 9, 1999, the NATO Supreme Commander in Europe, General Wesley Clark, said that "more could have been done" concerning strategy in Kosovo.[282] One option included targeting the bank accounts of Serbia's central leadership, which was avoided, given fears that war crimes could result from further unrest created by financial uncertainty.[283] NATO's Operation Allied Force was among the first to use "offensive computer warfare as a

[279] Brewin, "Kosovo Ushered in Cyberwar."
[280] Ibid.
[281] Ibid.
[282] Julian Borger, "Pentagon Kept the Lid on Cyberwar in Kosovo," *The Guardian*, (November 9, 1999), https://www.theguardian.com/world/1999/nov/09/balkans.
[283] Ibid.

precision weapon in connection with broader United States information operations against enemy defences."[284]

According to Benjamin Lambeth, a former Senior Research Associate at the RAND Corporation, the use of offensive cyber capabilities by Allies NATO within Operation Allied Force limited surface-to-air missile radar activity. The United States "did more information warfare in this conflict than we have ever done before, and we proved the potential of it," according to General John Jumper, former commander of United States Air Forces in Europe.[285] A United States Air Force Air Combat Command report suggested information operations involved "inserting viruses and deceptive communications into the enemy's computer systems."[286] Operation Allied Forces demonstrated that cyber capabilities were a precious and necessary asset for defence. Cyber incidents in Kosovo in 1999 represented the first critical juncture that impacted NATO's path dependence to become increasingly more cyber defence focused.

3.4 – Phase A, January 2000 to December 2006

3.4.1 NATO Prague Summit, 2002

On November 21, 2002, the NATO Summit occurred in Prague, Czech Republic. The Alliance adopted language within the Prague Summit Declaration to "strengthen [NATO] capabilities to defend against cyber attacks."[287] For the first time, the NATO Summit Declaration included language that focused on cyber defence. The inclusion of this language demonstrated

[284] Ibid.
[285] Benjamin S. Lambeth, *NATO's Air War for Kosovo: A Strategic and Operational Assessment* (RAND Corporation, 2001): 112, https://doi.org/10.7249/MR1365.
[286] Lambeth, "NATO's Air War for Kosovo," 112.
[287] NATO, "Prague Summit Declaration," *NATO*, (Brussels, NATO, November 21, 2002), http://www.nato.int/cps/en/natohq/official_texts_19552.htm.

recognition by NATO of the need to adapt the policy to address threats in cyberspace. Cyber attacks during NATO operations in Kosovo demonstrated unique challenges and opportunities.

NATO created the Computer Incident Response Capability following the Prague Summit in 2002 to "prevent, detect, and respond to cyber incidents" as part of the mandate of the NATO Communications Information Service Agency.[288] This Agency protected NATO's "own networks by providing centralized and round-the-clock cyber defence support to various NATO sites."[289] Beyond the language in the Summit Declaration and the announcement to launch the Agency, other significant cyber defence policy developments occurred at the 2006 NATO Riga Summit.

3.4.2 NATO Riga Summit, 2006

On November 28 to 29, 2006, the NATO Summit took place in Riga, Latvia. The Alliance agreed to "work to develop a NATO Network Enabled Capability to share information, data, and intelligence reliably, securely and without delay in Alliance operations, while improving the protection of… key information systems against cyber attacks."[290] This initiative represented one of many such endeavours to "increase the capacity… to address contemporary threats and challenges."[291] Related developments included improvements to intelligence sharing with the establishment of the Intelligence Fusion Cell.[292]

---

[288] Jason Healey and Klara Tothova Jordan, "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow" *Atlantic Council Issue Brief,* (Washington, DC, *Atlantic Council*, September 1, 2014): 4, https://www.jstor.org/stable/resrep03426.
[289] NATO, "NATO Cyber Defence Fact Sheet" (Brussels, NATO, July 2016), https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf.
[290] NATO, "Riga Summit Declaration," *NATO*, (Brussels, NATO, November 29, 2006), https://www.nato.int/cps/en/natohq/official_texts_37920.htm.
[291] Ibid.
[292] Ibid.

Figure 3.2 – Kosovo 1999, Summary of Critical Juncture

Critical Juncture 1 (Phase A)	Kosovo 1999
Events	Cyber attacks targeted Allies during NATO's Operation Allied Force operation.
Critical Juncture	Unprecedented cyber attacks demonstrated the value and dangers of these capabilities to Allies.
NATO Policy or Institutional Change	The first cyber language was included in the 2002 Prague Summit Communiqué. The additional cyber language was added at the 2006 Riga Summit.

3.5 – Key Findings from Phase A

Figure 3.4 compiled significant critical juncture and related policy developments from Phase A. Each phase will conclude with a similar chart of listed critical junctures and corresponding policy developments. The Appendix includes a collected list for all four phases. Phase A involved the founding of cyber defence at NATO. The impact of NATO operations in Kosovo in 1999 was a critical juncture leading Allies to formulate a cyber defence policy. The first phase demonstrated cyber capabilities and policy's value, danger, and opportunity. Policymakers implemented these observations to include related language in Summit Declarations at NATO Summits in Prague in 2002 and Riga in 2006. Causal mechanisms are observed based on research participants discussing cyber attacks in Kosovo at this time as an initial wake up call on the dangers of cyber defence. The inclusion of the first cyber language in the Prague Summit Communiqué is an early example to demonstrate this causal process between the external cyber attack, and developed cyber defence policy at relevant summits.

Chapter 4: Advancing NATO Cyber Defence

4.1 – Opening Remarks

In the years following the first critical juncture and cyber attacks experienced during Operation Allied Force in Kosovo in 1999, NATO formulated cyber defence policy developments during Phase A. Related policy developments included the NATO Summit Declarations in Prague in 2002 and Riga in 2006. Phase B began in January 2007 to advance NATO's cyber defence foundations and establish further cyber defence policy advancements after critical junctures in Estonia in 2007, Georgia in 2008, and Iran in 2010.

4.2 – Phase B, January 2007 to December 2013

4.2.1 Cyber Attacks on Estonia, 2007

The removal of a Soviet war memorial in Tallinn, Estonia, led to days of protests and hundreds of people were arrested on April 26, 2007.[293] Numerous cyber attacks targeted Estonian websites on April 27, including the Estonian Presidency, Parliament, all government ministries, major political parties, three of six national news organizations, other prominent media firms, and two of the largest banks.[294] Local websites were "suddenly swamped by tens of thousands of visits," as targeted distributed denial of service attacks overcrowded "the bandwidth for the servers running the sites."[295] NATO sent cyber experts to Estonia to assist with the investigation and incident response. Konstantin Goloskokov, a commissar in the pro-Kremlin

[293] BBC, "Tallinn Tense after Deadly Riots," *BBC,* April 28, 2007, http://news.bbc.co.uk/2/hi/europe/6602171.stm.
[294] Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *The Guardian*, (May 17, 2007), https://www.theguardian.com/world/2007/may/17/topstories3.russia.
[295] Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia."

youth movement in Moldova and Transnistria called Nashi, admitted to organizing the attacks with friends and did not act "under orders or instructions from parties in higher positions."[296]

During the attack, Estonian Defence Minister Jaak Aaviksoo stated that a crucial problem for NATO was that it "does not define cyber attacks as a clear military action… the provisions of Article 5… will not automatically be extended to the attacked country."[297] The cyber attack on Estonia raised questions within NATO about possible response options apart from Article 5, given that the attack had targeted a member state. In an interview for the *Economist*, an unnamed NATO official compared the cyber attack in Estonia to a conventional attack: "If a member state's communication centres [are] attacked with a missile, you call it an act of war. So, what do you call it if the same installation is disabled with a cyber-attack?"[298]

Minister Aaviksoo added that one major challenge surrounding appropriate response measures for NATO was to define "what can be considered… a cyber attack, or what are the rights of member states and the obligations of European Union and NATO in the event such attacks are launched."[299] The appropriate response problem is a significant challenge for classic deterrence by punishment because hybrid scenarios are decided on a case-by-case basis, and NATO has limited clear response measures for these incidents. Alternatively, NATO's toolbox approach involved many potential response options across all domains. Key stakeholders can both determine what is best for the challenge at hand and make these decisions to reach a consensus at the highest levels of the Alliance.

---

[296] Baltic News Service, "Commissar of Nashi Says He Waged Cyber Attack on Estonian Government Sites," *Swiss Baltic Chamber of Commerce in Lithuania*, (October 10, 2007).
[297] Baltic News Service, "Commissar of Nashi Says He Waged Cyber Attack on Estonian Government Sites."
[298] The Economist, "A Cyber-Riot," *The Economist*, (May 10, 2017), https://www.economist.com/europe/2007/05/10/a-cyber-riot.
[299] Arthur Bright, "Estonia Accuses Russia of 'Cyberattack,'" *Christian Science Monitor*, (May 17, 2007), https://www.csmonitor.com/2007/0517/p99s01-duts.html.

Figure 4.1 – Estonia 2007, Summary of Critical Juncture

Critical Juncture 2 (Phase B)	Estonia 2007
Events	Cyber attacks targeted Estonia after the removal of a Soviet-era statue.
Critical Juncture	Unprecedented cyber incidents included website defacements and disruptions, temporarily taking governmental and media webpages offline.
NATO Policy or Institutional Change	Major NATO cyber institutions (CDMA and CCDCOE) were created in 2008 in the years following the cyber attacks in Estonia. This attack emphasized the need for Alliance cyber defence to be beyond NATO's own networks, to support members when requested.

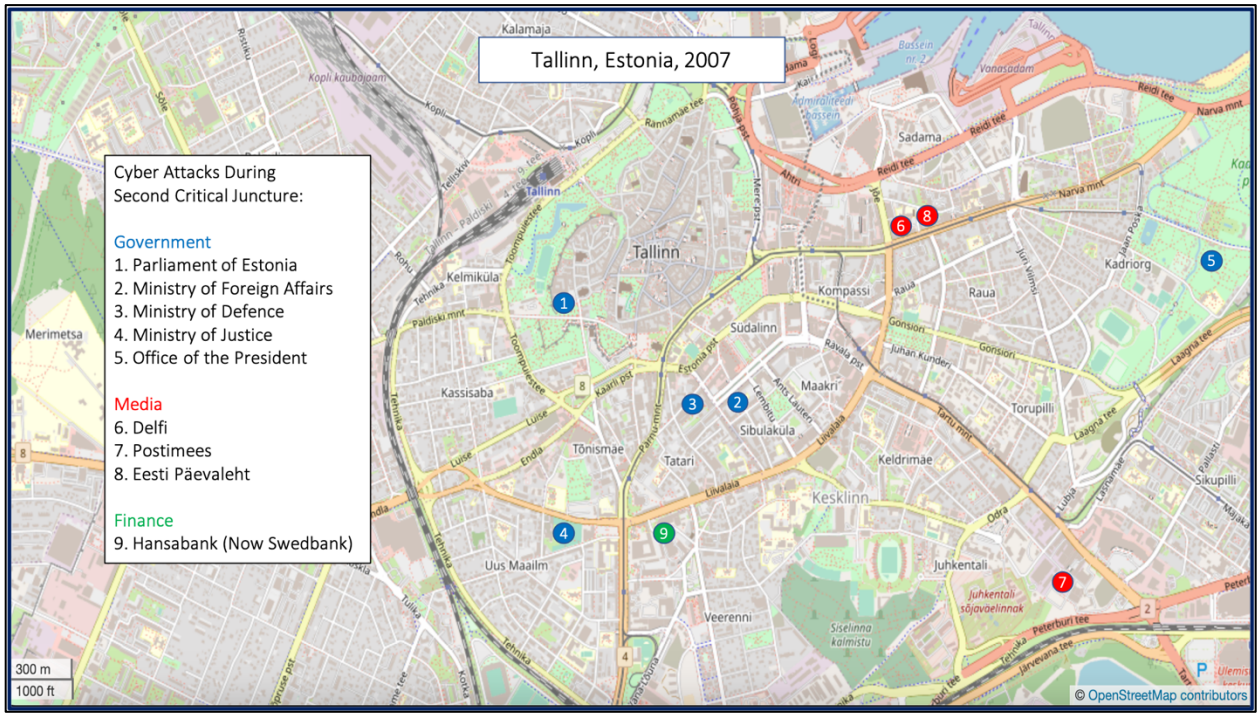
NATO learned from the cyber attacks in Estonia that cyber defence was not solely the security and defence of the networks of Alliance headquarters. Fast response measures were required for cyber defence to extend support to member states to ensure that the cyber security of individual member state networks was the sovereign responsibility of individual Allies. NATO's role in this regard developed to extend a focus to include response, assistance, and support to Allies. NATO developed cyber defence capabilities that extended beyond previously internal-focused approaches to extend support to Allies.[300]

Cyber attacks targeted Estonia in 2007 and are considered the second critical juncture which led to policy development at NATO during the timeline. Policy developments involved a

[300] Myriam D. Cavelty, "Cyber-Allies: Strengths and Weaknesses of NATO's Cyberdefense Posture," *IP Global Edition* 12, no. 3 (February 1, 2012): 15, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1997153.

perspective shift from NATO's primary focus on the cyber security of its networks to support Allies to assist in support of network defence if requested. In an interview for this study, NATO Official 5 described the cyber attacks in Estonia in 2007 as a wake-up call for the Allies.

Figure 4.2 – Cyber Attacks in Tallinn, Estonia 2007



© Ryan J. Atkinson, 2023*

4.2.2 NATO Bucharest Summit, 2008

The NATO Summit in Bucharest, Romania, was held on April 3, 2008, and led to the founding of the first NATO Cyber Defence Policy. The Bucharest Summit Declaration stated that the new Cyber Defence Policy emphasized: "the need for NATO and nations to protect key information systems following their respective responsibilities; share best practices; and provide

a capability to assist Allied nations upon request to counter a cyber attack."[301] The new policy continued to develop "NATO's cyber defence capabilities [to strengthen] the linkages between NATO and national authorities."[302]

NATO continued to face Alliance-wide cyber threats, yet NATO officials acknowledged that cyber defence was primarily the sovereign responsibility of the Allies. NATO primarily "focused on the protection of its networks" before 2007, and the use of cyber capabilities to shut down society "extended" the Alliance's focus to the broader cyber defence of Allies.[303] NATO maintained that Allies were primarily responsible for protecting national networks, and the Alliance provided resource support to assist with resources and capabilities when requested.

The Cyber Defence Management Authority was established in April 2008 to "coordinate cyber defences… and conduct… security risk management" to assist "member states to improve their own national cyber defence capabilities."[304] The initiative facilitated assistance to Allies on cyber defence concerns.[305] During an interview for this study, NATO Official 6 stated that despite NATO's focus on protecting Allied networks beginning in 2008, the ultimate responsibility remained with the Allies to protect their networks and critical infrastructure with NATO in a supportive role.

The NATO Cooperative Cyber Defence Centre of Excellence is the second NATO-affiliated cyber defence institution created following the Bucharest Summit. The Cyber Centre of Excellence, also known as the "CCDCOE," was established in May 2008 in Tallinn, Estonia, to "support… member nations and NATO with unique interdisciplinary expertise in the field of

[301] NATO, "Bucharest Summit Declaration," *NATO*, April 3, 2008, https://www.nato.int/cps/en/natohq/official_texts_8443.htm.
[302] NATO, "Bucharest Summit Declaration."
[303] Cavelty, "Cyber-Allies," 12.
[304] Healey and Bochoven, "NATO's Cyber Capabilities," 4.
[305] Hughes, "NATO and Cyber Defence."

cyber defence research, training, and exercises."[306] The Centre provided training, education, and exercises, like Locked Shields and Crossed Swords. The Centre complemented the work of the Cyber Defence Management Authority and Cyber Incident Response Centre with improved coordination for information sharing. The Centre hosted the International Conference on Cyber Conflict or "CyCon" held annually in Tallinn.

These exercises influenced cyber defence policy to provide meaningful training and education. In an interview for this study, NATO Official 18 noted that exercises incentivized weaker Allies to train and update their cyber defence capabilities to specific standards while working with stronger Allies. The Official noted exercises proved a vital way to facilitate training, improve expertise, and exchange information. The Locked Shields and Crossed Swords exercises hosted by the Cyber Centre of Excellence facilitate social learning amongst NATO staff and personnel. These exercises amounted to social learning which engaged participants and critical stakeholders in exercises to train cyber defence experts.

The development of the annual Cyber Coalition exercise within NATO stresses the institutionalization of cyber defence training and learning through practical application in exercises. The first Cyber Coalition exercise in 2008 operated as NATO's "flagship annual collective cyber defence exercise… one of the largest in the world."[307] The exercise was organized by NATO Allied Command Transformation in Norfolk, Virginia, under the governance of the Military Committee at NATO Headquarters in Brussels, Belgium. The Estonian Cyber Security Exercises and Training Centre in Tallinn facilitated the exercises, which included other relevant NATO entities, Allies, and Partners to "strengthen the Alliance's ability

[306] CCDCOE, "About Us," *CCDCOE,* https://ccdcoe.org/about-us/.
[307] NATO ACT, "Cyber Coalition," https://www.act.nato.int/cyber-coalition.

to deter, defend against, and counter threats in and through cyberspace in support of NATO's core task."[308]

In an interview for this study, NATO Official 6 outlined the significant value of Cyber Coalition and cyber exercises generally to facilitate the work of Allies and partners to test information-sharing tools and other coordination mechanisms. The official spoke about how cyber exercises created simulated networks to train on and provided decision-makers with innovative policy strategies. In another interview for this study, NATO Official 18 supported the sentiment that cyber defence exercises provided immense value to training and strengthening weaker member states.

4.2.3 Cyber Attacks and Russia's Invasion of Georgia, 2008

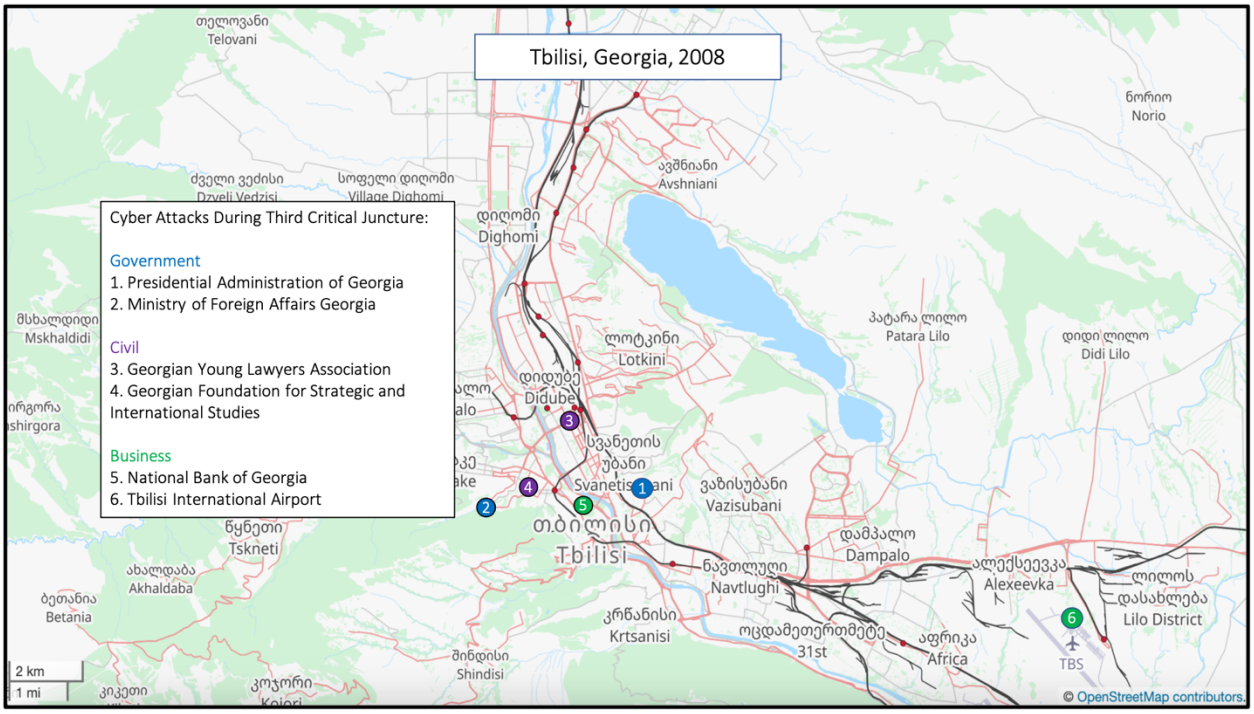
The third critical juncture occurred in August 2008 when unidentified foreign invaders breached Georgian computer networks to disrupt and deface government websites.[309] A series of cyber attacks targeted and disabled the websites of organizations in South Ossetia, Georgia, Russia, and Azerbaijan with distributed denial of service attacks.[310] The case of Georgia 2008 demonstrated how cyber attacks could be used to coordinate military operations.

The "tools" and "commands" used by the attackers were similar to those "used by the [Russian Business Network]," according to Don Jackson, Director of Cyber Threat Intelligence at Security Works, a cyber security firm in the United States. Jackson described the attacks as

[308] Ibid.
[309] David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, (January 6, 2011), https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf.
[310] Travis Wentworth, "How Russia May Have Attacked Georgia's Internet," *Newsweek*, (August 22, 2008), https://www.newsweek.com/how-russia-may-have-attacked-georgias-internet-88111.

"launched from computers [the Russian Business Network] are known to control."[311] In March 2009, researchers concluded that the attack was launched by Russian military intelligence (GRU) and Russian foreign intelligence services (FSB). High-level planning relied "on Nashi [proxy] intermediaries and… crowdsourcing to obfuscate their involvement and implement their strategy."[312] Russian intelligence maintained plausible deniability using proxy intermediaries to distance agencies from specific agents, funding methods, and proxies on the ground.

Figure 4.3 – Cyber Attacks in Tbilisi, Georgia 2008



© Ryan J. Atkinson, 2023*

[311] John Markoff, "Before the Gunfire, Cyberattacks," *The New York Times*, (August 12, 2008), https://www.nytimes.com/2008/08/13/technology/13cyber.html.
[312] John Leyden, "Russian Spy Agencies Linked to Georgian Cyber-Attacks," *The Register*, (March 23, 2009), https://www.theregister.com/2009/03/23/georgia_russia_cyberwar_analysis/.

Cyber attacks in Georgia demonstrated using capabilities coordinated with conventional military operations. Russia used cyber capabilities to shape the battlefield before launching a conventional invasion, demonstrating "the importance of control over the physical infrastructure of cyberspace… and the tendency towards magnifying outcomes in cyber conflicts."[313] The Georgia case is a valuable example of Russian coordination between cyber operations and conventional capabilities. Russia's invasion and war in Ukraine included combined cyber capabilities with conventional operations five months after Russia's February 24, 2022, invasion and before this project's scope ended on June 30, 2022.

Figure 4.4 – Georgia 2008, Summary of Critical Juncture

Critical Juncture 3 (Phase B)	Georgia 2008
Events	Cyber attacks targeted Georgia, which shaped the threat landscape for Russia's conventional invasion in August 2008.
Critical Juncture	Unprecedented coordination between cyber capabilities and conventional forces was observed.
NATO Policy or Institutional Change	Major NATO cyber institutions were created in 2008, around the time of the cyber incidents in Georgia. The NATO Cyber Coalition exercise took place for the first time. At the 2009 Strasburg/Kehl Summit, Allies agreed to strengthen cyber defence collaboration.

[313] Ronald J. Deibert, Rafal Rohozinski, and Masashi Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War," *Security Dialogue* 43, no. 1 (2012): 7.

On April 4, 2009, the NATO Summit in Strasbourg, France and Kehl, Germany, launched the process of developing the new Strategic Concept to be released at the Lisbon Summit in 2010.[314] The Strasbourg/Kehl Summit Declaration outlined initiatives to strengthen further "linkages between NATO and Partner countries on protection against cyber attacks." The initiative developed a "framework for cooperation on cyber defence between NATO and Partner countries." The Summit Declaration expanded the duties of the Cyber Defence Management Authority "to prevent and respond to attacks" to improve "existing" cyber incident response capabilities.[315]

Cyber attacks on Georgia in 2008 influenced NATO to develop relationships for cyber cooperation with partners to strengthen cyber incident response capabilities. In an interview for this study, NATO Official 6 stated that cyber attacks on Georgia in 2008 significantly demonstrated the broader deployment of cyber tools alongside conventional capabilities. In another interview for this study, NATO Official 12 added that cyber attacks in Georgia in 2008 demonstrated to the Allies the growing danger of cyber capabilities.

4.2.4 Cyber Attacks on Iran with Stuxnet, 2010

Stuxnet is a notable precedent-setting cyber weapon demonstrating malicious software's ability to destroy critical physical infrastructure. The virus first infected Iran before spreading globally, beyond the regional focus of the Transatlantic Alliance. However, the cyber attack is considered the fourth critical juncture given that it demonstrated to the Allies for the first time that natural physical destruction could result from malicious computer code.

[314] NATO, "Strasbourg / Kehl Summit Declaration," *NATO*, (April 4, 2009), http://www.nato.int/cps/en/natohq/news_52837.htm.
[315] Ibid.

The malicious computer worm Stuxnet was discovered in the summer of 2010. Development of the worm began in 2005 in joint efforts between the United States and Israel in Operation Olympic Games.[316] During the months before NATO unveiled its Strategic Concept at the Lisbon Summit in 2010, numerous security organizations debated the precedent set by Stuxnet in that computer code had caused physical destruction to critical infrastructure. Stuxnet targeted Supervisory Control and Data Acquisition or SCADA systems to gain access to Programmable Logic Controllers.[317] This technology controlled the machinery for industrial processes, such as the centrifuges used to separate nuclear material. The centrifuges at the Natanz Nuclear Facility were targeted by Stuxnet in 2010, and hundreds were destroyed.[318]

[316] David E. Sanger, "Obama Ordered Wave of Cyberattacks Against Iran," *The New York Times*, (June 1, 2012), https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=1.
[317] David Kushner, "The Real Story of Stuxnet," *IEEE Spectrum* 50, no. 3 (March 2013): 48–53, https://doi.org/10.1109/MSPEC.2013.6471059.
[318] James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival* 53, no. 1 (February 2011): 23–40, https://doi.org/10.1080/00396338.2011.555586.

Figure 4.5 – Iran 2010, Summary of Stuxnet Critical Juncture

Critical Juncture 4 (Phase B)	Stuxnet 2010
Events	Stuxnet is launched on an Iranian nuclear enrichment facility in Natanz.
Critical Juncture	The unprecedented cyber weapon demonstrated malicious software that caused real-world physical destruction to critical infrastructure.
NATO Policy or Institutional Change	At the 2010 Lisbon Summit, NATO agreed on a Strategic Concept, and Stuxnet was a major cyber attack in the threat environment in the months of debates leading up to the Summit. The precedent set by Stuxnet influenced decision-makers to develop policy given the realization of advancements in cyber weapons to cause actual physical destruction.

NATO was in the final months of preparation to launch the Strategic Concept at the Lisbon Summit in 2010 when the discovery of Stuxnet raised essential questions for Allies about how threats in the cyber domain applied to collective defence. In October 2010, one month before the Lisbon Summit, NATO Secretary General Anders Fogh Rasmussen warned that NATO is attacked by hackers "a hundred times a day," adding that "cyber attacks can take down a country's air traffic control system, shut down the banks, paralyze government services and cripple an economy."[319] Similar sentiments over the next few years addressed similar questions about the role of NATO collective defence in cyberspace.

[319] Richard Norton-Taylor, "Strategic Defence Review to Prioritise Cyber Security," *The Guardian*, (October 13, 2010), https://www.theguardian.com/politics/2010/oct/13/strategic-defence-review-cyber-security.

4.2.5 NATO's Lisbon Summit and New Strategic Concept, 2010

The Alliance met for the annual NATO Summit from November 19 to 20 in 2010 in Lisbon, Portugal. The Lisbon Summit Declaration outlined numerous crucial policy perspectives of the Alliance towards security and defence in cyberspace. A new Strategic Concept was adopted, which recognized that cyber challenges were a prominent part of emerging security threats to the Euro-Atlantic. A "cyber dimension" was applied to NATO security doctrine to "detect, assess, prevent, defend and recover" from cyber attacks.[320] Agreements related to enhancing the NATO Incident Response Centre to "full operational capacity" by 2012 to bring "all NATO bodies under centralized cyber protection."[321]

NATO implemented cyber defence policy into defence planning "to promote the development of… capabilities, to assist individual Allies upon request, and to optimize information sharing, collaboration, and interoperability." The declaration tasked the North Atlantic Council to draw "notably on existing international structures and the basis of a review of our current policy, a NATO in-depth cyber defence policy by June 2011… to prepare an action plan for its implementation."[322]

The 2010 Strategic Concept outlined that "cyber attacks" presented a "more frequent" threat that was "more organized and more costly in the damage that they inflict," when a "threshold" is reached to "threaten national and Euro-Atlantic prosperity, security, and stability."[323] The Strategic Concept outlined NATO's capabilities to "prevent, detect, defend

[320] NATO, "Lisbon Summit Declaration," *NATO*, (November 20, 2010), http://www.nato.int/cps/en/natohq/official_texts_68828.htm.
[321] Ibid.
[322] Ibid.
[323] NATO, "2010 Strategic Concept: Active Engagement, Modern Defence," *NATO*, (November 19, 2010), https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf.

against and recover from cyber attacks… using NATO planning processes to enhance and coordinate national cyber defence capabilities, bringing all NATO bodies under centralized cyber protection."[324] The Strategic Concept opened the way for the cyber defence to compound in importance, such that numerous policy developments and investments occurred in the development of NATO cyber defence in the years that followed.

The Lisbon Summit increased the appetite for cyber defence developments at NATO. The cyber-related language in the Summit Declaration and Strategic Concept justified increased policy and investment in cyber defence in 2011. In early 2011, United States Deputy Secretary of Defence, William J. Lynn, was in Brussels to discuss cyber defence with NATO and the European Union to "implement a NATO cyber defence policy and implementation plan with real capabilities."[325] The initiative brought “nations together under this NATO common vision to have them leverage each other’s expertise and experiences,” and draw a collaborative vision “based on the threat to better secure NATO’s networks.”[326]

Part of the publicly stated sentiments from these meetings included strengthened civil-military relations between the private sector and the Alliance. A goal was to provide “complete coverage across military networks with a bridge to civilian networks” to secure “the entire communications infrastructure.”[327] Private industry provided significant partnership requirements given "some 80 to 90 percent… rides on the private infrastructure." Strong civil-military relations fostered cyber defence policy developments and investments and gave the required interoperability.

---

[324] NATO, “2010 Strategic Concept: Active Engagement, Modern Defence.”
[325] Jim Garamore, “Lynn Arrives in Brussels for Cyber Security Talks,” *DVIDS*, (January 23, 2011), https://www.dvidshub.net/news/64060/lynn-arrives-brussels-cyber-security-talks.
[326] Ibid.
[327] Garamore, "Lynn Arrives in Brussels for Cyber Security Talks."

4.2.6 Cyber Attacks and Policy Developments, 2011

NATO's significant policy developments 2011 amounted to a "vision for coordinated efforts in cyber defence throughout the Alliance,… including the new policy, concept, and related action plan."[328] NATO cyber defence policy was included in the NATO Defence Planning Process to "invoke collective defence while maintaining ambiguity about specific thresholds."[329] The 2011 Cyber Defence policy centralized "protection of NATO's networks," and the development of NATO's first cyber defence policy.[330] These policy documents provided Allies with cyber defence language to discuss policy development and investment further.

In May 2011, NATO released a report warning Allies about the threat of "hacktivism." Groups such as Anonymous conducted several distributed denial of service attacks against MasterCard, Visa, PayPal, Amazon, and other companies and terminated services to WikiLeaks on December 6, 2010.[331] The report added that Anonymous was an "ad hoc international group of hackers and activists… [with] thousands of operatives and… no set rules or membership."[332] Anonymous responded to NATO's report, warning to "not make the mistake of believing you can behead a headless snake. If you slice off one head of Hydra, ten more heads will grow in its place. If you cut down one Anon, ten more will join us purely out of anger at your trampling of dissent."[333] During an interview for this study, NATO Official 18 noted that such non-state

[328] Healey and van Bochoven, "NATO's Cyber Capabilities," 13.
[329] Ibid., 13.
[330] NATO, "Defending the Networks: The NATO Policy on Cyber Defence," *NATO*, (2011), https://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf.
[331] Lance Whitney, "Online Activists Fighting to Keep WikiLeaks Alive," *CNET*, (December 6, 2010), https://www.cnet.com/tech/tech-industry/online-activists-fighting-to-keep-wikileaks-alive/.
[332] Ibid.
[333] Ibid.

actors, including Anonymous, posed an immense challenge to the Alliance, and members of Anonymous were arrested in Spain and Türkiye in June 2011.[334]

In March 2011, NATO Defence Ministers discussed a "new NATO Cyber Defence Concept."[335] Defence Ministers agreed upon a related policy in June 2011.[336] The Minister of State for the United Kingdom's Armed Forces, Liam Harvey, acknowledged the initiative to help "set the parameters for NATO's future cyber defence policy."[337] A Memorandum of Understanding was signed on cyber defence to "share information… to sign further bilateral agreements with countries whose capabilities are complementary to our own."[338] The new Cyber Defence Concept paved the "way for the Alliance to step up its defences against growing cyber threats… [on] NATO's own networks as the Alliance's fundamental cyber defence responsibility."[339] Essential features of the concept included cooperation with international organizations and partners for the new concept and formulating an Action Plan for the next Meeting of NATO Defence Ministers in June 2012.[340]

Phase B involved increased interoperability with the private industry. Private firms supported NATO's Incident Response Centre based on agreements with Allies to attain full operational capability.[341] Proposals requested capabilities for information assurance to "about 50

[334] Economist, "An Anonymous Foe," *The Economist*, (June 15, 2011), https://www.economist.com/international/2011/06/16/an-anonymous-foe.
[335] NATO, "NATO Defence Ministers Will Discuss Situation in Libya and Longer Term Prospects in Middle East," *NATO*, (March 7, 2011), http://www.nato.int/cps/en/natohq/news_71277.htm.
[336] NATO, "Cyber Defence: Next Steps," *NATO*, (June 10, 2011), http://www.nato.int/cps/en/natohq/news_75358.htm.
[337] John Leyden, "Defence Talks to Forge EU Cyberwar Strategy," *The Register*, (March 15, 2011), https://www.theregister.com/2011/03/15/cyberwar_defence_talks/.
[338] Ibid.
[339] NATO, "Defence Ministers Approve Cyber Defence Concept and Take next Step in Defence Reform," *NATO*, (March 10, 2011), https://www.nato.int/cps/en/natohq/news_71432.htm.
[340] Ibid.
[341] Defence News, "Firms Team for NATO Cybersecurity Work," *Defence News*, (December 21, 2011).

NATO sites and other installations in 28 countries."[342] On June 8, 2011, Defence Ministers met in Brussels to discuss cyber defence.[343] Allies agreed to revise NATO's cyber defence policy adopted in January 2008 to "develop an action plan to… better defend its populations and systems against cyber threats."[344] The June meeting of NATO Defence Ministers adopted a revised NATO Cyber Defence Policy to bring "all NATO structures… under centralized protection." NATO's Defence Planning Process integrated cyber defence to set "principles on NATO's cyber defence cooperation with partner countries, international organizations, the private sector, and academia."

NATO Deputy Assistant Secretary-General for Emerging Security Challenges Dr. Jamie Shea stated that the new policy enabled "NATO to defend its networks more quickly and efficiently." Shea added that it provided "assistance to Allies and partners in all the three crucial areas of cyber security: prevention, coping with cyber attacks… limiting their impact, and helping countries which are attacked to recover." On June 23, 2011, NATO was targeted by a data breach on "NATO's e-bookshop" that contained no classified data and was operated by an outside company.[345] In early July 2011, a separate cyber incident compromised NATO servers, and hackers posted NATO files online.[346]

Two events in 2010 influenced the increased political will for cyber defence policy developments and investment in 2011. The discovery of Stuxnet in 2010 demonstrated the potential for digital malware to destroy critical physical infrastructure. NATO's 2010 Strategic

[342] Ibid.
[343] NATO, "NATO Defence Ministers Adopt New Cyber Defence Policy," *NATO*, (June 8, 2011), https://www.nato.int/cps/en/natohq/news_75195.htm.
[344] Ibid.
[345] NATO, "Probable Data Breach from a NATO-Related Website," *NATO*, (June 23, 2011), https://www.nato.int/cps/en/natohq/news_75729.htm.
[346] Jeremy Kirk, "Hacking Team Claims NATO Server Compromised," *Computerworld*, (July 6, 2011), https://www.computerworld.com/article/2741641/hacking-team-claims-nato-server-compromised.html.

Concept included language on cyber defence and related policy developments in 2010 and 2011, establishing the "foundations for a self-directed, factual examination of the issue."[347] In September 2011, NATO launched a multinational effort to increase cyber defence investment for a "procurement process" to bring NATO cyber defence capabilities to "full operational capability" by the end of 2012.[348] Ambassador Gabor Iklody, NATO Assistant Security General for Emerging Security Challenges, stated these "new capabilities" operated to "strengthen [NATO's] ability to support Allies in case of cyber attacks."[349]

4.2.7 Institutional Developments

Cyber Defence Management Board

In 2011, the Cyber Defence Management Board replaced NATO's Cyber Defence Management Authority, the cyber defence governance body of the Alliance, to oversee the incident response.[350] The transformation addressed cyber incidents requiring immediate response to provide Allies "coordinated assistance when… victim to a cyber attack."[351] NATO established a cyber defence Memorandum of Understanding between Allies and national cyber authorities. The newly established Cyber Defence Management Board oversaw the Cyber Incident Response Centre. The Defence Policy and Planning Committee oversees the Board, which the North Atlantic Council oversees.[352]

[347] Olaf Theiler, "New Threats: The Cyber-Dimension," *NATO Review*, (September 4, 2011), https://www.nato.int/docu/review/articles/2011/09/04/new-threats-the-cyber-dimension/index.html.
[348] NATO, "NATO Boosts Cyber Defence Investments, Launches Multinational Effort," *NATO*, (September 22, 2011), https://www.nato.int/cps/en/natohq/news_78418.htm.
[349] Ibid.
[350] NATO, "Defending the Networks."
[351] Ibid.
[352] Ibid.

Rapid Reaction Team

NATO outlined Rapid Reaction Teams in March 2012 to operate from the Incident Response Centre by the end of the year. The teams were responsible for the "cyber defence of all NATO sites, whether… static HQs or HQs deployed for operations or exercises."[353] Rapid response teams provided a valuable institutional tool for incident response advisory missions to support Allies. However, further Alliance capabilities were needed to "offer cyber defence assistance to its members," argued Jamie Shea, "to help them guard against these attacks, to detect them, and – once they have happened – to react swiftly to limit the damage." The rapid response teams provided this direct assistance to Allies to enable NATO to develop capabilities based on observations and lessons from critical juncture cyber attacks like Estonia in 2007 and Georgia in 2008. In an interview for this study, NATO Official 6 outlined that a team chosen from a roster of hundreds of experts can be sent at any time. The response teams are made up on a case-by-case basis at the request of one or more Allies.

The rapid response teams were to provide NATO with assistance capabilities following requests by the Allies. However, the North Atlantic Council decided to deploy the rapid response team after deliberating upon the request. A handbook outlining response team procedures and actions was written and developed in the summer of 2012. The document "set out the guidelines for NATO's response to its Allies and partners who required assistance in the protection of their information communication systems."[354] The teams were operational by the end of 2012 and reached total operational capacity by early 2013.

[353] NATO, "NATO Rapid Reaction Team to Fight Cyber Attack," *NATO*, (March 13, 2012), https://www.nato.int/cps/en/natohq/news_85161.htm.
[354] Ibid.

NATO provided Allies with “professional and well-organized assistance to its members and partners.”[355] Response teams maintained access to required “IT and telecommunications equipment… satellite telephones, and equipment for digital evidence collection, cryptography, digital forensic analysis, vulnerability management, network security.”[356] The response teams exercised with other NATO cyber capabilities at the Cyber Coalition exercise in 2012, and by November, had been tested in an "intervention phase" to determine the value of the handbook when applied to particular responses due to incidents.[357]

4.2.8 NATO Chicago Summit, 2012

The Alliance met for its annual Summit in Chicago, Illinois, United States, May 20-21, 2012. Significant policy developments at the Summit involved NATO's commitment to centralizing cyber defence. Allies agreed to provide additional assistance to complete "the necessary reforms to bring all NATO bodies under centralized cyber protection, to… protect our collective investment in NATO."[358] Allies agreed to “integrate cyber defence measures into Alliance structures and procedures.”[359] No further cyber defence commitments were made, but further cyber defence centralization and oversight were developed, including the formation of NATO's Communication and Information Agency.[360]

In late May 2012, Ambassador Gabor Iklody, NATO Assistant Secretary-General for Emerging Security Challenges, spoke at the European Union Cybersecurity and Digital Crimes

[355] Ibid.
[356] Ibid.
[357] Ibid.
[358] NATO, “Chicago Summit Declaration,” *NATO*, (May 20, 2012), https://www.nato.int/cps/en/natohq/official_texts_87593.htm.
[359] Ibid.
[360] NATO, “Men in Black: NATO’s Cybermen,” *NATO*, (April 24, 2015), http://www.nato.int/cps/en/natohq/news_118855.htm.

Forum organized by Microsoft. Iklody identified significant areas for enhanced NATO-European Union cyber defence cooperation to provide training and education on information sharing, network protection, and crisis management.[361] He acknowledged the significant role of private industry in cyberspace, given that 80-85% is "owned and operated by the private sector, and technical solutions come from the private sector."[362]

4.2.9 Cyber Defence Exercises

NATO conducted its annual Crisis Management Exercise from November 12-16, 2012, to practice "Alliance crisis management procedures at the strategic political level… civilian and military staffs in Allied capitals, at NATO Headquarters, and in both Strategic Commands."[363] The 2012 iteration occurred alongside Cyber Coalition to test "Alliance technical and operational cyber defence capabilities."[364] A single fictional scenario was used for both exercises. The joint exercise included NATO International Staff, International Military Staff, Allied Command Transformation, and Allied Command Operations, along with participating partners Austria, Finland, and Sweden; the International Committee of the Red Cross, the Organization for the Prohibition of Chemical Weapons; and representatives of the European Union External Action Service.[365] Cyber Coalition 2012 provided the coordinated means to "test the effectiveness and efficiency of collaborative cyber defence procedures and capabilities."[366]

---

[361] NATO, "Defence Planning Process," *NATO*, (March 31, 2022), https://www.nato.int/cps/en/natohq/topics_49202.htm
[362] Julian Hale, "NATO Official Highlights Areas for EU-NATO Cyber Cooperation," *Defence News*, (May 31, 2012), http://rpdefense.over-blog.com/article-nato-official-highlights-areas-for-eu-nato-cyber-cooperation-106157528.html.
[363] Ibid.
[364] NATO, "NATO Conducts Annual Crisis Management Exercise and Cyber Coalition Exercise," *NATO*, (November 12, 2012), http://www.nato.int/cps/en/natohq/news_91115.htm.
[365] Ibid.
[366] Ibid.

In April 2013, the NATO Cyber Defence Centre of Excellence published the Tallinn Manual, which marked significant early developments in applying non-binding international law to cyberspace operations.[367] The scholarly work examined how international law, specifically humanitarian law, could be applied to cyber conflict. A multinational team of 20 experts worked from 2009 to 2012 to complete the manual. The drafting process included collaboration with organizations, including the International Committee of the Red Cross, Allied Command Transformation, the NATO Coordination Cyber Defence Centre of Excellence, and United States Cyber Command. The Tallinn Manual was peer-reviewed by thirteen international legal specialists. The stand-alone scholarly publication conveyed the viewpoints of its authors as individuals, not as representatives of NATO or any other government organization. The manual demonstrated yet another means for social learning to occur at NATO, based on the research by an affiliated organization to show internalized learning procedures that influenced the application of international law in the cyber domain.[368] Despite not being an official NATO document, the manual is an influential example of facilitated learning, as officials within NATO able to develop their own understanding of international law applied to various threats in the cyber domain.

In May 2013, the Cyber Centre of Excellence hosted its annual "live fire" cyber exercise, Locked Shields, with experts from Allies and partner countries to train to "detect and mitigate the effects of large-scale cyber attacks and to deal with incidents, while collaborating with other teams."[369] The exercise involved "various tools and techniques," according to Nuri Fattah, Senior Security Consultant at NATO Communication and Information Agency and Lead Ethical

[367] NATO, "System/Network Administrators from the Former Yugoslav Republic of Macedonia Train in Cyber Defence," *NATO*, (April 17, 2013), https://www.nato.int/cps/en/natohq/news_99718.htm.
[368] Michael N. Schmitt, "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed," *Harvard Law Journal* 54 (December 2012): 24.
[369] Paul Ames, "NATO's Geek Brigade," *Global Post*, (May 22, 2013), https://theworld.org/stories/2013-05-22/natos-geek-brigade

Hacker at the Incident Response Centre, “to see how [to] best lock down and secure all systems, while still keeping them operational.”[370] NATO signed cooperation agreements with private sector firms to establish a “good relationship between NATO and private companies [and] a win-win scenario.”[371]

On June 4, 2013, NATO hosted Defence Ministers in Brussels on cyber defence to announce capabilities to be fully operational by autumn, to be extended “to all networks owned and operated by the Alliance.”[372] NATO Secretary General Anders Fogh Rasmussen stated, "NATO can support and assist Allies who request its assistance if they are victims of a cyberattack."[373] A report addressed these challenges as a task for the NATO International Staff to complete, with drafts to be deliberated upon by key stakeholders during relevant committee meetings.[374] Defence Ministers requested that NATO conduct its first "in-depth cyber defence review." Future Rapid Response Teams be fully operational by fall 2013 to "respond to requests from allies who come under cyberattack."[375]

In November 2013, NATO Allies agreed to formulate communication nodes within one common cyber defence umbrella to further centralize NATO cyber defence. Allies were challenged by "cyber standards" to determine how to centralize cyber defence capabilities given different standardization among states across the Alliance.[376] NATO's Incident Response Centre

[370] Ibid.
[371] NATO, “White-Hat Hacker Fights Cyber Intrusions on NATO Systems,” *NATO*, (June 3, 2013), https://www.nato.int/cps/en/natohq/news_100992.htm.
[372] NATO, “Defence Ministers Make Progress on Cyber Protection,” *NATO*, (June 4, 2013), http://www.nato.int/cps/en/natohq/news_101143.htm.
[373] Ibid.
[374] Ibid.
[375] World News, “NATO to Set up Rapid Reaction Teams against Cyber Threats,” *Hürriyet Daily News*, (June 5, 2013), https://www.hurriyetdailynews.com/nato-to-set-up-rapid-reaction-teams-against-cyber-threats-48292.
[376] Brooks Tigner, “NATO Cyber Umbrella to Coalesce in November,” *Jane’s Defence Weekly*, (July 17, 2013).

was primarily charged 2011 to centralize all cyber-related structures at NATO and standardize information networks.

Cyber threat actors targeted NATO exercise Steadfast Jazz in 2013. The Alliance observed cyber attacks "against Latvia… from IP addresses in Russia," according to the Information Technology Security Incident Response Institution of Latvia operated by its Ministry of Defence.[377] The threat actors "attempted to post misleading information in Latvian online media websites about NATO, thus attempting to discredit the Alliance as well as the exercises."[378] The exercise was meant for NATO's Response Force - a rapid reaction force with operational components on land, sea, and air - to "deploy anywhere and deal with any threat."[379] Latvia's incident response institution tracked hackers from a fictitious group called "Anonymous Ukraine" and "recorded cyber attacks from IP addresses in ten countries during the military exercise, with many coming from Russia. Part of the attacks came from servers that had already been compromised."[380]

4.3 – Key Findings from Phase B

Key findings from Phase B included critical junctures in Estonia in 2007, Georgia in 2008, and Stuxnet in 2010. The cyber threat environment influenced significant cyber policy developments with the NATO 2010 Strategic Concept and other Summit documents. The occurrence of years of policy development and investment in Alliance cyber capabilities followed precedent-setting critical junctures in the form of cyber-attacks and related incidents.

[377] Baltic Course, "Cyber-Attacks Witnessed during NATO Exercises in Latvia Came from Russian IP Addresses," *Baltic Course*, (February 12, 2014), http://www.baltic-course.com/eng/Technology/://www.baltic-course.com/eng/Technology/?doc=87601&output=d&ins_print.
[378] Ibid.
[379] NATO, "Steadfast Jazz 2013," *NATO*, (December 15, 2015), http://www.nato.int/cps/en/natohq/103267.htm.
[380] Baltic Course "Cyber Attacks Witnessed during NATO Exercises."

Institutional developments within NATO's command structure involved the establishment of the Cyber Defence Management Board to oversee the Cyber Incident Response Centre and the Rapid Response Teams. Phase B concluded with crucial features which remained central in Phase C, including simulated cyber defence policy developments that followed critical junctures and helped the Alliance prepare for cyber attacks during Russia's 2014 annexation of Crimea and war against Ukraine.

The cyber language in the 2010 Strategic Concept resulted from a changed threat landscape that emphasized the importance of threats in cyberspace. The external events of cyber attacks in Kosovo, Estonia, Georgia, and Stuxnet, which resulted in significant critical junctures created the permissive conditions that allowed for significant developments in policy language focused on cyber defence, including within the 2010 Strategic Concept. Chapter 5 delves deeper into the narrative of critical junctures followed by significant policy developments, framed in this dissertation as Phase C. A crucial question raised during Phase B is whether the policy NATO developed in the years following critical junctures can become influential enough to be "internal advancements" which go on to inspire further policy and investment, as depicted in Figure 4.6. The concept of "internal advancement" is used by the Author to describe a significant internal change which then goes on to impact further internal policy developments. Both the 2010 and 2022 Strategic Concepts are considered to be internal advancements. These internal institutional dynamics can lead to policy change, given the permissive conditions that resulted from critical junctures caused by significant external events.

Figure 4.6 – NATO 2010 Strategic Concept, Summary of Internal Advancement

Internal Advancement (Phase B)	NATO 2010 Strategic Concept
Events	The Alliance agreed to a new Strategic Concept at the Lisbon Summit.
Internal Advancement	The document included language for the first time on cyber security and related threats.
NATO Policy or Institutional Change	Cyber-related language in the Strategic Concept and Summit Documents signalled that NATO acknowledged its interests in cyber space to develop defensive capabilities accordingly.

Chapter 5: Enhancing NATO Cyber Defence

5.1 – Opening Remarks

During Phase B, NATO advanced its cyber defence policy to support Allies with institutional entities like cyber defence rapid reaction teams. Cyber attacks in Estonia in 2007, Georgia in 2008, and Stuxnet in 2010 amounted to critical junctures. In the following years, NATO documents included related language to provide a strong foundation for further policy developments, like the 2010 Strategic Concept and Lisbon Summit Communiqué. Russia's annexation of Crimea demonstrated to NATO that there remained a need for quick multi-domain response measures, which led NATO to develop the 2014 Enhanced Cyber Defence Policy.

5.2 – Phase C, January 2014 to December 2017

5.2.1 Crimea, Geopolitics, and the Black Sea Region

The Black Sea Region included numerous naval ports to project state power, protect interests, and maintain a presence in a highly strategic geopolitical region. Figure 5.1 details numerous key naval ports in the Black Sea in yellow and two ports specifically relevant to the fifth critical juncture: Russia's annexation of Crimea. Russia's Black Sea Fleet Naval Port at Sevastopol, Crimea, is marked by a red circle. The former location of Ukraine's Southern Naval Base is marked by a blue circle in the town of Novoozernoe, which Russian forces captured on March 27, 2014.[381] Russia's presence in the Black Sea at Sevastopol provided immense strategic value to maintain a presence in the region.[382] The 1936 Montreux Convention limited Russia's

[381] Aleksandar Vasovic, "Russian Troops Seize Ukraine Marine Base In Crimea," *Business Insider*, (March 23, 2014), https://www.businessinsider.com/r-russian-troops-seize-ukraine-marine-base-in-crimea-soldiers-2014-24.
[382] Paul Stronski, "What Is Russia Doing in the Black Sea?" *Carnegie Endowment for International Peace*, (May 20, 2021), https://carnegieendowment.org/2021/05/20/what-is-russia-doing-in-black-sea-pub-84549.

military maneuverability through the Dardanelles and Bosporus channels controlled by Türkiye.[383] Coastal countries Bulgaria, Georgia, Romania, Türkiye, and Ukraine can send submarines through the channels. Türkiye can prohibit the use of the passage when a Black Sea country is at war.[384] As Figure 5.1 illustrates, Russia maintains a strong presence with its Black Sea Fleet at Sevastopol, given limitations on transport to access the Mediterranean for military and economic incentives.

Figure 5.1 – Black Sea Regional Map

© Ryan J. Atkinson, 2023

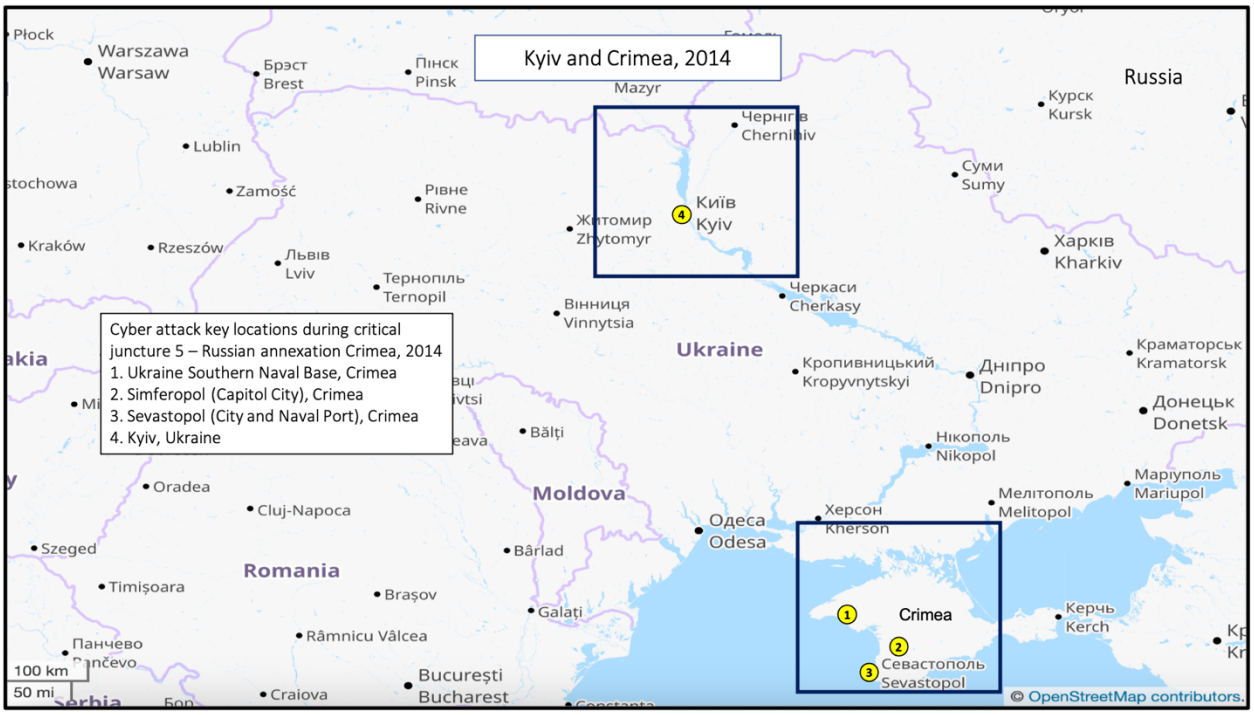
[383] The Economist, "Why the Black Sea Matters to Russia," *The Economist*, (May 6, 2022), https://www.economist.com/the-economist-explains/2022/05/06/why-the-black-sea-matters-to-russia.
[384] Adam Aliano Spivak Russell, "Ukraine Symposium - The Montreux Convention and Turkey's Impact on Black Sea Operations," *Lieber Institute West Point*, (April 25, 2022), https://lieber.westpoint.edu/montreux-convention-turkeys-impact-black-sea-operations/.

5.2.2 Cyber Attacks During Russia's Annexation of Crimea, 2014

NATO took significant steps to strengthen its cyber defence capabilities following cyber attacks during Russia's 2014 annexation of Crimea. Russia mobilized 150,000 troops under the guise of a military exercise in February 2014. Unmarked special forces occupied critical strategic locations in Crimea as Russia invaded Crimea to annex the peninsula from Ukraine. The annexation provided an illustrative case of precedent-setting cyber incidents as the next critical juncture, and the NATO cyber defence policy developed accordingly in the following years.[385] Figure 5.2 illustrates Cyber Attacks in Kyiv and Crimea using a regional map that locates key cyber attack locations and critical juncture 5.

[385] BBC, "Ukraine: Gunmen Seize Crimea Government Buildings," *BBC News*, (February 27, 2014), https://www.bbc.com/news/world-europe-26364891.

Figure 5.2 – Cyber Attacks in Kyiv and Crimea Regional Map



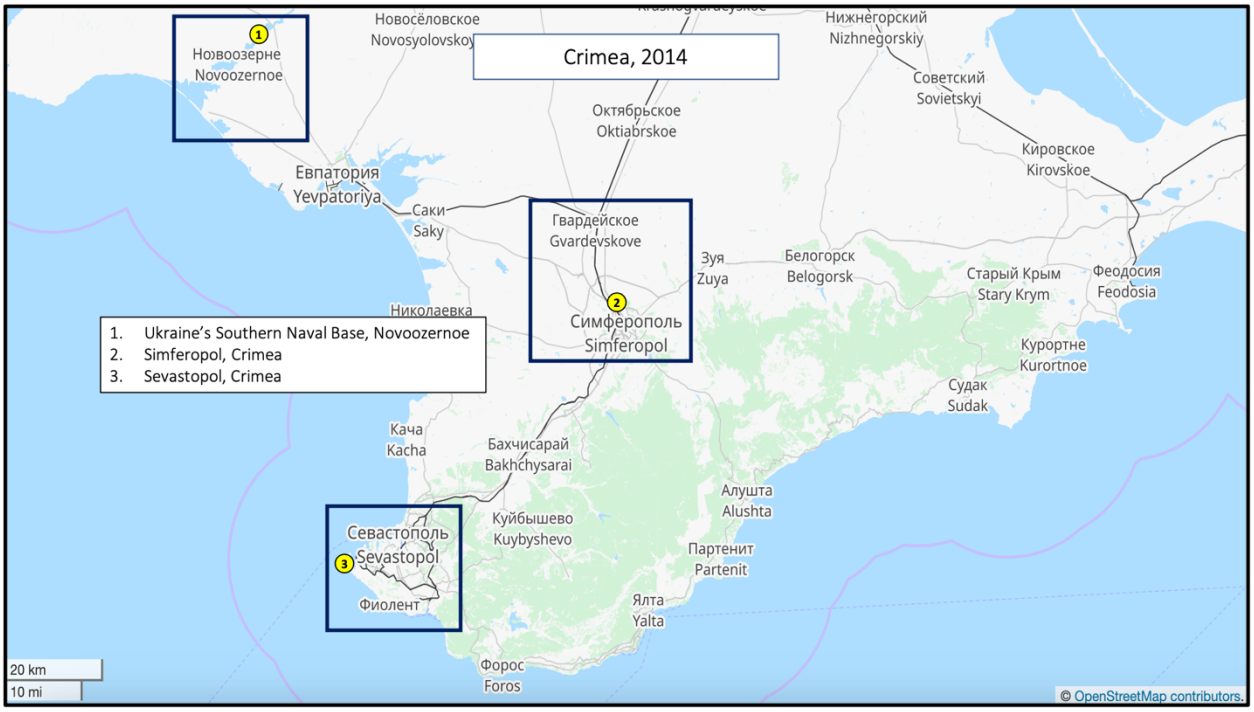
© Ryan J. Atkinson, 2023

On February 28, 2014, Russia targeted Ukraine's state-owned telecommunications service, Ukrtelecom, which reported: "Several of its offices in Crimea had been seized by unidentified intruders who cut telephone internet cables, temporarily disrupting… communications between [Crimea] and Ukraine."[386] On March 2, 2014, Russian units were reported to have cut power lines and services to Ukraine's Navy Headquarters in Sevastopol.[387] Ukraine's UNIAN news agency reported that "Russian units forced entry into other Ukrainian Naval Forces Communications facilities and sabotaged communications lines in a similar vein to

[386] Robin Hughes, "Ukraine Braces for Cyber Offensive," *International Defence Review*, (March 5, 2014).
[387] Ibid.

the attack on Ukrtelecom."[388] All these developments are illustrated in Figure 5.3, Crimean Peninsula Key Locations.

Figure 5.3 – Crimean Peninsula Key Locations



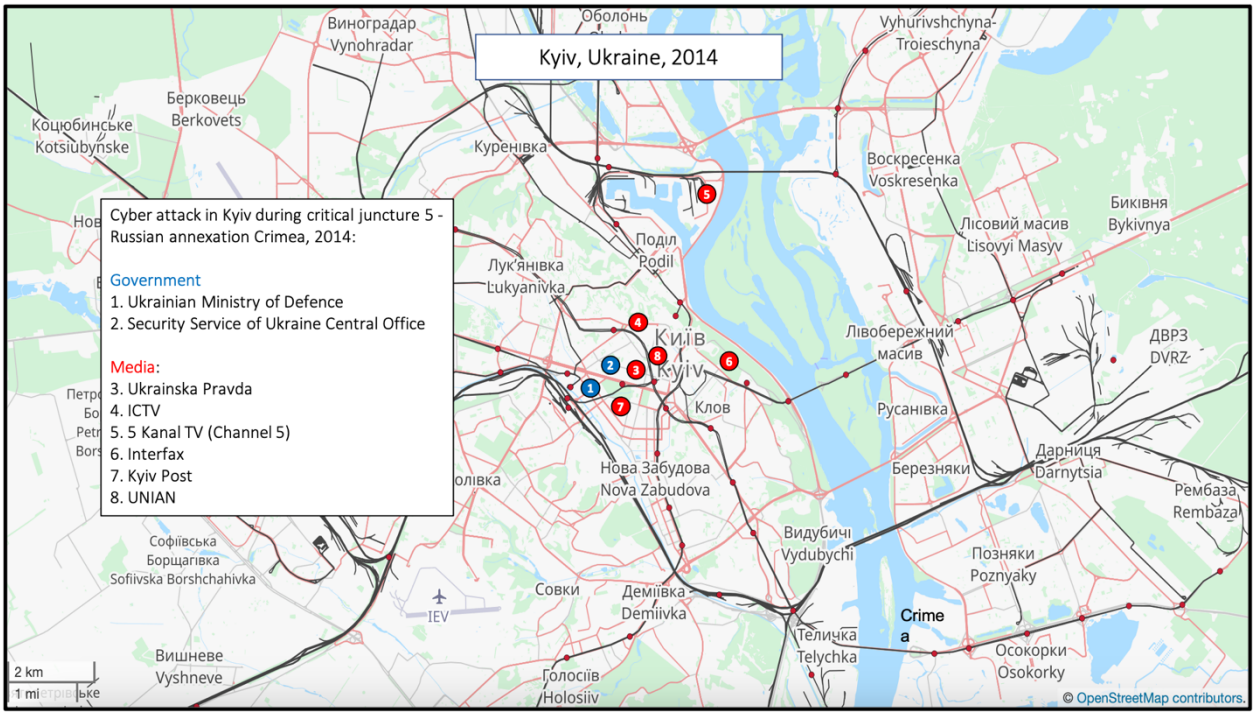
© Ryan J. Atkinson, 2023

On March 15, 2014, the hacker group Cyber Berkut claimed responsibility for an attack that took down the websites of NATO's Headquarters, NATO's Cooperative Cyber Defence Centre of Excellence, and the NATO Parliamentary Assembly.[389] Cyber Berkut publicly stated they targeted NATO for supporting Ukraine and warned the "Kyiv Junta… we will not allow the presence of NATO in our homeland."[390] NATO spokeswoman Oana Lungescu said that "a significant [distributed denial of service] attack" targeted NATO but had "no operational

[388] Ibid.
[389] Ibid.
[390] ABC News, "Ukrainian Hackers Claim NATO Cyber Attack," *ABC News*, (March 16, 2014), https://www.abc.net.au/news/2014-03-16/nato-websites-targeted-in-attack-claimed-by-ukrainian-hackers/5324362.

impact."[391] See Figure 5.4 – Cyber Attacks in Kyiv, Ukraine, for an illustration of critical juncture 5.

Figure 5.4 – Cyber Attacks in Kyiv, Ukraine



© Ryan J. Atkinson, 2023

The United Kingdom's National Cyber Security Centre later published a report in October 2018 identifying Cyber Berkut as affiliated with Russian military intelligence, the GRU.[392] On March 16, 2014, a referendum declared Crimea an autonomous republic.[393] Figure 5.5 illustrates subsequent Cyber Attacks on Energy Companies in Ukraine.

[391] Ibid.
[392] UK NCSC, "Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed," *United Kingdom Nation Cyber Security Centre*, (October 3, 2018), https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed.
[393] Ilya Somin, "Russian Government Agency Reveals Fraudulent Nature of the Crimean Referendum Results," *The Washington Post*, (May 6, 2014), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/05/06/russian-government-agency-reveals-fraudulent-nature-of-the-crimean-referendum-results/.

Figure 5.5 – Cyber Attacks on Energy Companies in Ukraine

© Ryan J. Atkinson, 2023

On May 29, 2014, a report published by cyber security firm FireEye provided further examples of Russia's use of cyber capabilities during the annexation of Crimea in 2014. The report tracked over 30 million "callbacks," or messages sent from computers infected with malware to grant threat actors remote access.[394] The report noted that in March 2014, callbacks to computers in Russia "jumped by 40 percent, giving it the fourth most [callbacks] in the entire world."[395] The report noted "a jump in the number of types of malware… a sign that both nations were flexing their digital muscles as tensions increased."[396] Taken altogether, the evidence of

[394] Russell Brandom, "Cyberattacks Spiked as Russia Annexed Crimea," *The Verge*, (May 29, 2014), https://www.theverge.com/2014/5/29/5759138/malware-activity-spiked-as-russia-annexed-crimea.
[395] Ibid.
[396] Ibid.

many cyber attacks against Crimea in 2014 demonstrates another critical juncture which corresponded with NATO cyber defence policy developments in the years that followed.

Russia's annexation of Crimea set a precedent for NATO to attain more strategic objectives through combined forces across several focus areas: military, political, social, informational, and economic. More advanced technology and increased resources supported NATO's combined forces and capabilities. Russian operations in Crimea had used "cyber forces as part of their conventional ground force intervention," according to Commodore Bruce Wynn (Retired), Former Director of Communications and Information Systems and Chief Technology Officer of Cyber for the United Kingdom Royal Air Force.[397] Russia's use of malicious cyber capabilities shaped the pre-conflict environment in Crimea in 2014, as it did in Georgia in 2008. Russian conventional operations in Crimea in 2014 increasingly combined conventional and non-conventional forces with cyber components. Figure 5.6 summarizes the impact of Critical Juncture 6.

[397] Robin Hughes, "Ukraine Braces for Cyber Offensive," *International Defence Review*, (March 5, 2014).

Figure 5.6 – Crimea 2014, Summary of Critical Juncture 6

Critical Juncture 6 (Phase C)	Crimea, 2014
Events	Russia's annexation of Crimea involved significant cyber incidents and hybrid threats.
Critical Juncture	Unprecedented events involved cyber capabilities and other unconventional tactics that attained strategic objectives. In addition, this demonstrated to Allies a weakness to respond to "hybrid threats" or those that operated below deterrence thresholds to justify a conventional military response.
NATO Policy or Institutional Change	Policy changes at the 2014 NATO Wales Summit, where cyber-attacks became part of Article 5. Further changes at the 2016 Warsaw Summit included the formation of the NATO Enhanced Forward Presence.

5.2.3 Policy Debates, Summer 2014

NATO as a Platform

NATO as a platform for information exchange and intelligence sharing was top of mind during the summer of 2014. Representatives of Allies acknowledged the need at the upcoming Summit "to improve our intelligence collaboration so we have better situational awareness," according to Adam Thomson, United Kingdom Permanent Representative to NATO.[398] Thomson added that such an approach provided the means to "share best practices about dealing with… [a] sophisticated propaganda machine… closely meshed to the Russian military, political, and

[398] Sam Jones, "NATO Leaders Plot Cyber Fightback," *Financial Times*, July 13, 2014, https://www.ft.com/content/0208cd24-0aa0-11e4-be06-00144feabdc0.

economic activity."[399] NATO facilitated intelligence collaboration to increase the speed of decision-making provided by an increased measure of constant discussion in the cyber domain. This challenged the North Atlantic Council as it had to make faster decisions.

Article 5

Allies discussed collective defence measures related to the cyber domain before NATO's Wales Summit in August 2014. NATO Secretary General Jens Stoltenberg stated "that cyber defence is part of collective defence... cyber attacks can be as dangerous as conventional attacks. They can shut down important infrastructure. They can have a great negative impact on our operations."[400] Russia's war in Ukraine demonstrated NATO needed to "replace strategic ambiguity with clarity" about how collective defence "plays out in the face of cyber threats," according to Jarno Limnell, Director of Cyber Security at McAfee.[401] Limnell argued that NATO needed appropriate measures which clearly outlined response options triggered by specific attacks. He pointed out that no explicit cyber-related threshold was outlined to invoke Article 5, given that "member states cannot have full confidence in collective cyber defence… when there are no precedents and… problems of attribution."[402]

Irrespective of concerns that NATO remained overly ambiguous on the threshold for when a cyber-attack would trigger Article 5, the prevailing sentiment failed to understand response measures which are "on a case-by-case basis… purposefully ambiguous," said Karla

[399] Jones, "NATO Leaders Plot Cyber Fightback."
[400] CCDCOE, "Secretary General Stoltenberg: Cyber Is Part of NATO Collective Defence," *CCDCOE*, (September 2014), https://ccdcoe.org/news/2014/secretary-general-stoltenberg-cyber-is-part-of-nato-collective-defence/.
[401] ICDS, "Increasing NATO's Role in Cyber Defence," *ICDS*, (August 28, 2014), https://icds.ee/en/increasing-natos-role-in-cyber-defence/.
[402] Jarno Limnell, "NATO's September Summit Must Confront Cyber Threats," *Breaking Defense*, (August 11, 2014), https://breakingdefense.sites.breakingmedia.com/2014/08/natos-september-summit-must-confront-cyber-threats/.

Tothova-Jordan, Cyber Warfare Specialist at the Atlantic Council's Centre for International Security.[403] Specific countermeasures are always a "political decision," given the dangers of publicly stating NATO's response options, added Tothova-Jordan. If NATO specifically outlined "a clear threshold," then competitors would be able "to calibrate their attacks to inflict just enough damage to avoid retaliation... and play just below the threshold."[404]

NATO Deputy Assistant Secretary-General for Emerging Security Challenges Jamie Shea spoke in 2014 about that case-by-case assessment of cyber attacks, which "established a principle that a certain level of intensity of damage, malicious intention… could be treated as the equivalent of an armed attack."[405] Shea mentions specifically how, in the cases of Georgia and Ukraine, there is a "rather big and ongoing cyber dimension which showed that a lot of sophisticated methods and techniques are being employed."[406] Shea concluded: "it is certainly meant as a deterrent. It is not meant to be escalatory, but a signal that NATO is not defending itself only in 20th-century terms."[407]

The danger remains of escalation from cyber attacks being incorporated as part of NATO's collective defence. For a deterrent to work, it requires a credible threat response, warns Thomas Rid, Professor of Cyber Security Studies at Johns Hopkins University. When response measures are not made clear, it can lead competitors to question the credibility of the deterrent.[408] Rid adds that most cyber incidents are not strictly the high-level attacks that are the

[403] Global News, "NATO Plans Response to Cyberattacks," *Global News*, (September 2, 2014), https://globalnews.ca/news/1539145/nato-plans-response-to-cyberattacks/.
[404] Ibid.
[405] Steve Ranger, "NATO Updates Cyber Defence Policy as Digital Attacks Become a Standard Part of Conflict," *ZDNET*, (June 30, 2014), https://www.zdnet.com/article/nato-updates-cyber-defence-policy-as-digital-attacks-become-a-standard-part-of-conflict/.
[406] Ibid.
[407] Ibid.
[408] Thomas Rid, "Escalation, Not Deterrence," *Medium*, (July 2, 2014), https://medium.com/@ridt/escalation-not-deterrence-f0ddf055d4c7.

focus of language in the NATO Wales Summit Declaration. Instead, most cyber incidents include malicious cyber activities and cyber espionage below the threshold of conventional warfare. Ambassador Sorin Ducaru, NATO's Assistant Secretary-General for Emerging Security Challenges, added that there is no "predetermined threshold [no] red line" to trigger Article 5 in response to a cyber attack."[409] NATO provided Allies with assistance based on what was "deemed necessary, including the use of armed force," added Ducaru.[410]

Article 5 has only ever been invoked once in NATO's history after the terrorist attacks on September 11, 2001, which demonstrates that decisions can be made on a case-by-case basis involving previously unprecedented circumstances unforeseen by the drafters of the North Atlantic Treaty in 1949. Ducaru added that "Article 5 was never designed to be triggered by a certain threshold" and was instead designed to be flexible to adapt to scenarios that "the founding partners had never contemplated," as the example of the September 11 terrorist attacks demonstrates.[411] Similarly, cyber-attacks are likely another threat the North Atlantic Treaty drafters never contemplated.

Attribution Problem

The attribution problem complicates NATO decision-making, given that 31 Allies must agree on threat actors responsible for the attack among various state and non-state actors. According to Dave Merkel, Chief Technology Officer of cyber security firm FireEye, a major challenge for NATO is the "wide proliferation of [cyber] warfare," according to Dave Merkel,

[409] Sydney J. Freedberg, "NATO Hews To Strategic Ambiguity On Cyber Deterrence," *Breaking Defense*, (November 7, 2014), https://breakingdefense.com/2014/11/natos-hews-to-strategic-ambiguity-on-cyber-deterrence/.
[410] Freedberg, "NATO Hews To Strategic Ambiguity On Cyber Deterrence."
[411] Ibid.

Chief Technology Officer of cyber security firm FireEye.[412] Hackers "launch hundreds of varied attacks in a short time," Merkel adds, and "governments may find it nearly impossible to identify, attribute and respond… in a timely manner."[413] The diversity of threat actors increasingly involves an interconnected threat landscape of state and non-state actors.

The North Atlantic Council released many statements in recent years to respond to attacks that targeted Europe and North America in the spring of 2021. On April 15, 2021, the North Atlantic Council released a statement which followed a statement by the United States that identified Russia as responsible for the SolarWinds hack in 2020.[414] On July 19, 2021, the North Atlantic Council made a statement to stand with those affected by the Microsoft Exchange Server compromise attributed to China.[415] These statements demonstrated unity within the Alliance to agree to attribute threat actors and publicly state opposition and condemnation for the action.

5.2.4 NATO Wales Summit, September 2014

On September 5, 2014, the NATO Summit was held in Wales. Various paragraphs of the Wales Summit Declaration outlined significant developments to address cyber defence and hybrid challenges. Russia's annexation of Crimea remained a foremost concern for Alliance members. Paragraph 13 required NATO to possess "the necessary tools and procedures… to deter and respond effectively to hybrid warfare threats, and the capabilities to reinforce national

[412] Everett Rosenfeld, "NATO Rattles Cybersabers: but Experts Have Doubts," *CNBC*, (September 9, 2014), https://www.cnbc.com/2014/09/09/nato-cyberdefense-a-military-response-to-virtual-warfare.html.
[413] Ibid.
[414] NATO, "North Atlantic Council Statement Following the Announcement by the United States of Actions with Regard to Russia," *NATO*, (April 15, 2021), https://www.nato.int/cps/en/natohq/official_texts_183168.htm.
[415] NATO, "Statement by the North Atlantic Council in Solidarity with Those Affected by Recent Malicious Cyber Activities Including the Microsoft Exchange Server Compromise," *NATO*, (July 19, 2021), https://www.nato.int/cps/en/natohq/news_185863.htm.

forces."[416] The toolbox approach allowed policymakers to adapt response measures to specific hybrid challenges and cyber threats. Paragraph 13 outlined the tools that were part of the approach, which included "enhancing strategic communications, developing exercise scenarios [of] hybrid threats, and strengthening coordination between NATO and other organizations." NATO coordinated exercises and engagements with affiliated entities and research institutions.

In 2014, NATO established the Strategic Communications Centre of Excellence in Riga, Latvia. The new Centre of Excellence marked the newest addition to institutional centres focused on hybrid countermeasures. The NATO Cooperative Cyber Defence Centre of Excellence was established in 2008, and the Strategic Communications Centre of Excellence was established in 2014. The Hybrid Threat Centre of Excellence was established in 2017 Helsinki, Finland. The Wales Summit Declaration included two paragraphs on cyber defence. Paragraph 72 outlined the new Enhanced Cyber Defence Policy, acknowledging that "cyber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability."[417] Paragraph 73 added that NATO enhanced its "cyber security of national networks upon which NATO depends for its core tasks… to integrate cyber defence into NATO operations and operational and contingency planning."[418] NATO's new cyber defence policy included language incorporating cyber attacks as part of collective defence, supported by member-state sovereign network defence and cyber operations. The approach resolves challenges involved in ongoing processes through processes of "puzzling," which establish ongoing learning processes within the policy development process.

---

[416] NATO, "Wales Summit Declaration," *NATO*, (September 5, 2014), https://www.nato.int/cps/en/natohq/official_texts_112964.htm.
[417] Ibid.
[418] Ibid.

Dr. Jamie Shea spoke at the Wales Summit of the value of NATO as a platform to facilitate a "significant amount of bilateral assistance between NATO and Allies to function as a platform for connection," to maintain "lists of national cyber security specialists who can be mobilized at short notice."[419] Dr. Shea discussed the opportunity for the platform approach to connecting less cyber-mature partners with more cyber-mature partners "to develop an intimate understanding of each other's procedures and work together to deal with threats."[420] The new enhanced cyber defence policy strengthened NATO as a platform and facilitated bilateral connections among Allies for rapid incident response support options.

The Wales Summit Declaration outlined the Industry Cyber Partnership to structure NATO's work with industry. The partnership aimed to "improve cyber security in NATO's defence supply chain, raise mutual understanding and awareness of cyber threats and risks,… information sharing,… [and] help NATO allies to learn from industry." The initiative launched on September 17, 2014, at the NATO Information Assurance Symposium in Mons, Belgium.[421] The industry partnership supported member states in developing bilateral and multilateral relationships, demonstrating that NATO is a platform in action with other Allies and non-state industry partners.

5.2.5 NATO Cyber Capability Development and Exercises

On November 14, 2014, NATO held the annual cyber defence exercise Cyber Coalition for three days. The exercise tested "systems to make sure… NATO keeps pace with the evolving

[419] Jamie Shea, "NATO to Unveil Cyber-Defence Strategy Fit for Changing Times," *The Conversation*, (September 4, 2014), http://theconversation.com/nato-to-unveil-cyber-defence-strategy-fit-for-changing-times-31143.
[420] Ibid.
[421] NCIA, "NATO Launches Industry Cyber Partnership," *NCIA*, (September 18, 2014), https://www.ncia.nato.int/about-us/newsroom/nato-launches-industry-cyber-partnership.html.

threat," said Sorin Ducaru.[422] Cyber Coalition allowed Allies to test the application of the new cyber defence policy passed at the Wales Summit.[423] The cyber Rapid Reaction Teams were exercised outside of Estonia's cyber range. During the exercise, the six-person team deployed to "assist" Allies to respond and recover from cyber-attacks and "provide technical assistance or respond to incidents arising from a cyber attack."[424] The response team was deployed to Athens, Greece, to demonstrate it could "be on site on short notice to diagnose cyber security issues and swiftly restore operational capability."[425]

The team acts "on concise notice to deal with an attack," according to Jean-François Agneessens, Cyber Security Expert with the NATO Communication and Information Agency.[426] Team specialists include professionals from cyber security auditing, penetration testing, and network forensics to operate out of the NATO Cyber Operations Centre in Mons, Belgium. The central value of these teams "constitute a strategic core capability," according to Suleyman Anil, Head of Cyber Defence at NATO. Anil added that the teams are "reinforced, as needed, by experts from nations when NATO is responding to an assistance request from a nation."[427]

The Locked Shields exercise was hosted by the Cyber Centre of Excellence in Tallinn, Estonia, on April 22-23, 2015. The Rapid Response Team trained with 15 other cyber experts to participate in the 2-day event, where teams exercised to deploy "to a fictitious [Alliance member] under cyber attack... to restore the primary drone control facility [and] help secure the auxiliary control system which can take command of the military drones."[428] The exercise included

[422] NATO, "Largest Ever NATO Cyber Defence Exercise Gets Underway," *NATO*, (November 18, 2014), https://www.nato.int/cps/en/natohq/news_114902.htm.
[423] Ibid.
[424] NATO, "Men in Black: NATO's Cybermen."
[425] NCIA, "Exercise Cyber Coalition 2014."
[426] Ibid.
[427] Ibid.
[428] Ibid.

"realistic technologies and existing networks and attack methods" to demonstrate a simulated cyber security exercise which involved multi-domain operations.[429]

The exercises provided focused training on real-world scenarios against strategies threat actors used to develop countermeasures. The exercise included themes focused on "threats you might see from Russia," said Robert Pritchard, Associated Fellow in Cyber Security at the United Kingdom Royal United Service Institute.[430] The NATO Rapid Response Team capability was exercised at Locked Shields in 2014. It demonstrated the fast-growing influence that the Cyber Centre of Excellence already exerted on policy, based on practical approaches to facilitate training and exercises.

In July, 2015, the NATO Science for Peace and Security program supported a cyber defence capacity-building workshop designed to increase cooperation between Allies and partners in the Caucuses and Black Sea region.[431] The workshop took place in Tbilisi, Georgia and involved other cyber experts and government representatives from Armenia, Azerbaijan, Georgia, Hungary, the Republic of Moldova, Poland, Romania, Türkiye, and Ukraine. Representatives from international organizations attended, including the International Telecommunications Union and the European External Action Service, among other partners in industry, academia, and civil society.[432] The Science for Peace and Security Program demonstrated the value of cyber defence capacity-building initiatives, which developed from the language included in various NATO Summit Declarations.

---

[429] Ibid.
[430] Makortoff, "NATO Cyber War Drills to Focus on Russia: Expert."
[431] Ibid.
[432] NATO, "Enhanced Cyber Defence Cooperation in the South Caucasus and Black Sea Region," *NATO*, (July 29, 2015), https://www.nato.int/cps/en/natohq/news_121969.htm.

Cyber capacity building facilitated the close cooperation between regional partners, which provided practical value through engagement, such as intelligence sharing among Allies. Cyber attacks stemmed "from common sources and shared many of the same characteristics, including method of attack," according to Michael Gaul, Senior Advisor on Projects and Strategy with NATO's Emerging Security Challenges Division."[433] Cyber capacity building workshops facilitated the communication channels, which increased dialogue to "provide the opportunity to collaborate on a common technical, legal, regulatory, and interoperability framework in cyber defence." The added value of the workshop's regional focus allowed tailored development strategies for workshop materials to be region-specific, given geopolitical trends to foster further collaboration between Allies and partners.

On September 15, 2015, the NATO Cyber Incident Response Centre expanded its response capabilities to invest €18.9 million over two years to reach full operational capability.[434] The centre was granted additional capabilities to better monitor "NATO's internal networks… for cyber incidents… and respond to them when necessary."[435] The centre is based at Supreme Headquarters Allied Powers Europe, or SHAPE, in Mons, Belgium, and is "responsible for protecting NATO's 35 critical networks and over 50 NATO sites."[436] This was yet another example of NATO outsourcing cyber capability developments to industry to help its learning centres reach total operational cyber capacity on an efficient timeline.

[433] Ibid.
[434] Ibid.
[435] Nicholas de Larrinaga, "NATO Extends Cyber Defences," *Jane's Defence Weekly*, (September 15, 2015).
[436] Ibid.

Cyber Attacks on Ukraine and NATO-EU Policy Response

On December 23, 2015, the BlackEnergy malware targeted Ukraine, intentionally causing massive hours-long electrical power outages for 225,000 Ukrainians.[437] Reports in early January 2016 by cyber security firms ESET and iSight linked the attack to the Russian advanced persistent threat group Sandworm.[438] The group is allegedly Unit 74455 of Russia's military intelligence service, the GRU.[439] Malware gained access to launch a distributed denial of service attack to target phone lines that obstructed "emergency responses and prolonged the impact of the attack," said Michael Assante, CEO of the SANS Institute.[440]

On January 16, 2016, a second wave of cyber attacks was reported by Ukrainian media. The wave of attacks targeted public utilities such as Boryspil International Airport in Kyiv.[441] The European Union took immediate legislative action to protect critical national infrastructure, and the Parliament Internal Market and Consumer Protection Committee approved legislation to form the Network and Information Security Directive passed into law in April 2016. The European Union member states had "21 months to transfer the directive into national law and six further months to identify companies subject to it."[442] The bill outlined the requirements that member states must meet, critical national infrastructure obliged by "public and private companies to reinforce networks against cyber attacks and to report breaches."[443] Cyber attacks

[437] Reuters, "US Firm Blames Russian 'Sandworm' Hackers for Ukraine Outage," *Reuters*, (January 8, 2016), https://www.reuters.com/article/us-ukraine-cybersecurity-sandworm-idUSKBN0UM00N20160108.
[438] Lora Chakarova, "EU-NATO Design Response to Cyber-Attacks," *Jane's Intelligence Review*, (March 2, 2016).
[439] Andy Greenberg, *Sandworm* (New York: Penguin Random House, 2019).
[440] Chakarova, "EU and NATO Design Response to Cyber-Attacks."
[441] Euractiv, "Ukraine Says Russian Cyber Attacks Targeted Its Main Airport," *Euractiv*, (January 18, 2016), https://www.euractiv.com/section/energy/news/ukraine-says-russian-cyber-attacks-targeted-its-main-airport/.
[442] Ibid.
[443] BBC, "Russian Hackers Used Windows Bug to Target NATO," *BBC News*, (October 14, 2014), https://www.bbc.com/news/technology-29613247.

on Ukraine in 2015 and 2016 targeted critical national infrastructure leading to new legislation in the European Union. The legislation was quickly approved in the months following the BlackEnergy cyber attacks on Ukraine in 2015 and 2016 and demonstrated member-led legislative compliance. The European Union compelled members to take preventative action to increase national resilience and foster cyber defence.

In February, 2016, NATO and the European Union agreed on a technical arrangement between the incident response teams for a framework to exchange "information and sharing best practices between emergency response teams," primarily the NATO Communication Incident Response Centre and the European Union's Computer Security Emergency Response Team.[444] The technical arrangement covers "both the exchange of information on specific threats, and the sharing of best practices on technical procedures… [and] covers the configuration of networks, and partnership with industry," according to Koen Gijsbers, General Management for NATO's Communication Incident Response Centre. This technical arrangement is one of many developments in a long history of NATO-EU cyber defence coordination, including mutual participation in NATO cyber exercises like Cyber Coalition, among other initiatives.

In March, 2016, NATO and the European Union developed policy response measures against Russian cyber attacks, which targeted Ukraine's electricity grid in December 2015, to "align data protection and cyber security standards across Europe."[445] Cyber attacks in Ukraine demonstrated the immense risk to critical national infrastructure, given an "increasing reliance on interconnected systems… parts of which are hosted online."[446] The targeting of critical national infrastructure caused real-world physical effects from cyber attacks such as those which

[444] Euractiv, "Ukraine Says Russian Cyber Attacks Targeted Its Main Airport."
[445] Ibid.
[446] NATO, "NATO and the European Union Enhance Cyber Defence Cooperation," *NATO*, (February 10, 2016), http://www.nato.int/cps/en/natohq/news_127836.htm.

targeted Iran's Natanz nuclear enrichment facility in 2010. The cases of Stuxnet in 2010 and Ukraine in 2015 and 2016 provided examples of cyber attacks that targeted critical national infrastructure and caused physical damage.[447] Figure 5.7 summarizes Critical Juncture 7.

Figure 5.7 – Ukraine, 2015-2016, Summary of Critical Juncture 7

Critical Juncture 7 (Phase C)	Ukraine, 2015-2016
Events	Many inter-related cyber events occurred, such as the Ukrainian energy plant Ukrenegro being targeted by Russian BlackEnergy malware to take Ukraine's power offline.
Critical Juncture	The unprecedented use of malware to target critical national infrastructure, especially in the energy sector, and establish dangerous precedents.
NATO Policy or Institutional Change	The European Union passed significant legislation on cyber reporting requirements. NATO established an Industry Cyber Partnership and increased cyber exercises by establishing more Centres of Excellence.

5.2.6 Policy Debates, Summer 2016

Locked Shields, 2016

On January 16, 2016, NATO's Cooperative Cyber Defence Centre of Excellence hosted the Locked Shields exercise in Tallinn, where 400 soldiers and civilians participated as attackers and defenders.[448] The fictitious country "Berylia" was attacked by "strategically placed

[447]Ibid."
[448] Julian Borger, "'Trident Is Old Technology': The Brave New World of Cyber Warfare," *The Guardian*, (January 16, 2016), https://www.theguardian.com/technology/2016/jan/16/trident-old-technology-brave-new-world-cyber-warfare.

explosives and an escalating cyber assault targeting its most sensitive industry, a drone manufacturer."[449] Suspected attackers worked for the rival neighbouring country "Crimsonia."

NATO Industry Cyber Partnership

In March 2016, the NATO Industry Cyber Partnership added new roster members with American companies Cisco Systems and Fortinet to join members Microsoft and Symantec, among others, that joined the Cyber Partnership in 2015 following the Wales Summit.[450] The importance of the industry is critical given that "ninety percent of computer networks resided in the private sector," according to Lieutenant-General Mark Schissler, Deputy Chairman of NATO's Military Committee. Schissler added that "collaboration is the only road to success" to leverage "private sector developments" to build a "cyber incubator," which began with limited funding strategically directed towards minor contracts to develop specific capabilities.[451]

Crossed Swords, 2016

The Crossed Swords cyber exercise was hosted by the NATO Cooperative Cyber Defence Centre of Excellence for the first time in 2016 to function as "an annual technical red teaming cyber exercise [for] training penetration testers, digital forensics experts, and situational awareness experts."[452] The exercise was initiated in 2014 to develop and test "the capabilities and practice skills that participants needed when planning and executing a full-spectrum cyber operation."[453] Crossed Swords is distinct from the Tallinn Cyber Centre of Excellence's other

[449] Ibid.
[450] Brooks Tigner, "NATO Brings Two More Players into Its Cyber Partnership with Industry," *Janes Defence Industry*, (March 2, 2016).
[451] Ibid.
[452] CCDCOE, "Crossed Swords," https://ccdcoe.org/exercises/crossed-swords/
[453] Ibid.

cyber exercise, Locked Shields, given that the former focused on fictitious technical red team attacking capabilities to incorporate "novel… tools, tactics and procedures" to train covert skills to "target information system… infiltration, precision take-down, [and] cyber-attack attribution."[454] Locked Shields included red-team attackers facing off against blue-team defenders. Crossed Swords only focused on red team attackers to specifically train offensive cyber capabilities. These new offensive capabilities are used against blue teams during Locked Shields to test and advance responsibilities.

The Cyber Domain

The United States recognized cyberspace as the fifth domain of warfare in 2011. In May 2016, Estonian President Toomas Hendrik Ilves spoke on cyberspace as a domain of warfare.[455] The question of cyber as a domain of military operations was at the forefront of the Allies' preoccupation in the months leading up to the Warsaw Summit 2016. Sven Sakkov, Director of the Tallinn Cyber Centre of Excellence, stated that Allies at the Warsaw Summit recognized that "cyber has evolved into a domain of warfare next to air, land, sea, and space."[456] The Czech Minister of Defence, Martin Stropnicky, added “if cyber is to be designated a fifth domain… Allies must take critical steps to develop appropriate defence capabilities, including increased defence budgets.”

[454] Bernhards Blumbergs, Rain Ottis, and Risto Vaarandi, “Crossed Swords: A Cyber Red Team Oriented Technical Exercise,” *Centre for Digital Forensics and Cyber Security*, (2019), https://ristov.github.io/publications/eccws19-xs.pdf.
[455] CCDCOE, “President Ilves Describes Cyber as Fifth Domain of Warfare,” (May 2016), https://ccdcoe.org/news/2016/president-ilves-describes-cyber-as-fifth-domain-of-warfare/.
[456] Ibid.

5.3 – NATO Warsaw Summit, 2016

5.3.1 Warsaw Summit Communiqué

On July 8 and 9, 2016, the NATO Summit was held in Warsaw, Poland, with Allies agreeing to two paragraphs in the Communiqué focused on cyber defence. Paragraph 70 of the Warsaw Summit Communiqué outlined that Allies recognized "cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea."[457] Strong support remained for NATO deterrence and defence, with cyber defence "to be integrated into operational planning and Alliance operations and missions."[458] NATO expanded the Cyber Range with increased "capabilities and scope… where Allies can build skills, enhance expertise and multilateral cyber defence cooperation, including on information sharing and situational awareness, education, training, and exercises."[459]

5.3.2 Cyber Defence Pledge

Paragraph 71 outlined the Cyber Defence Pledge as "committed to enhance the cyber defence of our national networks and infrastructures... Each Ally will honour its responsibility to improve its resilience and ability to respond quickly and effectively to cyber attacks, including… hybrid contexts."[460] The Pledge represented a strong commitment by the Alliance to national cyber defence developments, which are detailed further in the next section.

The Cyber Defence Pledge was released on July 8, 2016. It included six paragraphs and seven commitments to "strengthen and enhance the cyber defences of national networks and

[457] NATO, "Warsaw Summit Communiqué."
[458] Ibid.
[459] Ibid.
[460] Ibid.

infrastructures, as a matter of policy."[461] Features of the Pledge included treating cyber defence as a strategic issue; appropriately allocating national funding; coordinating between national stakeholders; and improving understanding of threats through awareness training and education.[462]

In an interview for this study, NATO Official 6 stated that the Cyber Defence Pledge is complementary to the Defence Planning Process and is entirely voluntary, such that Allies are responsible for national defences. The Pledge raised cyber defence awareness among senior leadership to incorporate all related defence, security, and intelligence toward the end of cyber resilience. The Pledge amplified NATO's goal as a platform for Allies to facilitate bilateral, multilateral, and Alliance-wide cyber-defence coordination. In an interview for this study, NATO Official 21 argued that the Pledge provided a mechanism to enhance Alliance cyber maturity and provide national representatives with leverage to bring to their governments' Alliance-based encouragement to develop national cyber capabilities.

NATO cyber defence policy officer, Neil Robinson, wrote for *NATO Review* that the Alliance could support cyber capability development by "offer[ing] a clear platform for advice and exchange of good detailed practices between Allies through a wider variety of formal and informal channels."[463] Robinson wrote that such an approach took various forms, including "advice on the establishment of a military cyber security program or brokering the exchange of good practice on resourcing for cyber defence."[464] In an interview for this study, NATO Official

[461] NATO, "Cyber Defence Pledge," NATO, (July 8, 2016), https://www.nato.int/cps/en/natohq/official_texts_133177.htm
[462] Ibid.
[463] Neil Robinson, "NATO: Changing Gear on Cyber Defence," *NATO Review*, (June 8, 2016), https://www.nato.int/docu/review/articles/2016/06/08/nato-changing-gear-on-cyber-defence/index.html.
[464] Ibid.

21 noted that the annual questionnaire of the Cyber Defence Pledge was answered voluntarily by Allies with updated communications about national cyber defence annually.

5.3.3 Rapid Response Team

In July 2016, NATO released details on the incident response capability designed to protect "NATO's networks by providing centralized and round-the-clock cyber defence support to various… sites."[465] The Cyber Incident Response Centre maintained the cyber Rapid Response Teams, which involved Memorandums of Understanding between NATO members. Then 28 member nations set "arrangements for the exchange of a variety of cyber defence-related information and assistance to improve cyber incident prevention, resilience and response capabilities." On July 26, 2016, the NATO Communication and Information Agency announced a €3 billion investment in cyber capabilities, including "air and missile defence… [and] advanced software… to strengthen the Alliance's deterrence and defence."[466]

The investment highlighted the increased importance of cooperation between sectors for defence and deterrence measures, emphasizing a strong relationship with private sector industries. "Industry drives today's technological change," added Major-General (Retired) Koen Gijsbers, General Manager of NATO Communications and Information Agency, given that "NATO will only be resilient if we… can do continuous rapid innovation. "[467] Cyber-specific investments included €70 million to "secure mobility, multi-level authentication and the secure

[465] Ibid.
[466] NATO, "NATO Announces 3 Billion EUR Investment in Defence Technology," *NATO*, (July 26, 2016), http://www.nato.int/cps/en/natohq/news_134254.htm.
[467] Ibid.

use of public clouds."[468] Gijabers added the importance of cloud computing for NATO cyber security to assess "information quickly and securely from any location."[469]

5.3.4 Cyber Partnerships

NATO hosted its annual Information Assurance and Cyber Defence Symposium in Mons, Belgium, on September 7-8, 2016. The cyber conference included national delegations and industry and focused on crucial cyber resilience partnerships for defence. Ambassador Sorin Ducaru, as the NATO Assistant Secretary General of Emerging Security Challenges, emphasized the essential nature of partnerships given that "none of us alone [are] better equipped to fight cyber threats than all of us together."[470] Major-General Walter Huhn of Allied Command Operations added that there remains the need "to recognize we are increasingly dependent on our networks and that there are no such thing as completely secure networks... A resilient force can continue to function when the network has been attacked or disrupted."[471]

5.3.5 Hybrid Threat Centre of Excellence

The new NATO Centre of Excellence in Helsinki, Finland, opened in November 2016 to defend against hybrid threats that "target a country's weakness and sow insecurity… [such as] disinformation or fake news via social media, cyber attacks on IT systems or… the use of anonymous troops."[472] The joint venture included the United States, Germany, Sweden, Spain,

---

[468] SC Media, "NATO to Spend €70 Million on 'Cyber-Refresh,'" *SC Media*, (August 24, 2016), https://www.scmagazine.com/news/strategy/nato-to-spend-e70-million-on-cyber-refresh.
[469] Ibid.
[470] NCIA, "NATO Opens Flagship Cyber Event with Vision for the Future," *NCIA*, (September 7, 2016), https://www.ncia.nato.int/about-us/newsroom/nato-opens-flagship-cyber-event-with-vision-for-the-future.html.
[471] Ibid.
[472] YLE News, "Helsinki to Host Hub Aimed at Curbing Cyber Warfare Threats," *YLE News*, (November 21, 2016), http://yle.fi/uutiset/osasto/news/helsinki_to_host_hub_aimed_at_curbing_cyber_warfare_threats/9307244.

the United Kingdom, Poland, and the Baltic States.[473] The Helsinki Hybrid Threat Centre of Excellence was led by Matti Saarelainen, Head of the Finnish Security and Intelligence Police Department, with 4-6 other employees on a budget of €2 million.[474] The centre facilitated NATO-European Union coordination and cooperation to increase member awareness and resilience to defend against hybrid threats in a manner that facilitated coordination between NATO and the European Union.

5.3.6 NATO Cyber Defence Capacity Building, Iraq 2016

From November 21 to December 2, 2016, NATO supported a cyber defence capacity-building initiative to train Iraqi soldiers in cyber defence at the Middle East Technical University in Ankara, Türkiye. The NATO Science for Peace and Security Programme supported the initiative, which was structured to "improve their expertise and technical knowledge and contribute to strengthening Iraqi national cyber defence capabilities."[475] The course was tailored to "Iraq's needs by focussing on its cyber security and defence requirements presented to NATO." The attendees included 16 civil servants from the new Iraqi Computer Incident Response Team. The value of the training was praised by Murad Assafi, National Security Council of Iraq, to advance future cyber training by allowing "Iraq's institutions to benefit from the expertise of [these] lecturers."

The NATO Science for Peace and Security programme involved education and training as part of the Defence Capacity Building initiative Allies endorsed at the Wales Summit 2014. The cyber defence capacity building initiative in Iraq resulted from a "request from the Iraqi

[473] Ibid.
[474] Ibid.
[475] NATO, "NATO Trains Iraqi Experts in Cyber Defence," *NATO*, (November 21, 2016), https://www.nato.int/cps/en/natohq/news_139179.htm

authorities," according to Senior Advisor to the program Deniz Beten. The NATO Science for Peace and Security "rapidly reacted and provided this tailor-made, high-level expert course, significantly contributing NATO's strategic objectives in the area of defence capacity building," added Beten.[476] NATO Science for Peace and Security has been involved in defence and capacity-building programs in other partner states, including initiatives beyond cyber defence, such as training, education, and specialist equipment to deal with Improvised Explosive Devices (IED) training, education, and specialist equipment.

5.3.7 Cyber Coalition, 2016

On December 2, 2016, NATO hosted its annual Cyber Coalition exercise in Estonia over three days, which involved over 700 cyber experts from government, military, academia, and industry.[477] The exercise simulated a cyber attack that required participants to "identify the threat and mitigate the impact before it could spread across national systems. The participants tested and trained on cyber incident information sharing to quickly and efficiently coordinate cyber defences in case of an attack."[478] The NATO Cyber Centre of Excellence provided an innovative storyline which involved hacking a Smart TV "because the vulnerabilities of current smart devices are often overlooked," according to Deividas Stumbras, a Centre Training and Exercise Expert.[479] NATO needed to "speed up the relationship with industry," according to Gijsbers, who

[476] Ibid.
[477] NATO, "NATO Holds Annual Cyber Exercise in Estonia," *NATO*, (December 2, 2016), http://www.nato.int/cps/en/natohq/news_138674.htm.
[478] Ibid.
[479] CCDCOE, "NATO CCD COE Contributed to NATO's Cyber Coalition Exercise."

emphasized the need to "prepare yourself for things you have not yet seen, you want to be prepared for the worst."[480]

5.3.8 Incident Response System

On February 28, 2017, NATO's Cyber Incident Response Centre began trials for a cyber incident response system to develop an information exchange tool to advance intelligence sharing, which involved Canada, the Netherlands, Norway, and Romania, and partner nations Finland and Ireland. The Cyber Information and Incident Coordination System enabled the "cyber defence team of one country to tailor the incident warnings and information it wants to be notified… to other participants."[481] The innovative new information-sharing platform allowed officers "to rationalize how we share information and how to work together on cyber incidents," according to Frederic Jordan, Head of the Cyber Security Capability Development Branch at NATO's Communication and Information Agency in the Hague.[482] The annual cyber exercise allowed Allies to test innovative practices with new developments.

5.3.9 NATO Cyber Investment, 2017

In late March 2017, NATO announced a €3 billion investment in technological developments, including cyberinfrastructure, satellite upgrades, and computer technology.[483] The investment included €1.7 billion for satellites to support troops, ship, and drone deployments;

---

[480] Vivienne Machi, "Private Sector Plays Bigger Role in NATO Cyber Strategy," *National Defence*, (August 2, 2017), https://www.nationaldefensemagazine.org/articles/2017/2/8/private-sector-plays-bigger-role-in-nato-cyber-strategy.
[481] Brooks Tigner, "SHAPE's Cyber Defence Unit Now Trialling Three-Nation Cyber Incident System," *Jane's Defence Weekly*, (March 2, 2017).
[482] Ibid.
[483] Caroline Mortimer, "NATO to Spend Three Billion on Russia Defence," *The Independent*, (March 28, 2017), https://www.independent.co.uk/news/world/politics/nato-to-spend-three-billion-euros-on-satellites-cyber-security-and-drones-a7651966.html.

€800 million on computer systems for missile and air defence; €180 million to provide secure mobile communications for operationally deployed troops; and €71 million to improve "the protection of NATO's 32 main locations from cyber attacks."[484]

NATO Cyber Defence Policy Officer Neil Robinson outlined how the Alliance spent resources and significantly invested in cyber defence at NATO in late 2016 and 2017.[485] Robinson emphasized the critical priority of training and hiring based on focused "recruitment, retention, training, and education," given the immense competition for talent with the private sector that can "easily lure away highly skilled [individuals] and experts."[486] Robinson notes the Cyber Defence Pledge is a crucial mechanism for discussion, planning, prioritization, and implementation "to share experiences and best practices regarding cyber defence spending,… contributing to [a] more effective and efficient… Alliance."[487]

5.3.10 Locked Shields, 2017

In April 2017, the Cyber Centre of Excellence hosted its annual Locked Shields exercise, which involved teams operating as red-team attackers and blue-team defenders from 25 countries in a simulated cyber attack on an air base.[488] The exercise was a "pure chaos-type environment," said Captain Sean Ruddy, United States Cyber Command and leader of the American team in the exercise.[489] Red team attackers identified vulnerabilities and launched attacks to gain network access by advancing "through your network on six or seven different fronts… NATO members

[484] CBC, "NATO Wants to Spend over $3B US to Bolster Satellite, Cyber Defence," *CBC*, (May 27, 2017), https://www.cbc.ca/news/world/nato-satellite-computer-proposals-1.4042050.
[485] Neil Robinson, "Spending for Success on Cyber Defence," *NATO Review*, (April 6, 2017), https://www.nato.int/docu/review/articles/2017/04/06/spending-for-success-on-cyber-defence/index.html.
[486] Robinson, "Spending for Success on Cyber Defence."
[487] Ibid.
[488] Eric Niiler, "The United States Takes On the World in NATO's Cyber War Games," *Wired*, (April 29, 2017), https://www.wired.com/2017/04/us-takes-world-natos-cyber-war-games/
[489] Ibid.

getting together and testing each other's defensive capabilities."[490] Simultaneously, blue team defenders took countermeasures against the attacks to scrimmage in preparation for real-world challenges.

5.3.11 NATO Cyber Operations Centre and NATO Cyber Command Centre

NATO remains a defensive Alliance. Debates have surrounded the role of offensive cyber capabilities in operations, and to what extent that impacts the defensive nature of the Alliance. In September 2017, NATO began to "rely on members to field cyber weapons" while building a cyber command independently.[491] The 2018 NATO Brussels Summit Declaration included language in Paragraph 20, which stated that Allies agreed on "how to integrate sovereign cyber effects, provided voluntarily by Allies, into Alliance operations and missions, in the framework of strong political oversight."[492]

NATO was in the process of establishing a cyber command within NATO's command structure. Camille Grand, NATO Assistant Secretary-General for Defence Investment, confirmed at a conference in 2017 that "NATO is in the process of building its own integrated cyber command structure for defensive purposes, although offensive capabilities with still reside with member nations."[493] Numerous already existing NATO institutions influenced the development of the new cyber command. Many NATO officials interviewed for this study noted that the development of the NATO Special Operations Headquarters and the Computer Incident

[490] Ibid.
[491] Zachary Fryer-Biggs, "NATO Will Rely on Members to Independently Field Cyber Weapons but Is Building Cyber Command," *Jane's Defence Industry*, (September 7, 2017).
[492] NATO, "Brussels Summit Declaration," NATO, (July 11, 2018), https://www.nato.int/cps/en/natohq/official_texts_156624.htm.
[493] Fryer-Biggs, "NATO Will Rely on Members to Independently Field Cyber Weapons."

Response Capability was influential and substantially impacted the cyber command's development.

These sentiments were echoed by Siim Alantalu, Head of International Relations at the Cyber Centre of Excellence, who added that "NATO-owned [cyber] offensive capabilities [are] financed by Allies as a decentralized structure… pooling and sharing of operational and tactical cyber defence expertise."[494] In November 2017, NATO Secretary General Jens Stoltenberg stated that the Cyber Command Centre provided the integration of "cyber effects into NATO missions and operations to respond to a new security environment… cyber [is] part of the threat picture we have to respond to... in any military conflict cyber will be an integral part, and therefore we need to strengthen our cyber defences and… capabilities."[495]

5.3.12 Seven Resilience Baselines and the Cyber Defence Pledge

In an interview for this study, NATO Official 1 outlined resilience as a concept distinct from deterrence, given that threats below conventional military thresholds challenge the latter. Allies agreed to seven resilience baselines for civil preparedness at the 2016 NATO Warsaw Summit.[496] These baselines included:

> Assured continuity of governments and critical government services; resilient energy supplies; ability to deal effectively with the uncontrolled movement of people; resilient food and water resources; ability to deal with mass casualties; resilient civil communications systems; resilient civil transportation systems.[497]

---

[494] Ibid.
[495] Patrick Howell O'Neill, "NATO Will Establish New Cyber Command Centers," *CyberScoop*, (November 9, 2017), https://www.cyberscoop.com/nato-cyber-command-centers/.
[496] Wolf-Diether Roepke and Hasit Thankey, "Resilience: The First Line of Defence," *NATO Review*, (February 27, 2019), https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html
[497] Ibid.

The *Commitment to Enhance Resilience* was issued by NATO Heads of State and Government at the North Atlantic Council meeting in Warsaw in July 2016. Commitments outlined a continued enhancement of resilience "against the full spectrum of threats, including hybrid threats, from any direction. Resilience is essential for credible deterrence and defence and effective fulfillment of the Alliance's core tasks."[498]

NATO's *Cyber Defence Pledge* was issued at the Warsaw Summit in 2016. The document outlined Alliance measures to "reinforce the cyber defence and resilience of the Alliance," through the development of cyber capabilities, allocation of resources, and skill enhancement.[499] Additional efforts focused on annual national cyber resilience and capability development reporting mechanisms whereby Allies voluntarily shared information.

5.4 – Key Findings from Phase C

Numerous vital findings were observed during Phase C as NATO enhanced its cyber defence immensely. NATO developed its cyber defence policy during Phase C, which included a strategy to counter cyber attacks within the doctrine of collective defence and Article 5. Rapid Response Teams were developed to respond to requests by Allies for assistance to expand the capabilities of the Cyber Incident Response Centre. NATO took part in numerous engagements which strengthened relations with the private sector to coordinate cyber defence and outsource capabilities when possible.

NATO increased its development of cyber defence exercises to provide training for Allies through the annual Cyber Coalition. The NATO-affiliated Cooperative Cyber Defence Centre of

[498] NATO, "Commitment to Enhance Resilience," North Atlantic Treaty Organization, (July 8, 2016), https://www.nato.int/cps/en/natohq/official_texts_133180.htm.
[499] NATO, "Cyber Defence Pledge," North Atlantic Treaty Organization, (July 8, 2016), https://www.nato.int/cps/en/natohq/official_texts_133177.htm.

Excellence hosted exercises under the banner of Crossed Swords and Locked Shields which facilitated training to amplify NATO cyber defence policy developments. The influence of the Cyber Centre of Excellence's exercises demonstrated social learning outside the NATO decision-making hierarchy and formalized internal lessons learned processes. The Centre operated as an affiliated entity that can train staff and facilitate learning environments through workshops and exercises, among other initiatives.

The Cyber Centre of Excellence influenced NATO cyber defence policy development to facilitate exercises with simulations to train interoperability among Allies, partners, industry, and academia. Allies declared cyberspace a domain of military operations in Phase C, which established NATO's Cyber Command Centre and volunteered cyber capabilities for NATO operations. These developments expanded the recognition by the Allies that the cyber domain provided immense challenges which demanded further policy and investment.

Chapter 6: Comprehensive NATO Cyber Defence

6.1 - Phase D, January 2018 to June 2022 Madrid Summit

6.1.1 Opening Remarks

Phase D encompassed the four years from 2018 to 2022. The scope of the project ended on June 30, 2022, with the NATO Summit in Madrid, Spain. The final NATO policy documents in the analysis include the Madrid Summit Declaration and 2022 Strategic Concept. The final six months of the timeline briefly discuss the initial phases of Russia's war in Ukraine; however, the project is solely focused on developing cyber defence at NATO from 2000-June 30, 2022.[500]

6.1.2 NATO Cyber Operations Centre

On February 14, 2018, NATO Defence Ministers agreed to reform the NATO Command Structure to establish the Cyber Operations Centre within Supreme Headquarters Allied Powers Europe in Mons, Belgium.[501] A NATO spokesperson outlined that the Centre would reinforce "broaden[ed] support to NATO's cyber operational domain in a more focussed and strategic way."[502] The Centre provided “situational awareness of the domain” to manage, according to which “operational direction [will] ensure freedom of manoeuvre in all domains affected by cyberspace activities.”[503] Chief of Cyber Security at NATO’s Communications Information Agency, Ian West, outlined that the Cyber Operations Centre sought to “integrate the political, operational, and technical levels… to create a common cyber situational awareness picture.”[504]

---

[500] Extraneous events outside this timeline and related to NATO Cyber Defence or otherwise will be examined for a future research agenda. See footnote 566 for more information.
[501] Brooks Tigner, “NATO Carries Cyber Operations, Security to New Levels as Command Structure Reformed,” *Jane’s Defence Weekly*, (February 21, 2018).
[502] Ibid.
[503] Don Lewis, “What Is NATO Really Doing in Cyberspace?,” *War on the Rocks*, (February 4, 2019), https://warontherocks.com/2019/02/what-is-nato-really-doing-in-cyberspace/.
[504] Ibid.

Further developments to the NATO Cyber Operations Centre were outlined at the 2021 Brussels Summit. The 2021 Brussels Declaration outcome document established the Cyber Operations Centre in Paragraph 29 "to provide situational awareness and coordination of NATO operational activity within cyberspace."[505] The Centre's Deputy Director, United States Air Force Colonel Don Lewis, stated it functioned as "the central hub of cyberspace operations in the alliance." The Centre provided "situational awareness of the domain" to manage which "operational direction ensure[d] freedom of manoeuvre in all domains affected by cyberspace activities." A NATO official suggested the Centre involved assigning a "national cyber operations liaison officer" to reach back to the capital immediately "to provide solutions to threats for NATO."[506]

Returning to June 6, 2018, the North Atlantic Council endorsed the NATO Military Committee's Vision and Strategy on Cyberspace as a Domain of Operations.[507] NATO needed to be “able to defend itself in cyber space… in a coordinated cross-domain approach that achieves joint operational effects in support of NATO’s deterrence and defence posture.”[508] The Military Committee recognized two lines of effort for developments in NATO cyber defence. First, NATO "must possess and maintain its networks" to secure its cyber infrastructure.[509] Second, the Alliance must “be prepared to carry on with Alliance Operations and Missions in a degraded environment if attacks conducted in and through cyber space against our systems are

[505] Ibid.
[506] Tigner, "NATO and Allies Struggle over Control of Cyber capabilities."
[507] Ibid.
[508] Paul J. Mackenzie, “Cyberspace NOTAM!: NATO’s Vision and Strategy on the Cyberspace Domain,” *Allied Command Transformation,* (November 18, 2021), https://www.japcc.org/cyberspace-notam/
[509] Ibid.

successful."[510] These two lines of effort remained essential themes during the 2018 Brussels Summit in Brussels, Belgium.

6.1.3 NATO Brussels Summit, 2018

On July 11-12, 2018, the Alliance met for the NATO Summit in Brussels, and numerous paragraphs of the Brussels Summit Communiqué focused on cyber and hybrid developments. The following sub-sections focus on the specific paragraphs of the Brussels Declaration that include language on key cyber defence policy and institutional developments.

Sovereign Cyber Effects and Counter Hybrid Support Teams

Paragraph 20 focuses on integrating "sovereign cyber effects, provided voluntarily by allies, into Alliance operations and missions, in the framework of strong political oversight."[511] Member states remained confident in cyber capabilities to obtain strategic objectives in the cyber domain. The North Atlantic Council supported an Ally "at any stage of a hybrid campaign" with the option to invoke Article 5 of the Washington Treaty. Paragraph 21 introduced additional measures to defend against hybrid challenges.[512]

NATO agreed to establish Counter Hybrid Support Teams "to provide tailored and targeted assistance to the request from Allies to provide support and assistance to respond to hybrid attacks."[513] In an interview for this study, NATO Official 13 outlined that the Counter Hybrid Support Teams provided the non-conventional capability to show resolve in response to hybrid threats like Russia's annexation of Crimea in 2014. The support team provided cyber defence policymakers with additional tools to remain versatile in the years after the critical

[510] Ibid.
[511] NATO, "Brussels Summit Declaration," *NATO*, (July 11, 2018), https://www.nato.int/cps/en/natohq/official_texts_156624.htm.
[512] https://www.japcc.org/cyberspace-notam/
[513] Ibid.

juncture of Crimea in 2014. The Counter Hybrid Support Teams included a roster of experts focused on various specialties related to hybrid challenges.

Cyber Defence Capacity Building

The 2018 NATO Brussels Summit Declaration outlined various cyber defence capacity-building initiatives involving partners Jordan and Tunisia as part of the Mediterranean Dialogue. Paragraph 56 outlined the initiative with Jordan to build on "the successful implementation … in such priority areas as cyber defence."[514] Paragraph 57 outlined the initiative with Tunisia to "include cyber defence… implemented mainly through education and training activities and the exchange of expertise and best practices, in line with NATO standards." A NATO-Jordan cyber capacity-building initiative occurred in July 2017.

In an interview for this project, NATO Official 4 spoke of the high demand for cyber capacity building since 2014, including missions in Iraq, Tunisia, Moldova, Jordan, Georgia, and others. In another interview for this study, NATO Official 5 spoke of how the Alliance assisted partner countries in establishing tailored cyber emergency response teams. For example, the Alliance assisted Jordan to build a cyber emergency response team on July 19, 2017, as part of the NATO Science for Peace and Security programme.[515]

6.1.4 NATO Cyber Exercises, 2018-2019

Locked Shields, 2018

In August 2018, the NATO Cooperative Cyber Defence Centre of Excellence hosted a five-day annual Locked Shields cyber exercise. This Cyber Centre of Excellence partnered with NATO's Communication and Information Agency to simulate attacks which targeted "the critical

[514] Ibid.
[515] NATO, "NATO Supports Jordan's National Cyber Defence Strategy."

infrastructure of a fictional country, Berylia."[516] The cyber attack resulted from a "deteriorating security situation… many hostile events coincided with coordinated cyberattacks against a major civilian internet service provider and a military airbase… involving as many as 4,000 virtualized systems and more than 2,500 attacks."[517] During the exercise, more than 1,000 cyber security experts from 30 countries engaged in related scenarios which involved red-team attackers against blue-team defenders. According to Cyber Centre of Excellence security expert Kadri Kutt, the exercise focused on the "constant development" of critical infrastructure to "test and drill our resilience and defence on a regular basis."

Cyber Coalition, 2018

On November 30, 2018, NATO hosted its annual Cyber Coalition exercise over three days in NATO's Cyber Range in Tartu, Estonia. The fictional simulation involved "a small developing country, Tytan," which requested NATO's help to secure its elections.[518] Tytan's elections were threatened by "neighbour country Stellaria… trying to undermine NATO's monitoring presence" to attain "regional dominance."[519] A fictional East African country was simulated under a cyber attack with "malware infecting water treatment plants to contaminate drinking supplies and an attack on the railway network, diverting trains carrying NATO Troops meant to be guarding polling stations."[520]

---

[516] Andrew Tunnicliffe, "NATO's Locked Shield Exercise: A Cybersecurity Success?," *Army Technology*, (August 20, 2018), https://www.army-technology.com/analysis/natos-locked-shield-exercise-cybersecurity-success/.
[517] Ibid.
[518] Alexandra Brzozowski, "NATO Braces Its Cyber Warriors against Hybrid Threats," *EURACTIV*, (November 30, 2018), https://www.euractiv.com/section/defence-and-security/news/nato-braces-its-cyber-warriors-against-hybrid-threats/.
[519] Ibid.
[520] Damon Wake, "NATO Exercises Cyber Defences as Threat Grows," *Yahoo News*, (November 30, 2018), https://sg.news.yahoo.com/nato-exercises-cyber-defences-threat-grows-161421627.html.

The exercise included 700 defence troops, cyber and legal experts, government officials from NATO member states, representatives from the European Union's Military Staff and cyber emergency response team, and partner nations Finland, Ireland, and Switzerland. The exercise aimed "to train cyber defenders from across the Alliance in their ability to defend NATO and national networks… to test information sharing, situational awareness in cyberspace, and decision-making."[521] NATO Cooperative Cyber Centre of Excellence Chief of Staff Franz Lantenhammer outlined the aim to "draw attention to the cooperative aspects of cyber defence… taking into account the latest and most relevant trends in cyberspace."[522]

Crossed Swords, 2019

Crossed Swords trained technical-focused cyber capabilities where red team attackers used new tools and capabilities to train blue team defenders in other exercises like Locked Shields. Crossed Swords in 2019 provided education for "security experts and penetration testers [to] learn to cope better with diverse attack vectors and to test the offensive cyber capabilities."[523] Uniquely, the exercise focused on “industrial control systems, physical security systems, unmanned aerial vehicles, and maritime surveillance systems.”[524] The exercise was described as a “joint tactical exercise including technical experts, data collection experts and special forces operators brought under the same command,” according to Bernhards Blumbergs, Exercise Founder, Technical Director, and Cyber Security Expert from Latvia’s Computer Emergency Response Team.

[521] Wake, “NATO Exercises Cyber Defences as Threat Grows.”
[522] Ibid.
[523] CCDCOE, “Exercise Crossed Swords 2019 Integrates Cyber into Full Scale of Operations,” *CCDCOE*, (2019), https://ccdcoe.org/news/2019/exercise-crossed-swords-2019-integrates-cyber-into-full-scale-of-operations/.
[524] Ibid.

Crossed Swords hosted over 100 participants from 21 countries and provided technical training for red team attackers, including "penetration testers, digital forensic professionals, [and] situational awareness experts" to prepare for Locked Shields.[525] The 2020 Crossed Swords exercise included 120 technical experts and military operators from 26 nations.[526] A variety of unique approaches to training was involved in each exercise, and this iteration involved a focus on attribution, unit collaboration, and individual integration, to "push participants out of their comfort zone."[527]

6.1.5 Social Resilience and the Pandemic

NATO did not host a Summit in 2020 due to the COVID-19 pandemic and instead hosted multiple virtual Defence Minister Meetings. From June 17-18, 2020, NATO Defence Ministers met over secure video conference calls to address challenges posed by the pandemic. NATO's significant expertise and resources related to crisis management and disaster response provided supportive pandemic assistance to the Allies. The COVID-19 pandemic tested NATO's resilience as numerous advancing challenges demanded the Alliance adapt capabilities and expertise as required.[528] Figure 6.1 - COVID-19 2020, Summary of Critical Juncture 8 summarizes the events and changes emblematic of this particular juncture.

[525] Ibid.
[526] Chiara Vercellone, "More Countries Participate in International Cyber Exercise," *C4ISRNet*, (January 29, 2020), https://www.c4isrnet.com/newsletters/daily-brief/2020/01/27/more-countries-participate-in-natos-cyber-exercise/.
[527] Ibid.
[528] Jamie Shea, "NATO in the Era of Global Complexity: New Perspectives on Shared Security NATO's Next 70 Years," *Carnegie Europe*, (November 28, 2019), https://carnegieeurope.eu/2019/11/28/nato-in-era-of-global-complexity-pub-80417

Figure 6.1 – COVID-19 2020, Summary of Critical Juncture 8

Critical Juncture 8 (Phase D)	COVID-19 Global Pandemic, 2020
Events	The global COVID-19 pandemic amplified cyber attacks and malicious cyber activities as threat actors took advantage of the chaos caused by the pandemic.
Critical Juncture	Hackers took advantage of the fear and uncertainty of the pandemic to target individuals with increased phishing and ransomware. State-sponsored cyber capabilities targeted vaccine-related research for theft.
NATO Policy or Institutional Change	NATO expertise in crisis management and disaster relief was applied to pandemic response measures to adapt past expertise to future challenges. This general sentiment applies to cyber defence when applied to the specific response teams developed for incident responses and other related goals.

A November 2020 report by NATO's Parliamentary Assembly evaluated the Alliance's pandemic response, which "reacted swiftly and effectively to… mitigate the impact of the spreading coronavirus early in 2020."[529] NATO's coordinated response involved more than 350 missions "to transport medical personnel and supplies, construct field hospitals, and furnish tens of thousands of treatment beds."[530] NATO repurposed specialized skills and resources from crisis management and disaster relief to apply to emergency pandemic relief. The Alliance

[529] Attila Mesterhazy, "NATO's Essential Role in the COVID-19 Pandemic," *NATO Parliamentary Assembly,* (November 22, 2020), https://www.nato-pa.int/document/2020-natos-essential-role-covid-19-pandemic-revised-draft-report-mesterhazy-091-dsc-20-e
[530] Ibid.

demonstrated the ability to transition existing resources, assets, capabilities, and experience from one focus area to another.

In an interview for this study, NATO Official 1 discussed the application of existing frameworks for hybrid challenges to other areas that similarly required strong societal resilience for a strong defence. Strong social resilience provided the dual application to defend against hybrid challenges and threats from climate security. The Madrid Summit Communiqué and 2022 Strategic Concept included language directed towards climate security, which framed the impact of climate change as a security issue that threatens military logistics and operations, given concerns over the multi-decade procurement processes and given severe anticipated climate changes.

6.1.6 Lessons Learned at Cyber Coalition, 2020

The annual Cyber Coalition exercise occurred over four days in mid-November 2020 to test NATO's capabilities to experiment with new technologies. The pandemic forced the exercise to operate remotely in a "controlled… distributed fashion," using multiple locations in addition to the NATO Cyber Range in Estonia, the host location in previous years.[531] The exercise involved 1,000 participants from 25 member nations, four partner states, and European Union representatives from the Military Staff and Cyber Emergency Response Team.[532]

The exercise involved a fictional scenario of two nations on a North Atlantic island called Icebergen. The first nation, Andvaria, recently became a NATO member, and the Alliance had established a local mission. These events were paired with the election of a new government in a

[531] Gerrard Cowan, "Cyber Coalition 2020: NATO Builds Cyberspace Situational Awareness," *Jane's International Defence Review*, (December 18, 2020).
[532] Ibid.

previously neutral neighbour, Harbarus, which became "antagonistic towards its neighbour and the alliance in general."[533] The “collective exercise” lacked a competitive element in order for “participants [to] work together towards a particular goal,” said Commander Robert Buckles, Exercise Director and United States Navy Commander.

A formal Lessons Learned process followed the 2020 Cyber Coalition exercise to determine the practicality and challenges involved in the virtual setting. Buckles noted that the remote model aided logistical "development and planning" for individuals to meet more frequently with a broader array of field experts, no longer limited by geography in the same manner.[534] The exercise provided a practical example of how a formal Lessons Learned approach can be applied to current policy developments. Buckles noted that the reporting from these processes goes to the NATO Military Committee and is then assigned to relevant divisions, committees, and Alliance focus areas.

NATO Allied Command Transformation in Norfolk, Virginia, ran the Cyber Coalition exercise in cooperation with NATO International Staff of the Cyber Defence Section of the Emerging Security Challenges Division. Additionally, the NATO International Military Staff, specifically the Command, Control, and Communications Board, or C3 Board, supported Allies through the Cyber Defence Committee. NATO's Joint Analysis and Lessons Learned Centre “formalize[d] the findings” to provide added assistance to “feed back into warfare development,” to be then sent up to the North Atlantic Council for final approval.[535]

Policymakers used institutionalized processes to determine whether NATO needed “to develop new or improve existing information sharing platforms… through [Allied Command

[533] Ibid.
[534] Ibid.
[535] Ibid.

Transformation] and our cyberspace branch."[536] Social learning demonstrated that NATO learned by institutionalized means, through internalized processes supporting learning initiatives to facilitate affiliated entities like the Cyber Centre of Excellence exercise. An example of institutionalized learning at NATO involved exercises which amounted to the annual Cyber Coalition exercise hosted by the Alliance each year. The cyber exercises hosted by the affiliated Cyber Centre of Excellence can facilitate learning, to train individuals and impact how officials understand appropriate threat responses and countermeasures. Historical institutionalism combined with a social learning approach was evident at NATO, given various institutional and affiliated external bodies involved in the learning processes.

In December 2020, an Atlantic Council report argued that NATO should establish a "continuous response" in the cyber domain.[537] This language is notable, given similarities to the words used to discuss persistent engagement and cyber persistence theory. Persistent engagement combats "the continuous campaigns of cyber attacks coming from Russia and China… [by] tracking adversaries, understanding their goals, analyzing the tools used for attacks, and taking actions to degrade their capabilities."[538] The report demonstrated the external proliferation of cyber persistence theory outside of official United States government documentation as an example of the think tank community that promotes social learning. As a product of the think tank community, the report demonstrated that cyber persistence theory was evolving outside of official circles and within think tanks in the United States and is further evidence of social learning incited by historical junctures typical of taking a historical institutionalist approach to

[536] Ibid.
[537] Franklin D. Kramer, Lauren Speranza, and Conor Rodihan, "NATO Needs Continuous Responses in Cyberspace," *New Atlanticist* (Washington, DC, Atlantic Council, December 9, 2020), https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-needs-continuous-responses-in-cyberspace/.
[538] Ibid.

understand outcomes and change. This example is generalizable to understand the role of think tanks in social learning, given that they provide the unique placement to be funded to host events, workshops, and other intellectual distribution mechanism on specific subjects.

On April 15, 2021, Estonia hosted the NATO Cyber Defence Pledge conference. Senior government officials and industry executives discussed protecting critical national infrastructure from cyber attacks. A surge of ransomware attacks in the winter and spring of 2021 targeted various NATO member state organizations in different sectors of society, including critical national infrastructure in North America and Europe. Increased "malicious cyber activities" targeted NATO and Allies during the pandemic, stated Estonian Prime Minister Kaja Kallas during the Pledge conference.[539] This observation demonstrated that cyberspace was at "the forefront of increased global competition, and democratic nations must stand together against deviations from acceptable behaviour."[540] Some Allies called for a solid cyber defence to be part of NATO 2030 initiatives, which were designed to formulate recommendations from across the Alliance toward developing the 2022 Strategic Concept.[541]

6.1.7 NATO Brussels Summit, 2021

Brussels Summit Communiqué, Paragraph 32

On June 14, 2021, the annual NATO Summit occurred in Brussels, Belgium. The Brussels Summit Communiqué included many significant cyber defence policy developments detailed in Paragraph 32.[542] NATO acknowledged that cyber threats were "complex, destructive,

[539] Sebastian Sprenger, "NATO to Improve Cyber Defense in Bid to Boost Alliance Resilience," *Defense News*, (April 15, 2021), https://www.defensenews.com/global/europe/2021/04/15/nato-checks-cyber-defense-under-bid-to-boost-alliance-resilience/.
[540] Ibid.
[541] NATO, "NATO 2030: Factsheet," (Brussels, NATO, June 2021), https://www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/2106-factsheet-nato2030-en.pdf.
[542] NATO, "Brussels Summit Communiqué," *NATO*, (June 14, 2021), https://www.nato.int/cps/en/natohq/news_185000.htm.

coercive, and becoming ever more frequent."[543] Ransomware was listed as a specific threat among "other malicious cyber activity targeting our critical infrastructure and democratic institutions."[544] This language reflected a change in how the international cyber defence community, specifically NATO, understood the cyber threat environment and is more evidence of social learning. Specially, the causal processes involved in social learning begin with the external events related to the rise in ransomware around the winter and spring of 2021. External events caused critical junctures which created the permissive conditions for internal change to take place for policy to develop. The added language demonstrates the completion of this process into working NATO documents.

Cumulative Malicious Cyber Campaigns

NATO reaffirmed, "Allies recognize significant malicious cumulative cyber activities… in certain circumstances, [could] be considered amounting to an armed attack."[545] Deliberations at the North Atlantic Council operate on a case-by-case basis to determine immediate response measures. Cumulative cyber activities acknowledged that most attacks experienced by Allies involved malicious cyber activities below the threshold of an armed attack. In an interview for this study, NATO Official 2 highlighted the importance of the perspective shift and acknowledged the cumulative effects of malicious cyber activities below the typical threshold expected by classical deterrence theory.

The frequency of malicious cyber campaigns required regular briefings to the Cyber Defence Committee, where representatives from all 30 Allies sit with other members of NATO's International Staff, Military Staff, and other key stakeholders to discuss related threats. The

[543] Ibid.
[544] Ibid.
[545] Ibid.

official noted the importance of these briefings, which demonstrated the cumulative effectiveness and impact of cyber campaigns over time and the mounting importance and gravity of NATO'S internal response systems.

6.1.8 Cyber Attacks in Russia's War on Ukraine, January to June 2022

The following section focuses primarily on the cyber attacks in the initial stages of Russia's invasion of Ukraine. The strict scope is maintained given that this project's central research question is specific to cyber threats and NATO deterrence over more than two decades.

WhisperGate

On January 13, 2022, the destructive malware WhisperGate erased hundreds of computers on Ukrainian government networks by an entity known as DEV-0586, allegedly affiliated with Russian military intelligence, the GRU.[546] On January 14, 2022, NATO Secretary General Jens Stoltenberg stated, "Cyber experts in Brussels have been exchanging information with their Ukrainian counterparts on the current malicious cyber activities."[547] Soon after, NATO signed an "agreement on enhanced cyber cooperation" with Ukraine to gain access to NATO's Malware Information Sharing Platform."[548] On February 1, 2022, United States Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger spoke at NATO Headquarters in Brussels on cyber defence support for Ukraine.

FoxBlade

On February 23, 2022, the Russian military intelligence unit Sandworm released the FoxBlade wiper virus, which took down 300 systems spanning agriculture, energy, banking, and

[546] Microsoft, "Destructive Malware Targeting Ukrainian Organizations," *Microsoft Security Blog*, (January 16, 2022), https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/.
[547] NATO, "Statement by the NATO Secretary General on Cyber Attacks against Ukraine," *NATO*, (January 14, 2022), https://www.nato.int/cps/en/natohq/news_190850.htm.
[548] Ibid.

the Ukrainian government's information technology sectors.[549] Russian forces invaded Ukraine on February 24, 2022. The European Union, United Kingdom, and the United States released statements that Russia was responsible for many cyberattacks in Central Europe beginning on February 24, which targeted Ukrainian communications firm Viasat and severely impacted internet usage.[550]

DesertBlade

Cyber threat actors infiltrated an unknown Ukrainian media organization in Kyiv on February 28, 2022.[551] The Russian Defence Ministry announced on March 1 that it had assaulted military facilities in Kyiv "to thwart informational attacks against Russia."[552] Russian missiles attacked a Ukrainian television tower, and the DesertBlade virus simultaneously attacked a significant media organization.[553] Vital media communications sources are precious in disseminating information, increasing the likelihood of being targeted.

[549] Microsoft, "An Overview of Russia's Cyberattack Activity in Ukraine," *Microsoft Digital Security Unit*, (April 27, 2022), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.
[550] UK FCDO, "Russia behind Cyber-Attack with Europe-Wide Impact an Hour before Ukraine Invasion," *Press Release*, (May 10, 2022), https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion.
[551] Microsoft, "An Overview of Russia's Cyberattack Activity in Ukraine."
[552] TASS, "Russian Defense Ministry Warns about Strikes Being Prepared on Military Sites in Kiev," *TASS Russian News Agency*, (March 1, 2022), https://web.archive.org/web/20220301133913/https:/tass.com/defense/1414199.
[553] Microsoft, "An Overview of Russia's Cyberattack Activity in Ukraine."

Figure 6.2 – Russia's War in Ukraine, Invasion 2022, Summary of Critical Juncture 9

Critical Juncture 9 (Phase D)	Russian Invasion of Ukraine, February 24, 2022
Events	Russia amassed troops on the border of Ukraine over months prior to a full military invasion on February 24, 2022. Numerous cyber attacks occurred in January and February prior to the invasion.
Critical Juncture	Cyber and related attacks set new precedents for the joint use of cyber and conventional capabilities. The example of Viasat demonstrated a dangerous display of cyber capabilities when combined with supporting conventional military operations.
NATO Policy or Institutional Change	Lessons Learned during Russia's war in Ukraine occurred between February and June 2022, according to NATO Official 6 in an interview for this study. Related initiatives were part of deliberations in the months leading up to the Madrid Summit and Strategic Concept.

Industroyer2

On April 12, 2022, Ukrainian authorities prevented a cyberattack against energy infrastructure, which resulted in blackouts for up to two million Ukrainians.[554] Researchers discovered an updated version of the virus, Industroyer2, which cut off Ukraine's electricity in

[554] Kevin Collier, "Ukraine Foiled Russian Cyberattack That Tried to Shut down Energy Grid," *NBC News*, (April 12, 2022), https://www.nbcnews.com/tech/security/ukraine-says-russian-cyberattack-sought-shut-energy-grid-rcna24026.

December 2016.[555] Three assaults on Ukraine's energy sector are attributed to Sandworm, which is Unit 74455 of Russia's GRU military intelligence service.[556]

In an interview for this study, NATO Official 6 acknowledged significant developments Ukraine used to strengthen its security and defence in the years since Russia's annexation and invasion in 2014. The official noted that Ukrainian cyber defence capabilities and expertise resulted from years of targeted malicious cyber activity, like Russia's cyber attacks against Ukraine's electricity grids in 2015 and 2016. NATO Allies have provided Ukraine with significant cyber-specific support in recent years, and Official 6 confirmed these cyber capabilities included digital forensics, education, training, and intelligence sharing.

Microsoft Report

Microsoft released a report on April 27, 2022, which detailed the initial months of Russia's conventional war in Ukraine supported by offensive cyber capabilities. The report noted that 32% of national, regional, and municipal cyber attacks targeted the Ukrainian government, and 40% of violent assaults targeted critical infrastructure.[557] The Microsoft report detailed how Russia's bombing of Ukrainian communications infrastructure on March 1, 2022, was combined with targeted cyber attacks. These joint capabilities demonstrated how combined forces achieved strategic objectives using multi-domain operations.

According to Microsoft Corporate Vice-President Tom Burt, at least six Russian state actors launched more than 237 cyber operations and roughly 40 harmful assaults that targeted

[555] ESET Research, "Industroyer2: Industroyer Reloaded," *WeLiveSecurity*, (April 12, 2022), https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/.
[556] Andy Greenberg, "Russia's Sandworm Hackers Attempted a Third Blackout in Ukraine," *Wired*, (April 12, 2022), https://www.wired.com/story/sandworm-russia-ukraine-blackout-gru/.
[557] Microsoft, "An Overview of Russia's Cyberattack Activity in Ukraine."

Ukraine.[558] The insights of this report demonstrate how Russian cyber and kinetic operations functioned in the early stages of the war in Ukraine. In an interview for this study, NATO Official 6 mentioned the Microsoft report as a valuable tool which outlined Russia's use of cyber and kinetic operations in the first months of the war. The official noted that cyber capabilities had underpinned the entire conflict as a domain within which strategic effects were achieved.

Researchers warned that Russian cyber attacks risked escalating the war, as the numerous cyber attacks that targeted Ukraine in May 2022 increased the likelihood of spillover to NATO member states.[559] The United States Cybersecurity and Infrastructure Security Agency warned that due to the "unprecedented economic costs imposed on Russia as well as material support" from the United States, Allies, and partners, Russia's invasion of Ukraine escalated the threat of cyber spillover to other members.[560] The NotPetya cyber attack in 2017 was one of the most significant cyber attacks in history, which caused US $10 billion in damage and almost ended multiple significant corporations.[561] It also demonstrated the danger of untested automation on cyber escalation and spillover.

[558] Tom Burt, "The Hybrid War in Ukraine," *Microsoft*, (April 27, 2022), https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/.
[559] Atkinson and Simpson, "Escalating Russian Cyber Attacks Could Risk Widening the War in Ukraine."
[560] CISA, "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure," CISA, (April 20, 2022), https://www.cisa.gov/uscert/ncas/alerts/aa22-110a.
[561] Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, (August 22, 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Figure 6.3 – Russia's War in Ukraine, War 2022, Summary of Critical Juncture 10

Critical Juncture 10 (Phase D)	Russia's War in Ukraine, 2022
Events	Russia's war in Ukraine involved the most wiper malware in history.
Critical Juncture	New tactics, techniques, and procedures were observed, including coordination between cyber capabilities and conventional operations. Specific cyber attacks used wiper malware attacks to erase government data.
NATO Policy or Institutional Change	Future research will answer more questions about what NATO policy or institutional change resulted from Russia's use of cyber capabilities during the war in Ukraine.

In March 2022, Ukraine became a "contributing participant" with NATO's Cooperative Cyber Defence Centre of Excellence, along with other non-NATO member participants: Finland, South Korea, Sweden, and Switzerland.[562] The Centre's Director, Colonel Jaak Tarien, said, "Ukraine could bring valuable first-hand knowledge of several adversaries within the cyber domain to be used for research, exercises, and training."[563] Tarien added that the Cyber Centre of Excellence benefitted from the "valuable experience" to be shared and learned from "previous cyberattacks" that Ukraine experienced and developed expertise to counter.[564] The learning that resulted in the years after the 2014 attack will help discover what particular external and internal

[562] CCDCOE, "Ukraine to Be Accepted as a Contributing Participant to NATO CCDCOE," (Tallinn, CCDCOE, 2022), https://ccdcoe.org/news/2022/ukraine-to-be-accepted-as-a-contributing-participant-to-nato-ccdcoe/.
[563] Reuters, "Ukraine to Join NATO Cyber Defence Centre as 'Contributing Participant,'" *Reuters*, (March 4, 2022), https://www.reuters.com/world/ukraine-join-nato-cyber-defence-centre-contributing-participant-2022-03-04/.
[564] Ibid.

critical junctures combined to impact internal decision-making processes, and it may be that historical institutionalism and social learning lenses will further illuminate the narrative of NATO's evolution over time.

Where is the Cyber War?

Throughout March 2022, numerous articles and op-eds questioned where the "cyber war" was in the initial weeks of Russia's war on Ukraine. For years theorists argued that cyber capabilities would accompany conventional war with significant high-level cyber attacks to be expected, such as shutting down energy grids.[565] In an interview for this study, conducted in August 2023, NATO Official 6 noted that one reason for limited cyber warfare thus far was that Ukraine's cyber defence capabilities had been significantly hardened since the annexation of Crimea in 2014. Ukraine's security and defence capabilities developed over eight years and limited the cyber effects Russia could impose on Ukraine.[566] The official cautioned against presupposing what we believe cyber capabilities are meant to do and instead observed the distinct case of cyber effects in times of war, which sharply contrasted with observations during times of peace. Other NATO officials interviewed for this study also remarked upon the impact of the 2014 annexation on Ukraine's cyber preparations.

[565] Paul Kari, "'Catastrophic' Cyberwar between Ukraine and Russia Hasn't Happened (yet), Experts Say," *The Guardian*, (March 9, 2022), https://www.theguardian.com/technology/2022/mar/09/catastrophic-cyber-war-ukraine-russia-hasnt-happened-yet-experts-say.
[566] Kimberly Underwood, "Initial Cyber Hardening Has Helped Ukraine," *AFCEA International*, (March 15, 2022), https://www.afcea.org/signal-media/cyber/initial-cyber-hardening-has-helped-ukraine.

6.1.9 Non-State Actors in Russia's War in Ukraine

Starlink and Microsoft

A crucial feature of the cyber domain during Russia's war in Ukraine was the vital role that private industry had been given now that the threat environment involved a diverse array of state and non-state actors, including major companies and criminal entities. For example, private sector support from Elon Musk's company Starlink provided satellites to ensure Ukraine maintained communications online during the war. In an interview for this project, NATO Official 6 outlined that private industry had already offered exceptional services to Ukraine. Microsoft helped back up Ukraine's data to the cloud, and this service ensured that data was less vulnerable compared to being stored on-premises to be targeted by Russian bombs. Data stored on the cloud is on physical infrastructure outside a state's borders. Even if Ukraine's physical infrastructure is destroyed, its data could quickly be recovered using data stored on the cloud.

In an interview for this project, NATO Official 2 stated that Ukraine's government had to change national legislation to allow data and government information to be handled by Microsoft in its cloud operated from Frankfurt, Germany. Microsoft provided proactive threat hunting to detect anomalous behaviour on its cloud. In the same interview, NATO Official 2 outlined how the cloud is an invaluable option to ensure continuity of government, given that even if a server is bombed, the data remains accessible on the cloud. When data no longer relies on a physical location in a war zone, it becomes nearly indestructible. The official noted that continuity of government remains the priority during a time of war, and storing government data on the cloud for security demonstrates a strong case where private industry can support a state at war.

6.1.10 NATO Madrid Summit and Strategic Concept, June 2022

On June 29 and 30, 2022, the annual NATO Summit occurred in Madrid, Spain. In Paragraph 10, the Madrid Summit Communiqué included language on cyber defence:

> We will accelerate our adaptation in all domains, boosting our resilience to cyber and hybrid threats and strengthening our interoperability. We will significantly strengthen our cyber defences through enhanced civil-military cooperation. We will employ our political and military instruments in an integrated manner…[567]

In Madrid, Allies volunteered "national assets, to build and exercise a virtual rapid response cyber capability to respond to significant malicious cyber activities."[568] In an interview for this project, NATO Official 6 discussed NATO's initial vision for the Virtual Rapid Response Team, which Allies identified by Lessons Learned based on root causes learned from the initial months of Russia's war in Ukraine. The official emphasized the need to identify lessons learned specific to the cyber domain and understand how it works, its boundaries, and how actors operate in it.

NATO Strategic Concept, Madrid 2022

NATO adopted the 2022 Strategic Concept at the Madrid Summit. The document outlined numerous significant developments towards combatting "malign actors [that] seek to degrade our critical infrastructure, interfere with our government services, extract intelligence, steal intellectual property and impede our military activities."[569] Further developments included the adaptation of "NATO Command Structure for the information age [to] enhance our cyber defences, networks and infrastructure," given the implementation of NATO Cyber Operations Command to be fully operational by 2023.[570]

---

[567] NATO, "Madrid Summit Declaration."
[568] Ibid.
[569] NATO, "NATO 2022 Strategic Concept," *NATO,* (June 29, 2022), https://www.nato.int/strategic-concept/.
[570] Ibid.

With respect to NATO's 2022 Strategic Concept, Allies agreed to "operate effectively in space and cyberspace to prevent, detect, counter and respond to the full spectrum of threats, using all available tools."[571] Notably, the toolbox approach emphasized cross-domain countermeasures not specific to the cyber domain and instead included other areas of hybrid threats or multi-domain operations: disinformation, economic coercion, climate security, and others.

Deter and Defend Forward

The 2022 Strategic Concept included language which suggested the influence of the proactive Defend Forward strategy. Application of the strategy to the cyber domain involved Cyber Persistence Theory in the form of Persistent Engagement to conduct hunt forward operations to proactively take down adversary networks before they could be used to launch attacks. Paragraph 22 of the 2022 Strategic Concept stated NATO's Core Task on Deterrence and Defence:

> We will deter and defend forward with robust in-place, multi-domain, combat-ready forces, enhance command and control arrangements, prepositioned ammunition and equipment and improve capacity and infrastructure to rapidly reinforce any Ally, including at short or no notice.[572]

The phrase "defend forward" suggested a multi-domain proactive stance beyond the cyber domain, including the land, sea, air, and space domains.

[571] Ibid.
[572] Ibid.

6.2 - Key Findings from Phase D

Phase D exhibited several essential findings for NATO cyber defence policy and related initiatives. NATO adapted to the COVID-19 pandemic to use crisis management and disaster relief expertise for pandemic-specific challenges. This flexible approach towards social resilience demonstrated NATO's ability to change and adapt to the quick emergence of previously unforeseen threats. Exercises during Phase D included the virtual Cyber Coalition in 2020, which provided Allies with the unique opportunity to experience a remote exercise.

NATO's Lessons Learned processes included social learning from exercises and other initiatives integrated into related NATO policy-making processes. NATO demonstrated social learning with various exercises in various settings, with some that occurred remotely during the pandemic for the first time and demonstrated the Alliance's ability to adapt to contemporary threats. Cyber defence exercises provided the medium for further learning.

Figure 6.4 – NATO 2022 Strategic Concept, Summary of Internal Adjustment

Internal Adjustment (Phase D)	NATO 2022 Strategic Concept
Events	The Alliance agreed to a new Strategic Concept at the Madrid Summit, which included further cyber defence policy development at NATO.
Critical Juncture	Future research will question whether these events are akin to the 2010 Strategic Concept. At present, it is too early to conduct this research. It is assumed that such conclusions point to the results of a critical juncture, which amounts to future policy development.
NATO Policy or Institutional Change	Future research will answer related questions.

Chapter 7: Findings, Conclusions, and Future Research

7.1 – Post-Timeline Discussion

The following section will address critical observations from the scope timeline to structure the project's key findings within the four phases. Three general themes of the discussion include NATO's relations with partners, including private industry in the cyber domain, NATO's various response teams, and the applications of new strategic approaches like persistent engagement beyond the cyber domain to include countering hostile information.

Below features several essential observations from the twenty-two-year project timeline. Diagrams of each critical juncture in the appendix address the specific role that each conceptual lens had in Phase A-D. This discussion points to crucial developments observed throughout the evolution of NATO's cyber defence policy. This sub-section is then followed by the key findings from each of the four phases of the timeline.

7.1.1 Cyber Defence Capacity Building

The 2014 Russian annexation of Crimea marked a crucial time for the Alliance to pivot toward collective defence, sharpen cyber activity with partners, and advance Euro-Atlantic security. In an interview for this research study, cyber defence capacity building is in high demand but with little supply, according to NATO Official 4. The Defence and Capacity Building initiative facilitated initial requests by partners, which included: Tunisia, Iraq, Moldova, Jordan, and Georgia. International Staff negotiated tailored packages based on state desires. In an interview for this study, NATO Official 5 noted that partners requested to develop a cyber lab which could provide more advanced scenario-based training. Notably, NATO

Headquarters was unwilling to aid the Allies with any resources that could be used to develop offensive cyber capabilities, such as those that cyber labs could help develop.

7.1.2 Cyber Threat Intelligence Industry

A unique feature of the cyber domain is its unprecedented reliance on private industry. In an interview for this project, NATO Official 5 spoke of the significant professionalization of the cyber threat intelligence industry in recent years. In another interview for this study, NATO Official 8 described how the most competitive firms have cyber threat intelligence professionals from government agencies who bring the highest sophistication of state intelligence to private industry to maintain the highest standards of analytic rigour. NATO Official 8 outlined the value of outsourced open-source intelligence industry reports save on resources, expertise, and staff.

In an interview for this study, NATO Official 2 added that states no longer have a monopoly on warfare in the second decade of the twenty-first century. Instead, states must share with industry and other non-state actors. Cyber defence policy must prioritize the industry's role, the official added, given that the domain is immensely fragmented, with diverse actors, interests, and objectives heavily reliant on private infrastructure.

7.1.3 Innovation at NATO

NATO's cutting-edge policy development involved Emerging Disruptive Technologies, which will be central to future research on defence and deterrence. NATO's Defence Innovation Accelerator for the North Atlantic, or DIANA, was established at the 2021 Brussels Summit, and DIANA's Charter was approved at NATO's 2022 Madrid Summit. DIANA aims to provide "deep tech, dual-use innovators in NATO countries with funding and a fast track to adapt their

technological solutions to defence and security needs."[573] NATO's stated innovation areas include artificial intelligence, data, autonomy, quantum-enabled technologies, biotechnology, hypersonic technologies, space, novel materials and manufacturing, and energy propulsion.[574]

In recent years, NATO conducted significant security policy developments related to Emerging Disruptive Technologies. For instance, NATO released an Artificial Intelligence Strategy on October 22, 2021.[575] NATO released a Data Exploitation Framework Policy at the same meeting.[576] The DIANA Board of Directors includes all representatives from member states, who first met in October 2022 and decided on December 12, 2022, that the 2023 "priority areas of focus" on Emerging Disruptive Technologies will be "energy resilience, secure information sharing, and sensing and surveillance."[577] In an interview for this study, NATO Official 19 noted that the Alliance's platform approach provided technology leadership to connect like-minded democracies with shared values, and global strategic competition involved geopolitical coercion in informational, military, economic, and social environments.

7.1.4 Response Support Teams

NATO developed numerous rapid-response support teams to quickly address threats in a changing threat landscape. Related entities at NATO included the cyber Rapid Response Team, Counter Hybrid Support Team, and Resilience Advisory Support Team. The emergence of the first cyber Rapid Response Teams was discussed in an earlier section of this project. The

[573] NATO, "NATO Approves 2023 Strategic Direction for New Innovation Accelerator," *NATO*, (December 12, 2022), https://www.nato.int/cps/en/natohq/news_210393.htm.
[574] NATO, "Emerging and Disruptive Technologies," *NATO*, (December 8, 2022), https://www.nato.int/cps/en/natohq/topics_184303.htm.
[575] NATO, "Summary of the NATO Artificial Intelligence Strategy," *NATO*, (October 22, 2021), https://www.nato.int/cps/en/natohq/official_texts_187617.htm.
[576] NATO, "Summary of NATO's Data Exploitation Framework Policy," *NATO*, (October 22, 2023), https://www.nato.int/cps/en/natohq/official_texts_210002.htm.
[577] NATO, "NATO Approves 2023 Strategic Direction for New Innovation Accelerator."

following section briefly considers the emergence of more teams, based on interviews for this study with NATO Officials: 1, 13, 14, 15, 16, 18.

Resilience Advisory Support Team

Before Russia annexed Crimea in 2014, hybrid threat countermeasures were hosted within NATO's Operations Division in the Civil Emergency Preparedness section. Russia's annexation renewed the political appetite for countermeasures to hybrid threats, and the Counter Hybrid Support Teams were formed. These teams were part of the Hybrid Challenges and Energy Security Section formed within the Emerging Security Challenges Division. These Resilience Advisory Support Teams and other related initiatives moved from the Civil Emergency Preparedness Section to the Enablement and Resilience Section in the Defence Planning and Procurement Division.

In an interview for this study, NATO Official 14 discussed how experts were chosen to be added to the team databases. To join the Resilience Advisory Support Team expert database, an expert must be nominated by Allies at the Civil Emergency Preparedness Committee. Vacant spots are announced to fill areas of talented rosters, and experts must be citizens of NATO countries with a security clearance and willingness to remain on the roster of experts for three years.

Counter Hybrid Support Team

NATO's Counter Hybrid Support Team was deployed to Montenegro in 2019 and Lithuania in 2021. In an interview for this study, NATO Official 15 explained that allies could

request NATO support teams, and the official noted that Lithuania's request in the fall of 2021 led to NATO deploying the team for ten days to advise the government in Vilnius.[578]

In an interview for this study, NATO Official 1 described the Counter Hybrid Support Team as a group of experts sent to a requesting state after approval by the North Atlantic Council. NATO compiled a team of experts from an extensive database, with team members chosen to have a specific expertise, niche, or focus area depending on what the requesting state required. The experts will speak with key stakeholders at various relevant government ministries about specific issues, and the onset of their engagement can take merely days.

The Counter Hybrid Support Teams are similar to the older Resilience Advisory Support Teams, as both provided expertise to Allies when requested. In contrast, the Resilience Advisory Support Teams are requested in times of peace to advise Allies on how they can improve capabilities from NATO-affiliated experts. A similar catalogue of experts is used. Notably, the Counter Hybrid Support Teams added new areas of expertise related to the legal protection of civilians, intelligence, and counterintelligence.

7.1.5 Persistent Engagement to Counter Hostile Information

It is vital to outline the concept of persistent engagement and how it has come to pervade NATO corridors in the wake of Russia's war on Ukraine. NATO Official 11 outlined the strategy of "pre-bunking" to counter hostile narratives with a proactive approach designing communication products to counter hostile narratives before they occur. Pre-bunking is helpful because it is proactive and demonstrates a means to get ahead of malicious narratives before their

[578] Lithuanian Radio and Television, "NATO Counter Hybrid Support Team Arrives in Lithuania," *Lithuanian Radio and Television*, (September 7, 2021), https://www.lrt.lt/en/news-in-english/19/1490097/nato-counter-hybrid-support-team-arrives-in-lithuania.

onset. It is an approach in response to external events where competitor misinformation can force the Alliance to defend its actions in the information domain. The internal learning based on these external events and the critical juncture created, leads to discussion on more appropriate practices. An example includes NATO calling itself a "defensive" Alliance to defend against those promoting misinformation which claims that NATO exercises are displays of offensive aggression.

In an interview for this study, NATO Official 2 added that persistent engagement could be applied to the hostile information environment. For example, the United States publicly released intelligence that Russian President Vladimir Putin was about to invade Ukraine. To release this intelligence publicly exposed the future action before it occurred, which eliminated the element of surprise and shaped the narrative information environment to expose actions before they were taken.

Fischerkeller, Goldman, and Harknett outlined similar sentiments that the United States release of intelligence before Russia invaded Ukraine warned of Putin's intentions to demonstrate persistent engagement applied to strategic communications. The persistent engagement remains required to support deterrence in militarized crises and conflict… in the context of the Russo-Ukrainian War."[579] The authors quote Amy Zegart, Senior Fellow at the Hoover Institution, to outline "the relentless and pro-active [United States] intelligence disclosure campaign to control the Russia-Ukraine narrative… that seizes and maintains the narrative initiative, at least for Western audiences."[580] Proactive approaches of persistent engagement will likely remain applicable in other domains to attain strategic objectives.

[579] Fischerkeller, Goldman, and Harknett, "Persistent Engagement in Cyberspace Is a Strategic Imperative."
[580] Ibid.

7.2 – Key Findings Revisited

7.2.1 Opening Remarks

In four phases over more than two decades, conceptual lenses of historical institutionalism and social learning help discover numerous vital findings on the evolution of NATO cyber defence policy. These central findings are revisited to provide critical observations and conclusions on Phases A, B, C, and D.

7.2.2 Phase A, January 2000 to December 2006

In Phase A, NATO founded its cyber defence capabilities after cyber attacks were experienced during NATO Operation Allied Force in Kosovo in 1999. This operation was the project's first critical juncture, as Allies faced cyber threats, which demonstrated challenges and opportunities to incentivize capability development. Cyber attacks in Kosovo in 1999 demonstrated for the Allies the unprecedented use of cyber capabilities for strategic political objectives. Numerous attacks were experienced to demonstrate to Allies the need to develop policy and NATO senior policymakers initiated the development of cyber defence capabilities as a result. These developments required the initial policy language that was agreed upon by the Allies during Phase A at NATO Summits in Prague in 2002 and Riga in 2006. During Phase A, NATO learned of the immense capabilities that cyber attacks had as the first external event to cause a critical juncture during NATO operations in Kosovo in 1999. Historical institutionalism and social learning are part of innovating policy and institutions at NATO in response to the evolving threat landscape.

7.2.3 Phase B, January 2007 to December 2013

In Phase B, NATO advanced its cyber defence policy to address a threat environment of numerous critical junctures, including Estonia in 2007, Georgia in 2008, and Iran in 2010 with Stuxnet. The Alliance agreed on the 2010 Strategic Concept and Summit Communiqué at the Lisbon Summit, where Allies provided language which justified further cyber defence policy developments and investment in private industry. During this phase, NATO incorporated threats in the cyber domain with its core task of deterrence and defence. The NATO Command Structure experienced institutional developments to centralize cyber defence. The Cyber Defence Management Board was established to oversee the Cyber Incident Response Centre and Cyber Rapid Response Teams. During Phase B, NATO learned of the continued evolution of cyber threats - incorporated policy innovations to merge the cyber domain with collective defence - created new NATO cyber institutional bodies - and facilitated further learning and deployment of the rapid response countermeasures.

7.2.4 Phase C, January 2014 to December 2017

In Phase C, NATO enhanced its cyber defence capabilities. Allies outlined in the new 2014 policy that cyber attacks could invoke Article 5, given that the collective defence clause now addressed high-level cyber attacks. NATO officially recognized cyberspace as a domain of military operations, which provided the language for further discussions on how NATO incorporated cyber capabilities into its operations. Two NATO cyber defence-related institutions were established during Phase C. First, NATO's Cyber Operations Centre was established within NATO's Command Structure. Second, NATO's Cyber Incident Response Centre incorporated Rapid Response Teams to support quick capability deployment to Allies that experienced a cyber

attack. The Rapid Response Teams proved practical policy development to support Allies in responding to cyber incidents and attacks. Malicious cyber activities targeted below threshold conventional military operations to challenge consensus-based decision-making.

As the 2021 NATO Brussels Summit Communiqué acknowledged that Allies recognized that "the impact of significant malicious cumulative cyber activities might, in certain circumstances, be considered as amounting to an armed attack."[581] Malicious cyber activities over a long enough time are considered cyber campaigns, and they can impact significant strategic damage if allowed to operate unrestricted. NATO-Industry relations expanded in Phase C with increased investment and outsourced development to industry. NATO-Industry relations demonstrated the unprecedented influence of non-state actors on NATO and member states. Exercises facilitated collaborative learning networks outside formalized NATO Lessons Learned processes. For example, the NATO Cooperative Cyber Centre of Excellence hosted annual exercises Locked Shields and Crossed Swords, which demonstrated the ability of the Alliance to function as a platform to facilitate numerous learning initiatives; thus, these centres and exercises demonstrate the impact of social learning on policy outcomes.

7.2.5 Phase D, January 2018 to June 2022

In Phase D, NATO's Comprehensive Cyber Defence Policy depicted the complexity of the threat landscape, and several critical junctures impacted policy development during this phase. NATO adapted to the cyber attacks of the COVID-19 pandemic with applied expertise and resources from years of crisis management and disaster relief to assist Allies with pandemic response measures. NATO's flexible yet tailored approach to social resilience helped the

[581] NATO, "Brussels Summit Communiqué."

Alliance adapt to unexpected changes in the threat landscape. Phase D involved numerous exercises, which included NATO Cyber Coalition 2020, and the pandemic forced this exercise to operate online. This unique opportunity allowed NATO to adapt as a learning organization to a remote exercise environment. Formalized Lessons Learned approaches facilitated the internalized social learning from Cyber Coalition 2020, demonstrating how NATO exercises provide a means to exchange ideas and practices among key stakeholders.

In November 2021, the Cyber Defence Management Board disbanded, and the cyber defence and incident management portfolio was transferred to the then-newly appointed Chief Information Officer, Manfred Boudreaux-Dehmer. The CIO's biography on NATO's webpage described the role as "the single point of authority for all cybersecurity issues… leading incident management, orienting specific investments, improving NATO's cyber security posture, as well as increasing cyber security awareness NATO-wide."[582] The Office of the Chief Information Officer managed all cyber defence and incident response-related requirements. NATO integrated a formalized Lessons Learned approach into policymaking through internalized processes facilitated by the Lisbon Joint Analysis and Lessons Learned Centre.[583] This Centre operated within NATO's military structure under the leadership of Allied Commander Transformation in Norfolk, Virginia. Such formalized learning procedures illustrate the manifestation of social learning beyond NATO HQs in Brussels to the United States complex in Norfolk during Phase D.

[582] NATO, "Chief Information Officer, Manfred Boudreaux-Dehmer," *NATO*, (November 15, 2021), http://www.nato.int/cps/en/natohq/who_is_who_188597.htm.
[583] NATO JALLC, "Lessons Learned," (Lisbon: NATO, 2021), https://www.jallc.nato.int/activities/lessons-learned.

7.3 – Conceptual Lenses Applied to NATO

7.3.1 Historical Institutionalism

Historical institutionalism analyzed critical junctures that changed NATO's cyber defence policy, with many significant precedent-setting cyber attacks and malicious cyber incidents over its 20-plus-year history. Multiple research participants discussed gradual policy responses to developments where influential cyber attacks were experienced. In an interview for this study, NATO Official 18 outlined the gradual development of measures to address cyber and hybrid challenges, which occurred as an evolution of policy rather than a revolution or individual period of immense change.[584] Notably, despite policy development evolving over time, the multiple critical junctures experienced throughout the timeline suggested a punctuated equilibrium model such that evolutionary change is experienced as a result of significant external events in the form of critical junctures. Historical institutionalism helps understand NATO's relatively rapid progress over twenty years in responding to cyber challenges. The entire timeline outlined numerous significant critical junctures which impacted policy development. Major cyber attacks targeted NATO, and historical institutionalism helps understand how those critical junctures impacted the direction of cyber policy development.

7.3.2 Social Learning

Social learning helps explain NATO's cyber defence policy because the Alliance formalized many Lessons Learned processes and established many Centres of Excellence,

[584] Paal Sigurd Hilde and Andrew A. Michta, *The Future of NATO: Regional Defense and Global Security* (Ann Arbor: University of Michigan Press, 2014), https://muse.jhu.edu/book/41275.

including those focused on developing best practices in specific subjects. Over time, institutional procedures of formalized learning demonstrated NATO's internal mechanisms to help it perform as a learning organization. NATO's institutional structures socialized and internalized policy positions beyond the formalized means of internal Lessons Learned processes, including setting up military and operational exercises with affiliated organizations. The Cooperative Cyber Defence Centre of Excellence provided an indirect means to train NATO entities and personnel through the affiliated exercises hosted.

In addition, NATO's Rapid Response Team participated in Crossed Shields and Locked Swords exercises. In an interview for this study, NATO Official 10 described the bureaucratic procedure to perform an internalized Lessons Learned initiative. Staff procedures and templates outlined strategic lessons, operation outcomes, and further conclusions to be discussed. Fundamentally, the official noted that the Lessons Learned approach looked to the past to prepare for the future. The process analyzed what went wrong practically to improve response measures for the future rather than to discover for the historical record what went wrong in the past.

Protocols involved in the Lessons Learned approach demonstrate an applied case of Peter Hall's "puzzling", as these deliberations over the "puzzle" that triggered the processes threaten past paradigms. Hall notes that "the movement from one paradigm to another that characterizes third order change is likely to involve the accumulation of anomalies, experimentation with new forms of policy, and policy failures that precipitate a shift in the locus of authority over policy and initiate a wider contest between competing paradigms."[585] In an interview for this study,

[585] Peter A. Hall, "Policy Paradigms, Social Learning, and the State: The Case of Economic Policymaking in Britain," *Comparative Politics* 25, no. 3 (1993): 280.

NATO Official 10 outlined that the Lessons Learned procedures are conducted by internalized institutional mechanisms facilitating social learning at NATO. Lessons Learned first involved identifying the root causes of what went wrong, which are then used to identify lessons that can aid in future policy development.

In an interview for this study, NATO Official 3 spoke of the value of NATO's unique decision-making that distinguishes the Alliance from other international organizations like the United Nations. All NATO decisions are made by consensus such that Allies must all agree (or agree not to disagree) on every proposal. NATO is unique, given that such other institutions as the UN lack sufficient active and ongoing dialogue to shape decision-making for a smoother consensus. NATO Official 3 emphasized that consensus-based diplomacy provides benefits, including holding a higher frequency and number of meetings that facilitate frequent conversations about ongoing issues. Consistent dialogue is facilitated between Allies, representatives, and NATO staff, to ensure that pressing issues are always top of mind for senior officials and staff and to avoid sticking points that risk eroding consensus**.** Effective social learning can take place when certain circumstances are present. The challenges that remain are related to the complications presented by collection of states making decisions together as a single institution.

Each year, NATO hosts three Defence Minister meetings, three Foreign Minister meetings, and the annual Heads of State Summit. NATO Official 3 noted that consensus decision-making contributed to the institution's historical resilience. The North Atlantic Council is the highest decision-making body at NATO, which oversees all political and military decisions to reach a consensus. Furthermore:

> Consensus decision-making means that there is no voting at NATO. Consultations take place until a decision that is acceptable to all is

> reached. Sometimes member countries agree to disagree on an issue. In general, this negotiation process is rapid since members consult each other regularly and often know and understand each other's position in advance.[586]

NATO Official 3 added that consensus-based decision-making is unique and robust at NATO compared to other international organizations, given that frequent meetings allow officials to discuss and debate subjects frequently, which provides for faster consensus. Taken altogether, it seems that the higher expectations of consensus decision-making at NATO are further evidence of social learning between 2000 and 2022. In response to precedent-setting critical junctures, NATO adapted to a threat landscape forever changed.

7.4 – Questions Revisited

7.4.1 Research Questions Revisited

This section returns to the research questions outlined in Chapter 1.

Central Research Question

How does NATO's evolving strategic deterrence doctrine address contemporary security threats in the cyber domain?

One specific example focuses on "cumulative" cyber defence in the 2021 Brussels Summit Communiqué.[587] A second example is the influence of persistence theory on language in the 2022 Strategic Concept, outlining that NATO's core task of deterrence and defence involves an approach to "deter and defend forward," a clear demonstration that the language outlined by the USDOD's Defend Forward is present in NATO's most recent Strategic Concept.[588]

---

[586] NATO, "Consensus Decision-Making at NATO," *NATO*, (October 2, 2020), https://web.archive.org/web/20220225212946/https:/www.nato.int/cps/en/natohq/topics_49178.htm.
[587] NATO, "Brussels Summit Communiqué," NATO, June 14, 2021, https://www.nato.int/cps/en/natohq/news_185000.htm.
[588] NATO, "NATO 2022 Strategic Concept," June 29, 2022, https://www.nato.int/strategic-concept/.

Supplementary Research Questions

The first set of three supplementary research questions seeks to apply deterrence and defence policy to the cyber domain.

Is deterrence an appropriate means to address threats in the cyber domain?

The thesis has proven that shaping language in NATO documents is essential. The inclusion of recent language in the NATO 2022 Strategic Concept suggests that defending forward will increasingly be part of discussions related to deterrence. Deterrence alone is not an appropriate means to address threats in the cyber domain, given that it falls short in several crucial areas. These challenges were outlined in a complete section on the cyber challenge to classical deterrence.

What are the characteristics of contemporary deterrence that can deter cyber attacks?

Aspects of deterrence by entanglement to align interests and deterrence by denial to strengthen network monitoring come with the added benefit of shifting perspective to professionalize network hunting efforts within an organization. Further combined cyber resilience efforts strengthen defences at home, with hunt forward and network defence capabilities extending proactive cyber defence beyond the network.

Compared to other security strategies, is contemporary deterrence the most appropriate security strategy to deter cyber attacks?

Contemporary deterrence is not the most appropriate security strategy because it needs to consider the theoretical tenets of persistence theory and accumulation theory. Both theories provide crucial concepts to contextualize the cyber threat landscape. Policymakers can develop appropriate countermeasures to seemingly undeterrable cyber threats. The second set of

supplementary research questions focuses on NATO's cyber defence capabilities and internal institutional dynamics.

What political and strategic considerations inform the evolution of NATO cyber defence policy?

Empirical evidence includes policymaking documents in the years that followed vital policy documents, with media articles from the actual years and dates going back twenty-two years to determine what key officials were saying about the issue. During elite interviews, numerous senior policymakers supported that the specific critical junctures signify the development of cyber defence policy at NATO.

What benefits result from these policy developments?

The benefit of these policy developments is a demonstrable awareness of and adherence to the state of current cyber threats. NATO maintains cutting-edge conceptual language, which opens the path to future developments. However, the specific policy developments and other empirical evidence remain on a wait-and-see basis, given that the last 2010 Strategic Concept only began to show evidence of new policies and investments in 2011 and 2012. In 2022, future policy direction and investment questions remained central to policymaking deliberations.

What theoretical approaches underline the implementation of these policy developments?

The entire focus of the present manuscript was on cyber deterrence, a sub-category of contemporary deterrence. The theoretical approaches that underline the implementation of these policy developments include persistence theory and accumulation theory. Contemporary deterrence remains valuable but needs to include crucial challenges related to the unique qualities of cyberspace. Adherence to persistence and accumulation theories provides tools to address these challenges where deterrence is limited. The project is not a testament to these new

strategic approaches but is on the shortcomings of deterrence to address threats in the cyber domain.

What challenges remain in NATO's approach to the cyber domain?

Many challenges remain, and future research will focus on how NATO centralizes its approach to counter threats in the cyber domain. The third set of supplementary research questions focuses on institutional change at NATO as a learning organization.

Is NATO a learning organization which facilitates the Alliance's adaptation to the evolving threat landscape?

NATO learns because it has various procedures to facilitate learning, training, and education. For example, NATO's exercises and institutionalized learning capabilities allow staff to learn and develop as required. NATO Centres of Excellence provide crucial elements to support NATO learning, given that they also facilitate exercises and other research. The learning among policy officers provides the possibility for a feedback loop for policy entrepreneurs. The Tallinn Manual is an excellent example of this, currently in the development of its third version. This treatise maintains cutting-edge policy relevance while remaining outside NATO's decision-making hierarchy.

Does NATO adapt policy in response to requirements for change?

NATO has demonstrated the empirical capability to adapt to the required change. NATO adapted to the threat landscape and continues to pursue maintained adaptation up to the end of the study in Madrid. The present case is one example of the Alliance developing capabilities to counter emerging technologies. The present case involves developing a security policy toward cyber defence countermeasures.

How do Lessons Learned protocols facilitate approaches to make change within NATO?

This question is phrased in a manner that is no longer helpful, given that the entire purpose of lessons learned is to facilitate change for the Alliance. The better question is what amounts from the lessons learned processes. In an interview, the research participant described a new cyber-related program mentioned in the Madrid Summit Communiqué. The program is only mentioned, and Allies need to develop the program details, which another research participant added in a separate interview.

Does NATO implement Lessons Learned into policy and institutional change?

The study focuses on how these processes worked to include critical features of intricate details, with an observation of future policy developments in the months following the Madrid Summit to demonstrate further change.

Does social learning occur at NATO beyond the formal Lessons Learned procedures?

Bilateral and multilateral means external to NATO's formal processes maintain intense, informal and internal learning processes based on the literature on technology ecosystems, research cities, and innovation hubs. Observation, research, interviews, and analysis suggest alternative learning occurs. For example, the NATO Centres of Excellence facilitate social learning within the vast network of NATO, operating as platforms to facilitate innovation in defence and security policy. The COE is a highly focused think tank with resources, expertise, and capabilities to launch full-scale military exercises. Specific Allies fund these COEs to provide funding for the project.

Are there affiliated organizations or informal networks to amplify social learning beyond formal Lessons Learned approaches?

The next five years will be necessary for DIANA and the Innovation Hub to develop as an accelerator of accelerators Alliance-wide. The goal is to support start-ups focused on innovative defence and security to accelerate small firms into massive technological champions. To map such a network is an enormous task that illuminates where knowledge centres of learning are located as specific nodes on the network that connects NATO Allies and their innovations.

Russia's invasion of Ukraine and the resultant war beginning on February 24, 2022, required NATO policy officials to continue deliberations over the Strategic Concept between February and June 30, 2022. The Madrid Summit Communiqué and the Strategic Concept provide two fascinating documents on these crucial developments over months of immense change. Research participants described the strategic concept as a kind of snapshot of the world at its publication. From this perspective, the 2022 Strategic Concept provides empirical evidence of an Alliance in stride with a fast-changing world.

Given that NATO's cyber defence policy addresses evolving threats during the timeline, what are some characteristics to define NATO's adaptation to these threats?

NATO's approach was highly reactive in the initial years. NATO's adaptation to these threats involves applied learning requiring leaders to facilitate a knowledge ecosystem within micro-units at NATO to facilitate the ecosystem of a learning organization. First, internal leaders encouraged reading the current literature for monthly discussions on cutting-edge areas of the field. Reading rooms were hosted for discussion where all team members were welcome, and special guests facilitated discussion from cutting-edge research.

Second, team members were encouraged to publish and participate in field expert talks and conferences. The academic model has been adapted into communities of policy and

investment. This trend is embraced as interdisciplinary collaboration to compete with new and emerging threats. When academics participate in these proceedings, NATO can ensure the export of academic rigour, peer review, and strict adherence to research ethics that maintain the most stringent intellectual discourse. All these were observed at NATO, demonstrating solid platforms and networks with all cutting-edge sectors, including with the academic community.

What does the project prove?

The project proposed and defended in May 2021 included primarily a descriptive analysis of cyber defence policy change at NATO. The project proved that historical analysis could map past trends and challenges for the Alliance based on unprecedented historical events that influenced policy change and investment. NATO sought to adapt to the cyber threat landscape over two decades. The project proves that legacy institutions can adapt to technological change and that the Alliance could adapt to a changing technological threat environment.

7.5 – Discussion and Conclusions

Recall the central research question: How has NATO's evolving strategic deterrence doctrine addressed contemporary security threats in the cyber domain? This project's scope employed a theoretical approach to examine the significant challenges that cyber threats posed over twenty years to apply classical and contemporary deterrence theory in NATO's security environment. Various contemporary approaches to deterrence include punishment, denial, and entanglement. These concepts addressed the challenge of evolving deterrence theory to contemporary threats. The value of these concepts demonstrated how classical deterrence impacted the development of contemporary deterrence in response to new threats.

In an interview for this study, NATO Official 2 spoke at length about the inability of deterrence to appropriately apply to cyber threats and how the concept threatened to escalate tensions in the cyber domain and beyond. The official noted that cyberspace is a constant contest of strategic competition in the vastly interconnected threat environment, where various actors compete for temporary dominance. NATO Official 2 argued that classical deterrence was insufficient and that it was better to assume that deterrence had failed and competitors had already gained network access.

Allies gradually recognized that cyber attacks could be used to invoke Article 5. In an interview for this study, NATO Official 6 noted that Article 5 was a historical political creation fraught with deliberate ambiguity. When a situation occurs, Allies consult the facts to decide on an appropriate response. The official emphasized that cyber countermeasures are more comprehensive than the cyber domain to demonstrate the direct application of the contemporary deterrence approach of Cross Domain Deterrence. NATO's toolbox approach provided the means to tailor the Alliance's response across many domains.

This manuscript outlines NATO's use of deterrence theory to expand classical security strategy to incorporate contemporary hybrid threats. NATO's application of deterrence became less appropriate over time as evolving threats in the cyber domain demonstrated challenges to defend against new threats and apply deterrence as a less appropriate strategy. NATO gradually supplemented learning with information from exercises constituting significant and frequent interactions between NATO personnel and other experts within member states. As a result, NATO in 2022 was a very different institution compared to 2010.

This dissertation demonstrated that deterrence in the cyber domain changed radically over two decades and involved significant learning, practice, and consensus-based discussion. Indeed,

it is fundamentally important to understand that NATO changed its employment of deterrence from classical to contemporary, as depicted by statements, communiqués, and the distribution of other resources. As a result of numerous interviews with NATO Officials, there was strong sentiment toward incorporating quick change in response to critical challenges. NATO staff facilitated the combined efforts of Allies with more substantial cyber defence capabilities to assist other Allies with training and capacity building.

Allies realized over time that non-attributable threat actors make it extremely difficult to invoke Article 5 appropriately. Innovative thinking was crucial to address new ways to combat cyber threats. The inclusion of defend forward and cyber persistence language into the NATO Madrid Summit Communiqué and 2022 Strategic Concept suggests future policy will direct investment towards these subject areas, in addition to the significant investment that Allies have placed toward the security and defence of Ukraine.

NATO made significant developments to transform its cyber defence policy over more than two decades. The language in policy documents suggests future investment directions, and this observable pattern is not without precedent in NATO's history. Recall how following the 2010 Strategic Concept, language detailed further policy documents on cyber defence, which led to further policy and investment in 2011 and 2012. The focus on malicious cyber incidents mirrors the language of NATO policy documents, where Allies agreed to focus on cumulative cyber threats in the 2021 Brussels Summit Communiqué. Allies agreed that cumulative cyber-attacks and campaigns could trigger Article 5, demonstrating that policymakers adapted to changes in the threat landscape.

Malicious cyber campaigns have a cumulative effect of damaging an institution consistently over time. Such campaigns operated as cumulative critical junctures to impact the path

dependence of NATO to formulate new cyber defence policy. The close examination of debates surrounding the development of cyber defence policy at NATO explains the required changes given the cyber challenge to deterrence. Increased investment in cyber defence at NATO followed significant critical junctures, and policies were established that opened the way to fund additional cyber capabilities to present maturity. After the 2010 Strategic Concept, Allies agreed on more cyber defence policy and investment in 2011 and 2012. In the aftermath of the 2022 Strategic Concept, it remains to be seen whether the language in the 2022 Strategic Concept will lead to increased policy and investment in 2023 and 2024.

The research conducted answered the project's central research question: Classic deterrence was not an appropriate strategic approach to address threats in the cyber domain. Contemporary deterrence has made innovations with concepts like entanglement and cross-domain deterrence, yet contemporary deterrence faces many challenges that limit the effectiveness of appropriate options in response to threats in the cyber domain. There are alternative strategies to provide added value to counteract threats in the cyber domain: hunt forward and persistent engagement provide future research directions beyond this thesis and may demonstrate how these new approaches may overcome the shortcomings of contemporary deterrence.

The deterrence theory literature benefits from using various tools of Historical Institutionalism and Social Learning. These tools analyze cyber conflict and International Relations theory applied to the NATO cyber defence timeline. The institutional focus demonstrates the case of NATO as a study of cyber defence, resilience, and deterrence policy. This approach is distinct from what could be a separate project focused on the diffusion of cyber

norms related to the cyber diplomacy literature on international law, governance, and norms to understand the evolution of relevant policy.

NATO policy cites the United Nations to acknowledge the development of international law and norms. Understanding cyber norms in the context of NATO requires a foundational understanding focused on developing international cyber norms within the United Nations. The inclusion of cyber norms within NATO is discussed, citing the United Nations' documentation and norms. For example, in the Vilnius Communiqué at the 2023 NATO Summit in Lithuania, Allies agreed that NATO was "committed to act under international law, including the United Nations Charter, international humanitarian law, and international human rights law as applicable."[589] A focus on international cyber norms is best suited to a case on the United Nations, even when the desired application is NATO, given that the Alliance cites United Nations norms in its documentation.

Classical deterrence theory is now insufficient; however, it remains to be seen how contemporary deterrence theory has evolved to include new strategic approaches such as Persistent Engagement and Cyber Persistence Theory. These latter developments demonstrate that deterrence continues to evolve. NATO is analyzed as a closed-box system where theory is applied based on direct merit and application to the evolution of Alliance cyber defence policy. Other sub-areas within the cyber conflict literature related to international relations theory are not necessarily directly applicable.

[589] NATO, "Vilnius Summit Communiqué Issued by NATO Heads of State and Government," NATO, July 11, 2023, Paragraph 66, https://www.nato.int/cps/en/natohq/official_texts_217320.htm.

7.6 – Future Research

Automation, Coercion, and Persistence

This manuscript provides a strong foundation for future research to expand on the dangers of emerging technologies for security policy - an under-analysed sub-discipline within the Security Studies literature. New emerging technologies, like artificial intelligence and automation will amplify malicious threats beyond the limitations of human intelligence. For example, the Europol Innovation Lab released a report in March 2023 on using Large Language Models like ChatGPT to conduct cyber criminal behaviour, social engineering, and cybercrime.[590]

The current project focused on the question of cyber deterrence. Due to the unique challenges of cyber threats, new strategic approaches will be needed to fill the gaps that contemporary deterrence is unable to deal with. Defend forward, hunt forward, and persistent engagement represent a new demarcation of coercive approaches that will challenge the cyber domain, possibly necessitating entirely new approaches to understanding strategic developments and offensive cyber capabilities.

In 2018, the United States Department of Defence released the Defend Forward strategy and a national cyber defence policy, which applied principles of cyber persistence theory to engage adversaries in the cyber domain constantly; these were outlined in the United States Cyber Command's Persistent Engagement strategy.[591] On May 4, 2018, General Paul M. Nakasone was appointed Commander of the United States Cyber Command and Director of the

[590] Europol Innovation Lab, "ChatGPT - the Impact of Large Language Models on Law Enforcement," *Europol Innovation Lab*, (The Hague, Netherlands, March 28, 2023), https://www.europol.europa.eu/publications-events/publications/chatgpt-impact-of-large-language-models-law-enforcement.
[591] Ibid.

National Security Agency. During a January 2019 interview, Nakasone outlined vital features of applied cyber persistence theory to the United States cyber policy.

Nakasone described foundational concepts of the cyber domain, which are crucial to understanding the dynamics of applied cyber persistence theory. Cyberspace involved states in "constant contact with… adversaries," which required them to "actively defend to conduct reconnaissance… to understand where our adversary is… his capabilities… [and] intent."[592] Operations are continuous to “seize and maintain the initiative in the face of persistent threats,” given that “superiority in cyberspace is temporary.”[593] To attain an advantage in cyberspace requires “initiative,” such that forces “actively work to either improve our defences, create new accesses, or upgrade our capabilities.”

In recent decades, competing states have been free to operate maliciously to wreak havoc – unchallenged below the threshold of armed conflict – with cyber capabilities to steal intellectual property, influence elections, and cause further destruction. These "strategic campaigns" involved a "series of tactical actions… to have a strategic impact by degrading our sources of national power… [United States Cyber Command] evolved its strategic concept and operational approach from a response force to a persistence force."[594] Constant engagement adopted a proactive stance to seek out and disrupt attacks before they could occur.

Persistent engagement changed the United States Cyber Command's strategic concept to emphasize active cyber defence measures. Defenders engaged the threat landscape persistently to operate "outside our borders… outside our networks, to ensure that we understand what our adversaries are doing. If we find ourselves defending inside our networks, we have lost the

[592] Joint Forces Quarterly, “Defending Forward: An Interview With Paul M. Nakasone,” *Joint Forces Quarterly*, (Winter 2019): 4–9.
[593] Ibid.
[594] Ibid.

initiative and the advantage."[595] Nakasone described the shifted focus that evolved strategically from a "responsive force" to a "persistence force" that disrupted "adversary plots… to achieve more decisive results in pursuit of objectives set by national leaders."

Cross Domain Deterrence demonstrated it applied deterrence across domains due to the interrelated aspects of cyber and other military domains. Multi-Domain Operations provided a military concept to adapt to threats, including ″the latest commercial technology… to improve command and control of forces."[596] The common theme of such operations is NATO's use of cutting-edge technology to demonstrate the "desire… to keep up with, and stay ahead of, the challenge imposed by complex future warfare."[597]

In November 2019, Jamie Shea noted numerous strategic implications required for NATO to prepare for these new avenues of multi-domain operations.[598] A "digital divide" remained for Allies given that "a minority of Allies have acquired the new technologies and thought through how to use them effectively, while a majority have not invested in them and are prepared to fight only in limited, low-intensity engagements."[599] Shea has stated that more exercises need to be conducted to facilitate processes that "incorporate lessons learned faster into its operational procedures and organization."[600] He emphasized these ideas again in an interview with the author. A group of senior advisors from the scientific and academic communities similarly emphasized how technological change facilitated cooperation provided by industry.

---

[595] Ibid.
[596] Jose Diaz de Leon, "Understanding Multi-domain Operations at NATO," *Three Swords Magazine*, (2021), https://www.jwc.nato.int/application/files/1516/3281/0425/issue37_21.pdf.
[597] Leon, "Understanding Multi-domain Operations at NATO."
[598] Shea, "NATO in the Era of Global Complexity."
[599] Ibid.
[600] Ibid.

An ecosystem that facilitates whole-of-society innovation incentivizes Allies with strong cyber capabilities to help strengthen Allies with weaker cyber capabilities. These strategic advancements are favorable with some Allies even contracting the United States Cyber Command to conduct hunt forward operations within the requesting Ally's territory. A starting point for research will focus on hunt forward operations conducted by the United States - 24 such operations across 14 countries since 2018.[601] The United States reportedly deployed a hunt-forward team to Ukraine in 2021.[602] In 2022, various Heads of State of NATO Allies invited the United States to deploy hunt-forward operations, including Lithuania, in May 2022[603] and Croatia in August 2022.[604]

The future of cyber defence at NATO involves the proliferation of capability development to provide strong cyber powers with the resources to protect weaker cyber powers. NATO functions as a leadership platform to foster bilateral and multilateral agreements. Hunt forward operations provide the means of stronger states, to assist requesting states with cyber threats. Allies lacking cyber capabilities of their own for hunt forward operations can outsource operations to Allies that can. To remain vigorous requires continued analysis on the impacts of new emerging technologies on security policy. Future research can build upon the foundation provided by the present manuscript to support further initiatives.

Ryan J. Atkinson
June 14, 2023

---

[601] Brad D. Williams, "CYBERCOM Has Conducted 'hunt-Forward' Ops in 14 Countries, Deputy Says," *Breaking Defense*, (November 10, 2021), https://breakingdefense.com/2021/11/cybercoms-no-2-discusses-hunt-forward-space-cybersecurity-china/.
[602] Suzanne Smalley, "Nakasone Says Cyber Command Did Nine 'Hunt Forward' Ops Last Year, Including in Ukraine," *CyberScoop*, (May 4, 2022), https://www.cyberscoop.com/nakasone-persistent-engagement-hunt-forward-nine-teams-ukraine/.
[603] Ines Kagubare, "US Deployed Cyber 'Hunt Forward' Team to Croatia," *The Hill*, (August 19, 2022), https://thehill.com/policy/cybersecurity/3608312-us-deployed-cyber-hunt-forward-team-to-croatia/.
[604] Ibid.

Chapter 8: Appendix

8.1 – Bibliography

ABC News. "Ukrainian Hackers Claim NATO Cyber Attack." *ABC News*, March 16, 2014. https://www.abc.net.au/news/2014-03-16/nato-websites-targeted-in-attack-claimed-by-ukrainian-hackers/5324362.

Adams, Perri, Dave Aitel, David Perkovitch, and JD Work. "Responsible Cyber Offense." Lawfare, August 2, 2021. https://www.lawfareblog.com/responsible-cyber-offense.

Adler, Emanuel. "Seizing the Middle Ground: Constructivism in World Politics." *European Journal of International Affairs* 3, no. 3 1997.

Ames, Paul. "NATO's Geek Brigade." *Global Post*, May 22, 2013. https://theworld.org/stories/2013-05-22/natos-geek-brigade.

Angers, Lucie. "Combating Cyber-Crime: National Legislation as a Pre-Requisite to International Cooperation." In *Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research* edited by Ernesto U. Savona, 39–54. Dordrecht: Springer Netherlands, 2004.

Appathurai, James. "NATO Speech: Briefing by NATO Spokesman." *NATO*, June 6, 2006. https://www.nato.int/docu/speech/2006/s060608m.htm.

Associated Press. "NATO Response Force Is Being Activated, Stoltenberg Reveals; Its Numbers Can Grow to 40,000." *Associated Press*, February 25, 2022. https://www.msn.com/en-us/news/world/nato-response-force-is-being-activated-stoltenberg-reveals-its-numbers-can-grow-to-40000/ar-AAUjgJZ.

Atkinson, Ryan. "From Reassurance to Deterrence: Canada's Contribution to NATO Operations in Central and Eastern Europe." *NATO Association of Canada*, February 4, 2017.

https://natoassociation.ca/from-reassurance-to-deterrence-canadas-contribution-to-nato-operations-in-central-and-eastern-europe/.

Atkinson, Ryan, and Erika Simpson. "Escalating Russian Cyber Attacks Could Risk Widening the War in Ukraine." *The Hill Times*, May 11, 2022. https://www-hilltimes-com.proxy1.lib.uwo.ca/2022/05/11/escalating-russian-cyber-attacks-could-risk-widening-the-war-in-ukraine/361402.

———. "Hybrid Warfare NATO's Next Headache." *London Free Press*, February 28, 2020. https://lfpress.com/opinion/columnists/simpson-hybrid-warfare-natos-next-headache.

Baliga, Sandeep, Ethan Bueno De Mesquita, and Alexander Wolitzky. "Deterrence with Imperfect Attribution." *American Political Science Review* 114, no. 4, 2020: 1155–78. https://doi.org/10.1017/S0003055420000362.

Ball, Joshua. "What Is Hybrid Warfare? Non-Linear Combat in the 21st Century." *Global Security Review*, August 1, 2018. https://globalsecurityreview.com/hybrid-and-non-linear-warfare-systematically-erases-the-divide-between-war-peace/.

Baltic Course. "Cyber-Attacks Witnessed during NATO Exercises in Latvia Came from Russian IP Addresses." *Baltic Course*, February 12, 2014. http://www.baltic-course.com/eng/Technology/://www.baltic-course.com/eng/Technology/?doc=87601&output=d&ins_print.

Baltic News Service. "Commissar of Nashi Says He Waged Cyber Attack on Estonian Government Sites." *Swiss Baltic Chamber of Commerce in Lithuania*, October 10, 2007. https://web.archive.org/web/20071010081133/http://www.sbcc-chamber.com/index.php?lng=en&page_id=60&news_id=888.

Bandura, Albert. *Social Learning Theory*. Social Learning Theory. Oxford, England: Prentice-Hall, 1977.

Barr, Stephen. "Anti-NATO Hackers Sabotage 3 Web Sites." *Washington Post*, May 12, 1999. https://www.washingtonpost.com/wp-srv/inatl/longterm/balkans/stories/hackers051299.htm.

Baumgartner, Frank R., Christoffer Green-Pedersen, and Bryan D. Jones. "Comparative Studies of Policy Agendas." *Journal of European Public Policy* 13, no. 7, September 1, 2006: 959–74. https://doi.org/10.1080/13501760600923805.

BBC. "Russian Hackers Used Windows Bug to Target NATO." *BBC News*, October 14, 2014. https://www.bbc.com/news/technology-29613247.

———. "Tallinn Tense after Deadly Riots." *BBC News,* April 28, 2007. http://news.bbc.co.uk/2/hi/europe/6602171.stm.

———. "Ukraine: Gunmen Seize Crimea Government Buildings." *BBC News*, February 27, 2014. https://www.bbc.com/news/world-europe-26364891.

BBC News. "Kosovo Profile - Timeline." *BBC News*, June 5, 2012. https://www.bbc.com/news/world-europe-18331273.

———. "NATO Hits Chinese Embassy." *BBC News*, May 9, 1999. http://news.bbc.co.uk/1/hi/world/europe/338424.stm.

———. "Serbia Profile - Timeline." *BBC News*, May 1, 2012. https://www.bbc.com/news/world-europe-17913357.

Belo, Dani, and David Carment. "Grey Zone Conflict: Implications for Conflict Management." *CGAI Policy Perspective*, December 2019. https://www.cgai.ca/grey_zone_conflict_implications_for_conflict_management.

Blumbergs, Bernhards, Rain Ottis, and Risto Vaarandi. "Crossed Swords: A Cyber Red Team Oriented Technical Exercise." *Centre for Digital Forensics and Cyber Security*, 2019. https://ristov.github.io/publications/eccws19-xs.pdf.

Borger, Julian. “Pentagon Kept the Lid on Cyberwar in Kosovo.” *The Guardian*, November 9, 1999. https://www.theguardian.com/world/1999/nov/09/balkans.

———. “‘Trident Is Old Technology’: The Brave New World of Cyber Warfare.” *The Guardian*, January 16, 2016, https://www.theguardian.com/technology/2016/jan/16/trident-old-technology-brave-new-world-cyber-warfare.

Borghard, Erica D, and Shawn W Lonergan. “Cyber Operations as Imperfect Tools of Escalation.” *Strategic Studies Quarterly*, (Fall 2019), 122–45.

Borghard, Erica, and Shawn Lonergan. “The Logic of Coercion in Cyberspace.” *Security Studies* 26 (July 3, 2017): 452–81.

Brandon, Russell. “Cyberattacks Spiked as Russia Annexed Crimea.” *The Verge*, May 29, 2014. https://www.theverge.com/2014/5/29/5759138/malware-activity-spiked-as-russia-annexed-crimea.

Brantly, Aaron. “Conceptualizing Cyber Deterrence by Entanglement.” *SSRN Scholarly Paper*. (Rochester, NY, April 5, 2018). https://doi.org/10.2139/ssrn.2624926.

Brantly, Aaron F. “The Cyber Deterrence Problem.” In *2018 10th International Conference on Cyber Conflict*, 31–54. (Tallinn: *IEEE*, 2018). https://doi.org/10.23919/CYCON.2018.8405009.

Bright, Arthur. “Estonia Accuses Russia of ‘Cyberattack.’” *Christian Science Monitor*, May 17, 2007. https://www.csmonitor.com/2007/0517/p99s01-duts.html.

Brzozowski, Alexandra. “NATO Braces Its Cyber Warriors against Hybrid Threats.” *EURACTIV*, November 30, 2018. https://www.euractiv.com/section/defence-and-security/news/nato-braces-its-cyber-warriors-against-hybrid-threats/.

Buchanan, Ben. *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations*. (Oxford: Oxford University Press, 2016).

https://books.google.ca/books/about/The_Cybersecurity_Dilemma.html?id=YBlhvgAACAAJ&redir_esc=y.

———. *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Cambridge, Massachusetts: Harvard University Press, 2020.

But, Tom. "The Hybrid War in Ukraine." *Microsoft*, April 27, 2022. https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/.

Capoccia, Giovanni, and R. Daniel Kelemen. "The Study of Critical Junctures: Theory, Narrative, and Counterfactuals in Historical Institutionalism." *World Politics* 59, no. 3, April 2007: 341–69. https://doi.org/10.1017/S0043887100020852.

Carment, David, and Dani Belo. "Gray Zone Conflict Management: Theory, Evidence, and Challenges." *Journal of European, Middle Eastern, & African Affairs*, June 2020. https://www.airuniversity.af.edu/JEMEAA/Display/Article/2213954/gray-zone-conflict-management-theory-evidence-and-challenges/.

Cavelty, Myriam D. "Cyber-Allies: Strengths and Weaknesses of NATO's Cyberdefense Posture." *IP Global Edition* 12, no. February 3 1, 2012. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1997153.

CBC. "NATO Wants to Spend over $3B US to Bolster Satellite, Cyber Defence." *CBC*, May 27, 2017. https://www.cbc.ca/news/world/nato-satellite-computer-proposals-1.4042050.

CCCS. "Cyber Attack," *CCCS*. July 30, 2020. https://www.canada.ca/en/global-affairs/news/2020/07/canada-welcomes-european-unions-announcement-of-new-cyber-sanctions-listings.html.

———. "Cyber Threat." *CCCS,* May 3, 2022. https://cyber.gc.ca/en/glossary#c.

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). "CCDCOE-ACT Workshop 2021: Cyberspace Strategic Outlook 2030 - Doctrinal Thinking and Tactics, 2021, https://www.youtube.com/watch?v=eMQm5EGhNK4.

———. "Crossed Swords," n.d. https://ccdcoe.org/exercises/crossed-swords/.

———. "Exercise Crossed Swords 2019 Integrates Cyber into Full Scale of Operations." *CCDCOE*, 2019. https://ccdcoe.org/news/2019/exercise-crossed-swords-2019-integrates-cyber-into-full-scale-of-operations/.

———. "President Ilves Describes Cyber as Fifth Domain of Warfare." *CCDCOE*, May 2016. https://ccdcoe.org/news/2016/president-ilves-describes-cyber-as-fifth-domain-of-warfare/.

———. "Secretary General Stoltenberg: Cyber Is Part of NATO Collective Defence." *CCDCOE*, September 2014. https://ccdcoe.org/news/2014/secretary-general-stoltenberg-cyber-is-part-of-nato-collective-defence/.

———. "Strategy and Governance Archive." *CCDCOE*. https://ccdcoe.org/library/strategy-and-governance/.

———. "Ukraine to Be Accepted as a Contributing Participant to NATO CCDCOE." *CCDCOE* March 2022. https://ccdcoe.org/news/2022/ukraine-to-be-accepted-as-a-contributing-participant-to-nato-ccdcoe/.

Chakarova, Lora. "EU and NATO Design Response to Cyber-Attacks." *Jane's Intelligence Review*, March 2, 2016.

Chambers, John. "Countering Gray-Zone Hybrid Threats: An Analysis of Russia's New Generation Warfare and Implications for the US Army." *West Point Modern War Institute*, October 18, 2016. https://mwi.usma.edu/wp-content/uploads/2016/10/Countering-Gray-Zone-Hybrid-Threats.pdf.

Check Point. "Global Cyberattacks Continue to Rise with Africa and APAC Suffering Most." Highlight Report, April 27, 2023. https://blog.checkpoint.com/research/global-cyberattacks-continue-to-rise/.

Checkel, Jeffrey T. "The Constructivist Turn in International Relations Theory." Edited by Martha Finnemore, Peter Katzenstein, and Audie Klotz. *World Politics* 50, no. 2 (1998): 324–48.

CISA. "Critical Infrastructure Sectors," 2022. https://www.cisa.gov/critical-infrastructure-sectors?stream=top.

CISA. "Ransomware Awareness for Holidays and Weekends." *CISA Cybersecurity Advisory*, February 10, 2022. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-243a.

———. "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure," April 20, 2022. https://www.cisa.gov/uscert/ncas/alerts/aa22-110a.

Clarke, Richard Alan, and Robert K. Knake. *The Fifth Domain: Defending Country and Companies in the Age of Cyber Threats*. London: Penguin Press, 2019. https://books.google.ca/books/about/The_Fifth_Domain.html?id=NRuIvQEACAAJ&redir_esc=y.

Cohn, Carol. "Sex and Death in the Rational World of Defense Intellectuals." *Signs* 12, no. 4 (1987): 687–718.

Collier, Kevin. "Ukraine Foiled Russian Cyberattack That Tried to Shut down Energy Grid." *NBC News*, April 12, 2022. https://www.nbcnews.com/tech/security/ukraine-says-russian-cyberattack-sought-shut-energy-grid-rcna24026.

Collins, Allan, John Seely Brown, and Susan E. Newman. "Cognitive Apprenticeship: Teaching the Crafts of Reading, Writing, and Mathematics." In *Knowing, Learning, and Instruction*, edited by Lauren B. Resnick, 1st ed., 453–94. Routledge, 2018.

Collins, Sean, and Stephen McCombie. "Stuxnet: The Emergence of a New Cyber Weapon and Its Implications." *Journal of Policing, Intelligence and Counter Terrorism* 7, no. 1 (April 1, 2012): 80–91. https://doi.org/10.1080/18335330.2012.653198.

Couzigou, Irène. "Securing Cyber Space: The Obligation of States to Prevent Harmful International Cyber Operations." *International Review of Law, Computers & Technology* 32, 1 (April 2018): 37–57. https://doi.org/10.1080/13600869.2018.1417763.

Cowan, Gerrard. "Cyber Coalition 2020: NATO Builds Cyberspace Situational Awareness." *Jane's International Defence Review*, December 18, 2020.

Cox, Robert Henry, and Daniel Béland. "Valence, Policy Ideas, and the Rise of Sustainability." *Governance* 26, no. 2 (2013): 307–28. https://doi.org/10.1111/gove.12003.s

Creative Commons. "Attribution-ShareAlike 2.0 Generic." https://creativecommons.org/licenses/by-sa/2.0/.

"Crimea Crisis: Pro-Russians Seize Ukrainian Naval Bases." *BBC News*, March 19, 2014. https://www.bbc.com/news/world-europe-26643141.

Cullen, Patrick, and Erik Reichborn-Kjennerud. "Understanding Hybrid Warfare." *Multinational Capability Development Campaign*, 2017. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf.

D'Antonio, Collin, Stephanie Gower, Andrea Young, and Edward Teague. "Non-Kinetic Operations for Stabilizing Government." In *2014 Systems and Information Engineering Design Symposium*. (2014): 90–95.

Deep, Alex. "Hybrid War: Old Concept, New Techniques." *Small Wars Journal*, February 3, 2015. https://smallwarsjournal.com/jrnl/art/hybrid-war-old-concept-new-techniques.

Defence News. "Firms Team for NATO Cybersecurity Work." *Defence News*, December 21, 2011.

Deibert, Ronald J., Rafal Rohozinski, and Masashi Crete-Nishihata. “Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War.” *Security Dialogue* 43, no. 1 (2012): 3–24.

Ducheine, P. L. “Non-Kinetic Capabilities: Complementing the Kinetic Prevalence to Targeting.” *Amsterdam Law School Research Paper*, July 30, 2014. https://papers.ssrn.com/abstract=2474091.

Economist. “A Cyber-Riot.” *The Economist*, May 10, 2017. https://www.economist.com/europe/2007/05/10/a-cyber-riot.

———. “An Anonymous Foe.” *The Economist*, June 15, 2011. https://www.economist.com/international/2011/06/16/an-anonymous-foe.

Edmondson, Amy, and Bertrand Moingeon. “From Organizational Learning to the Learning Organization.” *Management Learning* 29, no. 1 (March 1, 1998): 5–20.

ENISA. “National Cyber Security Strategies - Interactive Map.” NCSS Map. *European Union Agency for Cybersecurity.* https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.

Research, ESET. "Industroyer2: Industroyer Reloaded." *WeLiveSecurity*, April 12, 2022. https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/.

Euractiv. “Ukraine Says Russian Cyber Attacks Targeted Its Main Airport.” *Euractiv*, January 18, 2016. https://www.euractiv.com/section/energy/news/ukraine-says-russian-cyber-attacks-targeted-its-main-airport/.

Farwell, James P., and Rafal Rohozinski. “Stuxnet and the Future of Cyber War.” *Survival* 53, no. 1 (February 2011): 23–40. https://doi.org/10.1080/00396338.2011.555586.

Finnemore, Martha, and Kathryn Sikkink. "International Norm Dynamics and Political Change." *International Organization* 52, no. 4 (1998): 887–917.

Fischerkeller, Michael P., Emily O. Goldman, and Richard J. Harknett. *Cyber Persistence Theory: Redefining National Security in Cyberspace*. New York: Oxford University Press, 2022.

Fischerkeller, Michael P, Emily O. Goldman, and Richard J Harknett. "Persistent Engagement in Cyberspace Is a Strategic Imperative." *The National Interest*, July 6, 2022. https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/persistent-engagement-cyberspace.

Fischerkeller, Michael P, and Richard J Harknett. "Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation." *The Cyber Defence Review*, (2019): 267–87.

Freedberg, Sydney J. "NATO Hews To Strategic Ambiguity On Cyber Deterrence." *Breaking Defense*, November 7, 2014. https://breakingdefense.com/2014/11/natos-hews-to-strategic-ambiguity-on-cyber-deterrence/.

Fryer-Biggs, Zachary. "NATO Will Rely on Members to Independently Field Cyber Weapons but Is Building Cyber Command." *Jane's Defence Industry*, September 7, 2017.

Gallagher, Mike. "State of Deterrence by Denial." *The Washington Quarterly* 42, no. 2 (April 3, 2019): 31–45. https://doi.org/10.1080/0163660X.2019.1626687.

Garamore, Jim. "Lynn Arrives in Brussels for Cyber Security Talks." *DVIDS*, January 23, 2011. https://www.dvidshub.net/news/64060/lynn-arrives-brussels-cyber-security-talks.

Gartzke, Erik, and Jon R. Lindsay. "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace." *Security Studies* 24, no. 2 (April 3, 2015): 316–48.

Gartzke, Erik, and Jon R. Lindsay, eds. *Cross-Domain Deterrence: Strategy in an Era of Complexity*. Oxford: Oxford University Press, 2019. https://books.google.ca/books/about/Cross_Domain _deterrence. html?id=JPiFDwAAQBAJ&source=kp_book_description&redir_esc=y.

Gazula, Mohan B. "Cyber Warfare Conflict Analysis and Case Studies." *MIT Sloan School Working Paper*, (May 2017): 100.

Gerasimov, Valery. "The Value of Science Is the Foresight." *Military Review*, (February 2016), 23–29.

Glenn, Russell W. "Thoughts on 'Hybrid' Conflict." *Small Wars Journal*, February 3, 2009. https://smallwarsjournal.com/jrnl/art/thoughts-on-hybrid-conflict.

Global Affairs Canada. "Canada Welcomes European Union's Announcement of New Cyber Sanctions Listings." *Statements of Global Affairs Canada*, July 30, 2020. https://www.canada. ca/en/global-affairs/news/2020/07/canada-welcomes-european-unions-announcement-of-new-cyber-sanctions-listings.html.

Global News. "NATO Plans Response to Cyberattacks." *Global News*, September 2, 2014. https://globalnews.ca/news/1539145/nato-plans-response-to-cyberattacks/.

Greenberg, Andy. "Russia's Sandworm Hackers Attempted a Third Blackout in Ukraine." *Wired*, April 12, 2022. https://www.wired.com/story/sandworm-russia-ukraine-blackout-gru/.

———. *Sandworm*. Penguin Random House, 2019. https://www.penguinrandomhouse.com/books/597684/sandworm-by-andy-greenberg/.

———. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *Wired*, August 22, 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

———. “Ukraine Suffered More Data-Wiping Malware in 2022 Than Anywhere, Ever.” *Wired*, February 22, 2023. https://www.wired.com/story/ukraine-russia-wiper-malware/.

Grigsby, Alex. “The End of Cyber Norms.” *Survival* 59, no. 6 (November 2, 2017): 109–22. https://doi.org/10.1080/00396338.2017.1399730.

Hacker, Jacob S., and Paul Pierson. “After the ‘Master Theory’: Downs, Schattschneider, and the Rebirth of Policy-Focused Analysis.” *Perspectives on Politics* 12, no. 3 (September 2014): 643–62. https://doi.org/10.1017/S1537592714001637.

Hale, Julian. “NATO Official Highlights Areas for EU-NATO Cyber Cooperation.” *Defence News,* May 31, 2012. http://rpdefense.over-blog.com/article-nato-official-highlights-areas-for-eu-nato-cyber-cooperation-106157528.html.

Hall, Peter A., and Rosemary C. R. Taylor. “Political Science and the Three New Institutionalisms.” *Political Studies* 44, no. 5 (1996): 936–57. https://doi.org/10.1111/j.1467-9248.1996.tb00343.x.

Hare, Forrest. “The Significance of Attribution to Cyberspace Coercion: A Political Perspective.” (Tallinn, Estonia: NATO NATO Cooperative Cyber Defence Centre of Excellence, 2012). https://ccdcoe.org/uploads/2012/01/2_5_Hare _TheSignificanceOfAttribution.pdf.

Hasenclever, Andreas, Peter Mayer, and Volker Rittberger. “Integrating Theories of International Regimes.” *Review of International Studies* 26, no. 1 (2000): 3–33.

Healey, Jason. “Cyber Attacks Against NATO, Then and Now.” *Atlantic Council*, September 6, 2011. https://www.atlanticcouncil.org/blogs/new-atlanticist/cyber-attacks-against-nato-then-and-now/.

Healey, Jason, and Robert Jervis. "The Escalation Inversion and Other Oddities of Situational Cyber Stability," 2020. https://doi.org/10.26153/TSW/10962.

Healey, Jason, and Klara Tothova Jordan. “NATO’s Cyber Capabilities: Yesterday, Today, and Tomorrow.” *Atlantic Council*, September 1, 2014. https://www.jstor.org/stable/resrep03426.

Hicks, Kathleen H., and Melissa Dalton. *Center for Strategic & International Studies. By Other Means: US Priorities in the Gray Zone*. (Washington, DC: Rowman & Littlefield, 2019).

Hilde, Paal S., and Andrew A. Michta. *The Future of NATO: Regional Defense and Global Security*. Ann Arbor: University of Michigan Press, 2014. https://muse.jhu.edu/book/41275.

Hoffman, Frank G. "Conflict in the 21st Century: The Rise of Hybrid Wars." Arlington: Potomac Institute for Policy Studies, 2007. https://potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.

———. "The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War." *The Heritage Foundation*, 2016, 25–36.

Hollis, David. "Cyberwar Case Study: Georgia 2008." *Small Wars Journal*, January 6, 2011. https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf.

Hughes, Robin. "Ukraine Braces for Cyber Offensive." *International Defence Review*, March 5, 2014.

Huth, Paul K. "Deterrence and International Conflict: Empirical Findings and Theoretical Debates." *Annual Review of Political Science* 2, no. 1 (June 1999): 25–48.

IBM. "2019 Cost of a Data Breach Report," 2019. https://www.ibm.com/downloads/cas/RDEQK07R#:~:text=The%20lifecycle%20of%20a%20data%20breach%20is%20getting%20longer.

ICDS. "Increasing NATO's Role in Cyber Defence." *ICDS*, August 28, 2014. https://icds.ee/en/increasing-natos-role-in-cyber-defence/.

INTERPOL. "INTERPOL Report Shows Alarming Rate of Cyberattacks during COVID-19." *INTERPOL*, August 4, 2020. https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19.

Ittelson, Pavlina. “What’s New with Cybersecurity Negotiations? United Nations Cyber OEWG Final Report Analysis.” *Diplo*, March 19, 2021. https://www.diplomacy.edu/blog/whats-new-cybersecurity-negotiations-un-cyber-oewg-final-report-analysis/.

Jasper, Scott. *Strategic Cyber Deterrence: The Active Cyber Defense Option*. Lanham: Rowman & Littlefield, 2017.

Jervis, Robert. “Deterrence and Perception.” *International Security* 7, no. 3 (1982): 3–30. https://doi.org/10.2307/2538549.

Joint Forces Quarterly. “Defending Forward: An Interview With Paul M Nakasone.” *Joint Forces Quarterly*, (Winter 2019), 4–9.

Jones, Sam. “Nato Leaders Plot Cyber Fightback.” *Financial Times*, July 13, 2014. https://www.ft.com/content/0208cd24-0aa0-11e4-be06-00144feabdc0.

Jose De Leon, Diaz. "Understanding Multidomain Operations at NATO." *Three Swords Magazine*, 2021. https://www.jwc.nato.int/application/files/1516/3281/0425/issue37_21.pdf.

Kagubare, Ines. “US Deployed Cyber ‘Hunt Forward’ Team to Croatia.” *The Hill*, August 19, 2022. https://thehill.com/policy/cybersecurity/3608312-us-deployed-cyber-hunt-forward-team-to-croatia/.

Kello, Lucas. *The Virtual Weapon and International Order*. New Haven: Yale University Press, 2017. https://books.google.ca/books?hl=en&lr=&id=W0QzDwAAQBAJ&oi=fnd&pg=PP1&ots=Kei4yoUfeZ&sig=oXP4uAzXkzem88Ixg_p7g_VlnWI&redir_esc=y#v=onepage&q=UNPEACE&f=false.

Keohane, Robert O. “International Institutions: Two Approaches.” *International Studies Quarterly* 32, no. 4 (1988): 379–96. https://doi.org/10.2307/2600589.

Kimball, Spencer. “NATO Moves to Apply Armed Conflict Law to Cyber Warfare.” *DW*, July 2, 2014. https://www.dw.com/en/nato-moves-to-apply-armed-conflict-law-to-cyber-warfare/a-17754359.

Kirk, Jeremy. “Hacking Team Claims NATO Server Compromised.” *Computerworld*, July 6, 2011. https://www.computerworld.com/article/2741641/hacking-team-claims-nato-server-compromised.html.

Klimburg, Alexander. “National Cyber Security Framework Manual.” *NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)*, 2012. https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf.

Kotsias, James, Atif Ahmad, and Rens Scheepers. “Adopting and Integrating Cyber-Threat Intelligence in a Commercial Organisation.” *European Journal of Information Systems* 32, no. 1 (January 2, 2023): 35–51. https://doi.org/10.1080/0960085X.2022.2088414.

Kondrotas, Albertas. “Private Armies Throughout the Generations of Warfare: Pitfalls and Prospects.” National Defense Academy of Estonia, 2010.

Kramer, Franklin D, Lauren Speranza, and Conor Rodihan. “NATO Needs Continuous Responses in Cyberspace.” *New Atlanticist*. (Washington, DC, Atlantic Council, 2020). https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-needs-continuous-responses-in-cyberspace/.

Kruhlov, Vitalii, Mykola Latynin, Alina Horban, and Anton Petrov. “Public-Private Partnership in Cybersecurity,” 2020. https://ceur-ws.org/Vol-2654/paper48.pdf.

Kushner, David. “The Real Story of Stuxnet.” *IEEE Spectrum* 50, no. 3 (March 2013): 48–53. https://doi.org/10.1109/MSPEC.2013.6471059.

Lahtinen, Johanna. "Local Social Knowledge Management: A Case Study of Social Learning and Knowledge Sharing across Organizational Boundaries." *Journal of Information Science* 39, no. 5 (October 1, 2013): 661–75.

Lambeth, Benjamin S. *NATO's Air War for Kosovo: A Strategic and Operational Assessment*. (Santa Monica: RAND Corporation, 2001). https://doi.org/10.7249/MR1365.

Lave, Jean, and Etienne Wenger. *Situated Learning: Legitimate Peripheral Participation*. 1st ed. Cambridge University Press, 1991.

Larrinaga, Nicholas. "NATO Extends Cyber Defences." *Jane's Defence Weekly*, September 15, 2015.

Leach, William, and Paul Sabatier. "To Trust An Adversary: Integrating Rational and Psychological Models of Collaborative Policymaking." *American Political Science Review* 99 (2005): 491–503. https://doi.org/10.1017/S000305540505183X.

Lewis, Don. "What Is NATO Really Doing in Cyberspace?" *War on the Rocks*, February 4, 2019. https://warontherocks.com/2019/02/what-is-nato-really-doing-in-cyberspace/.

Leyden, John. "Defence Talks to Forge EU Cyberwar Strategy." *The Register*, March 15, 2011. https://www.theregister.com/2011/03/15/cyberwar_defence_talks/.

———. "Russian Spy Agencies Linked to Georgian Cyber-Attacks." *The Register*, March 23, 2009. https://www.theregister.com/2009/03/23/georgia_russia_cyberwar_analysis/.

Limnell, Jarno. "NATO's September Summit Must Confront Cyber Threats." *Breaking Defense*, August 11, 2014. https://breakingdefense.sites.breakingmedia.com/2014/08/natos-september-summit-must-confront-cyber-threats/.

Lind, William J, Keith Nightengale, John Schmitt, Joseph W Sutton, and Gary Wilson. "The Changing Face of War: Into the Fourth Generation." *Marine Corps Gazette* 73, no. 10 1989. https://www.academia.edu/7964013/The_Changing_Face_of_War_Into_the_Fourth_Generation.

Lithuanian Radio and Television. “NATO Counter Hybrid Support Team Arrives in Lithuania.” *Lithuanian Radio and Television*, September 7, 2021. https://www.lrt.lt/en/news-in-english/19/1490097/nato-counter-hybrid-support-team-arrives-in-lithuania.

Lundgren, Magnus, Theresa Squatrito, and Jonas Tallberg. “Stability and Change in International Policy-Making: A Punctuated Equilibrium Approach.” *The Review of International Organizations* 13, no. 4 (December 1, 2018): 547–72.

Lupovici, Amir. “Cyber Warfare and Deterrence: Trends and Challenges in Research.” *Military and Strategic Affairs*, p, 3, no. December 3, 2011. https://www.inss.org.il/wp-content/uploads/2017/02/FILE1333533336-1.pdf.

———. “The Emerging Fourth Wave of Deterrence Theory—Toward a New Research Agenda.” *International Studies Quarterly* 54, no. 3 (2010): 705–32.

Machi, Vivienne. “Private Sector Plays Bigger Role in NATO Cyber Strategy.” *National Defence*, August 2, 2017. https://www.nationaldefensemagazine.org/articles/2017/2/8/private-sector-plays-bigger-role-in-nato-cyber-strategy.

Mackenzie, Paul J. “Cyberspace NOTAM ! : NATO’s Vision and Strategy on the Cyberspace Domain,” *JAPCC.* November 18, 2021. https://www.japcc.org/cyberspace-notam/.

Mahoney, James. “Path Dependence in Historical Sociology.” *Theory and Society* 29, no. 4 (2000): 507–48.

Mahoney, James and Kathleen Thelen. *Explaining Institutional Change: Ambiguity, Agency, and Power*. Cambridge University Press, 2009.

Makortoff, Kalyeena. “NATO Cyber War Drills to Focus on Russia: Expert.” *CNBC*, April 23, 2015. https://www.cnbc.com/2015/04/23/nato-cyber-war-drills-to-focus-on-russia-expert.html.

March, James G., and Johan P. Olsen. “The New Institutionalism: Organizational Factors in Political Life.” *The American Political Science Review* 78, no. 3 (1984): 734–49.

Markoff, John. “Before the Gunfire, Cyberattacks.” *The New York Times*, August 12, 2008. https://www.nytimes.com/2008/08/13/technology/13cyber.html.

Maurer, Tim. *Cyber Mercenaries: The State, Hackers, and Power*. (Cambridge: Cambridge University Press, 2018). https://doi.org/10.1017/9781316422724.

Mavrona, Katerina, and Raluca Csernatoni. “The Artificial Intelligence and Cybersecurity Nexus: Taking Stock of the European Union’s Approach.” *Carnegie Europe*, September 15, 2022. https://carnegieeurope.eu/2022/09/15/artificial-intelligence-and-cybersecurity-nexus-taking-stock-of-european-union-s-approach-pub-87886.

Mazarr, Michael J. “The Essence of the Strategic Competition with China.” *PRISM* 9, no. 1 (2020): 2–21.

———. “Understanding Competition: Great Power Rivalry in a Changing International Order — Concepts and Theories.” RAND Corporation, March 30, 2022. https://www.rand.org/pubs/perspectives/PEA1404-1.html.

McCuen, John J. “Hybrid Wars.” Joint Special Operations University, August 2013. https://www.hsdl.org/?view&did=744761.

Mearsheimer, John J. *The Tragedy of Great Power Politics*. Norton, 2001.

Messmer, Ellen. "Kosovo Cyber-War Intensifies: Chinese Hackers Targeting US Sites, Government Says." *CNN*, May 12, 1999. http://edition.cnn.com/TECH/computing/9905/12/cyberwar.idg/.

Mesterhazy, Attila. “NATO’s Essential Role in the COVID-19 Pandemic.” Report. NATO Parliamentary Assembly, November 22, 2020. https://www.nato-pa.int/document/2020-natos-essential-role-covid-19-pandemic-revised-draft-report-mesterhazy-091-dsc-20-e.

Mhajne, Anwar, Luna K. C, and Crystal Whetstone. “A Call for Feminist Analysis in Cybersecurity: Highlighting the Relevance of the Women, Peace and Security Agenda.” *Women, Peace and Security*, September 17, 2021.

Microsoft. “An Overview of Russia’s Cyberattack Activity in Ukraine.” Digital Security Unit. Microsoft, April 27, 2022. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

———. “Destructive Malware Targeting Ukrainian Organizations.” *Microsoft Security Blog* (blog), January 16, 2022. https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/.

Miller, Maggie. “FBI Sees Spike in Cyber Crime Reports during Coronavirus Pandemic.” *The Hill*, April 16, 2020. https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic/.

Moravcsik, Andrew. “Taking Preferences Seriously: A Liberal Theory of International Politics.” *International Organization* 51, no. 4 (1997): 513–53. https://doi.org/10.1162/002081897550447.

Morgan, Patrick M. *Deterrence Now*. Cambridge Studies in International Relations. Cambridge: Cambridge University Press, 2003. https://doi.org/10.1017/CBO9780511491573.

Morgenthau, Hans J. *Politics Among Nations: The Struggle for Power and Peace*. New York: Knopf, 1948.

Morris, Lyle J., Michael J. Mazarr, Jeffrey W. Hornung, Stephanie Pezard, Anika Binnendijk, and Marta Kepe. “Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War.” RAND Corporation, June 27, 2019. https://www.rand.org/pubs/research_reports/RR2942.html.

Mortimer, Caroline. “NATO to Spend Three Billion on Russia Defence.” The Independent, March 28, 2017. https://www.independent.co.uk/news/world/politics/nato-to-spend-three-billion-euros-on-satellites-cyber-security-and-drones-a7651966.html.

Murray, Williamson, and Peter R. Mansoor. *Hybrid Warfare: Fighting Complex Opponents From The Ancient World To The Present*. New York: Cambridge University Press, 2012. https://assets.cambridge.org/97811070/26087/frontmatter/9781107026087_frontmatter.pdf.

Myrli, Sverre. “NATO and Cyber Defence.” NATO’s Nations and Partners for Peace: Annual Cyberspace Focus Issue, March 2011.

Nakao, Keisuke. “Modeling Deterrence by Denial and by Punishment.” *SSRN Electronic Journal*, 2019. https://doi.org/10.2139/ssrn.3419332.

NATO. “2010 Strategic Concept: Active Engagement, Modern Defence,” November 19, 2010. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf.

———. “Brussels Summit Communiqué.” NATO, June 14, 2021. https://www.nato.int/cps/en/natohq/news_185000.htm.

———. “Brussels Summit Declaration.” NATO, July 11, 2018. https://www.nato.int/cps/en/natohq/official_texts_156624.htm.

———. “Bucharest Summit Declaration.” NATO, April 3, 2008. https://www.nato.int/cps/en/natohq/official_texts_8443.htm.

———. “Chicago Summit Declaration.” NATO, May 20, 2012. https://www.nato.int/cps/en/natohq/official_texts_87593.htm.

———. “Chief Information Officer, Manfred Boudreaux-Dehmer.” NATO, November 15, 2021. http://www.nato.int/cps/en/natohq/who_is_who_188597.htm.

———. “Commitment to Enhance Resilience.” North Atlantic Treaty Organization, July 8, 2016. https://www.nato.int/cps/en/natohq/official_texts_133180.htm.

———. “Consensus Decision-Making at NATO,” October 2, 2020. https://web.archive.org/web/20220225212946/https:/www.nato.int/cps/en/natohq/topics_49178.htm.

———. “Cyber Defence: Next Steps.” NATO, June 10, 2011. http://www.nato.int/cps/en/natohq/news_75358.htm.

———. “Cyber Defence Pledge.” NATO, July 8, 2016. https://www.nato.int/cps/en/natohq/official_texts_133177.htm.

———. “Defence Ministers Approve Cyber Defence Concept and Take next Step in Defence Reform.” NATO, March 10, 2011. https://www.nato.int/cps/en/natohq/news_71432.htm.

———. “Defence Ministers Make Progress on Cyber Protection.” NATO, June 4, 2013. http://www.nato.int/cps/en/natohq/news_101143.htm.

———. “Defence Planning Process.” NATO, March 31, 2022. https://www.nato.int/cps/en/natohq/topics_49202.htm.

———. “Defending the Networks: The NATO Policy on Cyber Defence,” 2011. https://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf.

———. “Emerging and Disruptive Technologies.” NATO, October 17, 2022. https://www.nato.int/cps/en/natohq/topics_184303.htm.

———. “Emerging and Disruptive Technologies.” NATO, December 8, 2022. https://www.nato.int/cps/en/natohq/topics_184303.htm.

———. “Enhanced Cyber Defence Cooperation in the South Caucasus and Black Sea Region.” NATO, July 29, 2015. https://www.nato.int/cps/en/natohq/news_121969.htm.

———. “Enlargement and Article 10.” NATO, July 10, 2022. https://www.nato.int/cps/en/natohq/topics_49212.htm.

———. “Kosovo Air Campaign, March-June 1999.” *NATO*, May 17, 2022. https://www.nato.int/cps/en/natohq/topics_49602.htm.

———. “Largest Ever NATO Cyber Defence Exercise Gets Underway.” NATO, November 18, 2014. https://www.nato.int/cps/en/natohq/news_114902.htm.

———. “Lisbon Summit Declaration.” NATO, November 20, 2010. http://www.nato.int/cps/en/natohq/official_texts_68828.htm.

———. “Madrid Summit Declaration.” NATO, June 29, 2022. https://www.nato.int/cps/en/natohq/official_texts_196951.htm.

———. “Member Countries.” NATO, September 14, 2022. https://www.nato.int/cps/en/natohq/topics_52044.htm.

———. “Membership Action Plan (MAP).” NATO, March 23, 2020. https://web.archive.org/web/20220227230934/https:/www.nato.int/cps/en/natolive/topics_37356.htm.

———. “Men in Black – NATO’s Cybermen.” NATO, April 24, 2015. http://www.nato.int/cps/en/natohq/news_118855.htm.

———. “NATO 2022 Strategic Concept,” June 29, 2022. https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf.

———. “NATO 2022 Strategic Concept,” June 29, 2022. https://www.nato.int/strategic-concept/.

———. “NATO 2030.” Factsheet. NATO, June 2021. https://www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/2106-factsheet-nato2030-en.pdf.

———. “NATO and the European Union Enhance Cyber Defence Cooperation.” NATO, February 10, 2016. http://www.nato.int/cps/en/natohq/news_127836.htm.

———. “NATO Announces 3 Billion EUR Investment in Defence Technology.” NATO, July 26, 2016. http://www.nato.int/cps/en/natohq/news_134254.htm.

———. “NATO Approves 2023 Strategic Direction for New Innovation Accelerator.” NATO, December 12, 2022. https://www.nato.int/cps/en/natohq/news_210393.htm.

———. “NATO Boosts Cyber Defence Investments, Launches Multinational Effort.” NATO, September 22, 2011. https://www.nato.int/cps/en/natohq/news_78418.htm.

———. “NATO Conducts Annual Crisis Management Exercise and Cyber Coalition Exercise.” NATO, November 12, 2012. http://www.nato.int/cps/en/natohq/news_91115.htm.

———. “NATO Cyber Defence Fact Sheet.” NATO, July 2016. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf.

———. “NATO Defence Ministers Adopt New Cyber Defence Policy.” NATO, June 8, 2011. https://www.nato.int/cps/en/natohq/news_75195.htm.

———. “NATO Defence Ministers Will Discuss Situation in Libya and Longer Term Prospects in Middle East.” NATO, March 7, 2011. http://www.nato.int/cps/en/natohq/news_71277.htm.

———. “NATO Holds Annual Cyber Exercise in Estonia.” NATO, December 2, 2016. http://www.nato.int/cps/en/natohq/news_138674.htm.

———. “NATO Rapid Reaction Team to Fight Cyber Attack.” NATO, March 13, 2012. https://www.nato.int/cps/en/natohq/news_85161.htm.

———. “NATO Rapid Reaction Team to Fight Cyber Attack.” NATO. Accessed September 11, 2022. https://www.nato.int/cps/en/natohq/news_85161.htm.

———. “NATO Supports Jordan’s National Cyber Defence Strategy.” NATO, n.d. https://www.nato.int/cps/en/natohq/news_146287.htm.

———. “NATO Trains Iraqi Experts in Cyber Defence.” NATO, November 21, 2016. https://www.nato.int/cps/en/natohq/news_139179.htm.

———. “NATO’s Military Presence in the East of the Alliance.” NATO, July 8, 2022. https://www.nato.int/cps/en/natohq/topics_136388.htm.

———. “North Atlantic Council Statement Following the Announcement by the United States of Actions with Regard to Russia.” NATO, April 15, 2021. https://www.nato.int/cps/en/natohq/official_texts_183168.htm.

———. “Prague Summit Declaration.” NATO, November 21, 2002. http://www.nato.int/cps/en/natohq/official_texts_19552.htm.

———. “Press Conference by NATO Secretary General Jens Stoltenberg Following the Meeting of the NATO-Ukraine Commission.” NATO, November 26, 2018. http://www.nato.int/cps/en/natohq/opinions_160789.htm.

———. “Probable Data Breach from a NATO-Related Website.” NATO, June 23, 2011. https://www.nato.int/cps/en/natohq/news_75729.htm.

———. “Report of the Committee of Three on Non-Military Cooperation in NATO.” NATO, December 13, 1956. https://www.nato.int/cps/en/natohq/official_texts_17481.htm.

———. “Riga Summit Declaration.” NATO, November 29, 2006. https://www.nato.int/cps/en/natohq/official_texts_37920.htm.

———. “Statement by the NATO Secretary General on Cyber Attacks against Ukraine.” NATO, January 14, 2022. https://www.nato.int/cps/en/natohq/news_190850.htm.

———. “Statement by the North Atlantic Council in Solidarity with Those Affected by Recent Malicious Cyber Activities Including the Microsoft Exchange Server Compromise.” NATO, July 19, 2021. https://www.nato.int/cps/en/natohq/news_185863.htm.

———. “Statement by the North Atlantic Council on Crimea.” NATO, March 18, 2019. https://www.nato.int/cps/en/natohq/news_164656.htm.

———. “Statement by the North Atlantic Council on Russia’s Attack on Ukraine.” NATO, February 24, 2022. https://www.nato.int/cps/en/natohq/official_texts_192404.htm.

———. “Steadfast Jazz 2013.” NATO, December 15, 2015. http://www.nato.int/cps/en/natohq/103267.htm.

———. “Strasbourg / Kehl Summit Declaration.” NATO, April 4, 2009. http://www.nato.int/cps/en/natohq/news_52837.htm.

———. “Summary of NATO’s Data Exploitation Framework Policy.” NATO, October 22, 2023. https://www.nato.int/cps/en/natohq/official_texts_210002.htm.

———. “Summary of the NATO Artificial Intelligence Strategy.” NATO, October 22, 2021. https://www.nato.int/cps/en/natohq/official_texts_187617.htm.

———. “System/Network Administrators from the Former Yugoslav Republic of Macedonia Train in Cyber Defence.” NATO, April 17, 2013. https://www.nato.int/cps/en/natohq/news_99718.htm.

———. “The North Atlantic Treaty.” NATO, April 4, 1949. https://www.nato.int/cps/en/natohq/official_texts_17120.htm.

———. “The Situation In and Around Kosovo.” NATO Press Release, June 29, 2011. https://web.archive.org/web/20110629141056/http://www.nato.int/docu/pr/1999/p99-051e.htm.

———. “Vilnius Summit Communiqué Issued by NATO Heads of State and Government (2023).” NATO, July 11, 2023. https://www.nato.int/cps/en/natohq/official_texts_217320.htm.

———. “Wales Summit Declaration.” NATO, September 5, 2014. https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

———. “Warsaw Summit Communiqué.” NATO, July 9, 2016. https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

———. “White-Hat Hacker Fights Cyber Intrusions on NATO Systems.” NATO, June 3, 2013. https://www.nato.int/cps/en/natohq/news_100992.htm.

NATO JALLC. “Lessons Learned,” 2021. https://www.jallc.nato.int/activities/lessons-learned.

NATO PA. “NATO PA.” Accessed March 28, 2023. https://www.nato-pa.int/content/finland-sweden-accession.

NATO Parliamentary Assembly. “Ratification of Finland and Sweden’s Accession to NATO.” Finland and Sweden Accession, March 27, 2023. https://www.nato-pa.int/content/finland-sweden-accession#:~:text=RATIFICATION%20OF%20FINLAND%20AND%20SWEDEN'S%20ACCESSION%20TO%20NATO&text=NATO%20Heads%20of%20State%20and,after%20completion%20of%20accession%20talks.

NATO Standardization Office. “Cyber Space.” In *NATO Glossary of Terms and Definitions (English and French)*, 37, December 2021. https://standards.globalspec.com/std/14486494/AAP-06.

———. “Cyber Space Attack.” In *NATO Glossary of Terms and Definitions (English and French)*, 37, December 2021. https://standards.globalspec.com/std/14486494/AAP-06.

———. “Defensive Cyberspace Operation.” In *NATO Glossary of Terms and Definitions (English and French)*, 40, December 2021. https://standards.globalspec.com/std/14486494/AAP-06.

———. “Deterrence.” In *NATO Glossary of Terms and Definitions (English and French)*, 42, December 2021. https://standards.globalspec.com/std/14486494/AAP-06.

———. “Hybrid Threats.” In *NATO Glossary of Terms and Definitions (English and French)*, 65, December 2021. https://standards.globalspec.com/std/14486494/AAP-06.

———. “Offensive Cyberspace Operation.” In *NATO Glossary of Terms and Definitions (English and French)*, 94, December 2021. https://standards.globalspec.com/std/14486494/AAP-06.

NCIA. "NATO Launches Industry Cyber Partnership." forum.ncia.nato.int, September 18, 2014. https://www.ncia.nato.int/about-us/newsroom/nato-launches-industry-cyber-partnership.html.

———. “NATO Opens Flagship Cyber Event with Vision for the Future.” NCIA, September 7, 2016. https://www.ncia.nato.int/about-us/newsroom/nato-opens-flagship-cyber-event-with-vision-for-the-future.html.

Nemeth, William J. “Future War and Chechnya: A Case for Hybrid Warfare.” *Naval Postgraduate School*, June 2002. https://core.ac.uk/download/pdf/36699567.pdf.

Niiler, Eric. “The US Takes On the World in NATO’s Cyber War Games.” *Wired*, April 29, 2017. https://www.wired.com/2017/04/us-takes-world-natos-cyber-war-games/.

NIST. “Cybersecurity Framework.” NIST, November 12, 2013. https://www.nist.gov/cyberframework.

———. “Cyberspace.” In *Computer Security Resource Centre*, n.d. https://csrc.nist.gov/glossary/term/cyberspace.

NIST. “Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.” Gaithersburg, MD: National Institute of Standards and Technology, April 16, 2018.

Norton-Taylor, Richard. “Strategic Defence Review to Prioritise Cyber Security.” *The Guardian*, October 13, 2010, sec. Politics. https://www.theguardian.com/politics/2010/oct/13/strategic-defence-review-cyber-security.

Nye, Joseph S. “Deterrence and Dissuasion in Cyberspace.” *International Security* 41, no. 3 (January 2017): 44–71. https://doi.org/10.1162/ISEC_a_00266.

O’Neill, Patrick Howell. “NATO Will Establish New Cyber Command Centers.” CyberScoop, November 9, 2017. https://www.cyberscoop.com/nato-cyber-command-centers/.

Open Data Commons. “Open Data Commons Open Database License,” n.d. https://opendatacommons.org/licenses/odbl/.

OpenStreetMap. “OpenStreetMap Copyright.” OpenStreetMap, n.d. https://www.openstreetmap.org/copyright.

OpenStreetMap Foundation. “Licence/Attribution Guidelines,” n.d. https://wiki.osmfoundation.org/wiki/Licence/Attribution_Guidelines#Why_attribution_is_important.

Paul, Kari. “‘Catastrophic’ Cyberwar between Ukraine and Russia Hasn’t Happened (yet), Experts Say.” *The Guardian*, March 9, 2022, sec. Technology. https://www.theguardian.com/technology/2022/mar/09/catastrophic-cyber-war-ukraine-russia-hasnt-happened-yet-experts-say.

Paulauskas, Kęstutis. “On Deterrence.” *NATO Review*, August 5, 2016. https://www.nato.int/docu/review/articles/2016/08/05/on-deterrence/index.html.

Peters, Mark. “Cyber Enhanced Sanction Strategies: Do Options Exist?” *Journal of Law & Cyber Warfare* 6, no. 1 (2017): 95–154.

Pierson, Paul. “Increasing Returns, Path Dependence, and the Study of Politics.” *The American Political Science Review* 94, no. 2 (2000): 251–67. https://doi.org/10.2307/2586011.

Ranger, Steve. “NATO Updates Cyber Defence Policy as Digital Attacks Become a Standard Part of Conflict.” ZDNET, June 30, 2014. https://www.zdnet.com/article/nato-updates-cyber-defence-policy-as-digital-attacks-become-a-standard-part-of-conflict/.

Raska, Michael. “Strategic Competition for Emerging Military Technologies: Comparative Paths and Patterns.” *PRISM* 8, no. 3 (2019): 64–81.

Reggio, Gianna. “Entities: An Institution for Dynamic Systems.” In *Recent Trends in Data Type Specification*, edited by H. Ehrig, K. P. Jantke, F. Orejas, and H. Reichel, 534:246–65. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 1991. https://doi.org/10.1007/3-540-54496-8_13.

Republic of Türkiye. "Implementation of the Montreux Convention." Republic of Türkiye Ministry of Foreign Affairs, n.d. https://www.mfa.gov.tr/implementation-of-the-montreux-convention.en.mfa.

Reuters. “Turkish Parliament Ratifies Finland’s NATO Accession as Sweden Kept Waiting,” March 31, 2023. https://www.reuters.com/world/europe/turkish-parliament-approves-finlands-nato-accession-2023-03-30/.

———. “Ukraine to Join NATO Cyber Defence Centre as ‘Contributing Participant.’” *Reuters*, March 4, 2022, sec. World. https://www.reuters.com/world/ukraine-join-nato-cyber-defence-centre-contributing-participant-2022-03-04/.

———. "US Firm Blames Russian 'Sandworm' Hackers for Ukraine Outage." *Reuters*, January 8, 2016, sec. Technology News. https://www.reuters.com/article/us-ukraine-cybersecurity-sandworm-idUSKBN0UM00N20160108.

Rid, Thomas. "Escalation, Not Deterrence." *Medium* (blog), July 2, 2014. https://medium.com/@ridt/escalation-not-deterrence-f0ddf055d4c7.

Rid, Thomas, and Ben Buchanan. "Attributing Cyber Attacks." *Journal of Strategic Studies* 38, no. 1–2 (January 2, 2015): 4–37. https://doi.org/10.1080/01402390.2014.977382.

Rixen, Thomas, Lora Anne Viola, and Michael Zurn, eds. *Historical Institutionalism and International Relations: Explaining Institutional Development in World Politics*. (Oxford ; New York, NY: Oxford University Press, 2016.) https://www.amazon.ca/Historical-Institutionalism-International-Relations-Institutional/dp/0198779623.

Robinson, Neil. "NATO: Changing Gear on Cyber Defence." *NATO Review*, June 8, 2016. https://www.nato.int/docu/review/articles/2016/06/08/nato-changing-gear-on-cyber-defence/index.html.

———. "Spending for Success on Cyber Defence." *NATO Review*, April 6, 2017. https://www.nato.int/docu/review/articles/2017/04/06/spending-for-success-on-cyber-defence/index.html.

Roepke, Wolf-Diether, and Hasit Thankey. "Resilience: The First Line of Defence." *NATO Review*, February 27, 2019. https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html.

Rosenfeld, Everett. "NATO Rattles Cybersabers—but Experts Have Doubts." *CNBC*, September 9, 2014. https://www.cnbc.com/2014/09/09/nato-cyberdefense-a-military-response-to-virtual-warfare.html.

Sanger, David E. "Obama Ordered Wave of Cyberattacks Against Iran." *The New York Times*, June 1, 2012. https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=1.

SC Media. "NATO to Spend €70 Million on 'Cyber-Refresh.'" SC Media, August 24, 2016. https://www.scmagazine.com/news/strategy/nato-to-spend-e70-million-on-cyber-refresh.

Schmitt, Michael N. "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed." *Harvard Law Journal* 54 (December 2012): 13–37.

Schmitt, Michael N. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge: Cambridge University Press, 2017. https://doi.org/10.1017/9781316822524.

Schmitt, Michael N. "Taming the Lawless Void: Tracking the Evolution of International Law Rules for Cyberspace." *Texas National Security Review* 3, no. 3 (Autumn 2020): 32–47.

Schmitt, Michael N, and Liis Vihul. "International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms." Just Security, June 30, 2017. https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/.

Schmitt, Michael N., and Liis Vihul. "Respect for Sovereignty in Cyberspace." SSRN Scholarly Paper. Rochester, NY, November 3, 2017. https://papers.ssrn.com/abstract=3180669.

Scott, Claudia. "The Choice of Formal Policy Analysis Methods." In *Routledge Handbook of Comparative Policy Analysis*. Routledge, 2017. https://www.taylorfrancis.com/chapters/edit/10.4324/9781315660561-3/choice-formal-policy-analysis-methods-claudia-scott.

Shea, Jamie. "Cyberspace as a Domain of Operations: What Is NATO's Vision and Strategy?" *MCU Journal* 9, no. 2 (December 21, 2018): 133–50. https://doi.org/10.21140/mcuj.2018090208.

———. "How Is NATO Meeting the Challenge of Cyberspace." *PRISM* 7, no. 2 (December 21, 2017). https://cco.ndu.edu/PRISM-7-2/Article/1401835/how-is-nato-meeting-the-challenge-of-cyberspace/.

———. “NATO in the Era of Global Complexity: New Perspectives on Shared Security NATO’s Next 70 Years.” Carnegie Europe, November 28, 2019. https://carnegieeurope.eu/2019/11/28/nato-in-era-of-global-complexity-pub-80417.

———. “NATO Press Conference: NATO’s Role in Kosovo.” *NATO HQ Press Release*, March 31, 1999. https://www.nato.int/kosovo/press/p990331a.htm.

———. “NATO to Unveil Cyber-Defence Strategy Fit for Changing Times.” The Conversation, September 4, 2014. https://theconversation.com/nato-to-unveil-cyber-defence-strategy-fit-for-changing-times-31143.

Erika Simpson, “Game Theory and Peace Research: Professor Anatol Rapoport’s Contributions,” *In Factis Pax* 12, no. 1 (2018): 38–58.

Smalley, Suzanne. “Nakasone Says Cyber Command Did Nine ‘hunt Forward’ Ops Last Year, Including in Ukraine.” CyberScoop, May 4, 2022. https://www.cyberscoop.com/nakasone-persistent-engagement-hunt-forward-nine-teams-ukraine/.

Smeets, Max. “NATO Members’ Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis.” In *2019 11th International Conference on Cyber Conflict (CyCon)*, 900:1–15, 2019. https://doi.org/10.23919/CYCON.2019.8756634.

———. *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force*. Oxford University Press, 2022.

Smeets, Max, Robert Chesney, and Monica Kaminska. “The Transatlantic Dialogue on Military Cyber Operations-Amsterdam.” Lawfare, December 5, 2019. https://www.lawfareblog.com/workshop-report-transatlantic-dialogue-military-cyber-operations-amsterdam.

Smeets, Max, and Robert Chesney. *Deter, Disrupt, or Deceive: Assessing Cyber Conflict as an Intelligence Contest*. Washington, DC: Georgetown University Press, 2023.

Smith, Brad. "The Need for a Digital Geneva Convention." *Microsoft On the Issues* (blog), February 14, 2017. https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

Snyder, Glenn. "Deterrence: A Theoretical Introduction." In *Theories of Peace and Security: A Reader in Contemporary Strategic Thought*, edited by John Garnett, 106–12. London: Palgrave Macmillan UK, 1970. https://doi.org/10.1007/978-1-349-15376-3_6.

———. *Deterrence and Defense*. Princeton: Princeton University Press, 2016. https://press.princeton.edu/books/hardcover/9780691652092/deterrence-and-defense.

Soesanto, Stefan. "When Does a 'Cyber Attack' Demand Retaliation? NATO Broadens Its View." *Defense One*, June 30, 2021. https://www.defenseone.com/ideas/2021/06/when-does-cyber-attack-demand-retaliation-nato-broadens-its-view/175028/.

Soifer, Hillel. "The Causal Logic of Critical Junctures." *Comparative Political Studies* 45, no. 12 (2012): 1572–97.

Somin, Ilya. "Russian Government Agency Reveals Fraudulent Nature of the Crimean Referendum Results." *The Washington Post*, May 6, 2014. https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/05/06/russian-government-agency-reveals-fraudulent-nature-of-the-crimean-referendum-results/.

Spivak, Adam Aliano, Russell. "Ukraine Symposium - The Montreux Convention and Turkey's Impact on Black Sea Operations." Lieber Institute West Point, April 25, 2022. https://lieber.westpoint.edu/montreux-convention-turkeys-impact-black-sea-operations/.

Sprenger, Sebastian. “NATO to Improve Cyber Defense in Bid to Boost Alliance Resilience.” Defense News, April 15, 2021. https://www.defensenews.com/global/europe/2021/04/15/nato-checks-cyber-defense-under-bid-to-boost-alliance-resilience/.

Stevens, Yuan, Stephanie Tran, and Ryan Atkinson. “See Something, Say Something? Coordinating the Disclosure of Security Vulnerabilities in Canada’s Infrastructure.” In *2021 IEEE International Symposium on Technology and Society (ISTAS)*, 1–5, 2021.

Stronski, Paul. “What Is Russia Doing in the Black Sea?” Carnegie Endowment for International Peace, May 20, 2021. https://carnegieendowment.org/2021/05/20/what-is-russia-doing-in-black-sea-pub-84549.

TASS. “Russian Defense Ministry Warns about Strikes Being Prepared on Military Sites in Kiev.” *TASS Russian News Agency*, March 1, 2022. https://web.archive.org/web/20220301133913/https:/tass.com/defense/1414199.

Tate, Ryan, and Chad Bates. “Deterrence Thru Transparent Offensive Cyber Persistence.” *The Cyber Defense Review* 7, no. 4 (2022): 227–46.

Taillat, Stéphane. “Disrupt and Restraint: The Evolution of Cyber Conflict and the Implications for Collective Security.” *Contemporary Security Policy* 40, no. 3 (July 3, 2019): 368–81.

The Economist. “Why the Black Sea Matters to Russia.” *The Economist*, May 6, 2022. https://www.economist.com/the-economist-explains/2022/05/06/why-the-black-sea-matters-to-russia.

Theiler, Olaf. “New Threats: The Cyber-Dimension.” *NATO Review*, September 4, 2011. https://www.nato.int/docu/review/articles/2011/09/04/new-threats-the-cyber-dimension/index.html.

Thelen, Kathleen. "Historical Institutionalism in Comparative Politics." *Annual Review of Political Science* 2, no. 1 (1999): 369–404.

Tigner, Brooks. "NATO Brings Two More Players into Its Cyberpartnership with Industry." *Janes Defence Industry*, March 2, 2016.

———. "NATO Carries Cyber Operations, Security to Newlevels as Command Structure Reformed." *Jane's Defence Weekly*, February 21, 2018.

———. "NATO Cyber Umbrella to Coalesce in November." *Jane's Defence Weekly*, July 17, 2013.

———. "SHAPE's Cyber Defence Unit Now Trialling Three-Nation Cyber Incident System." *Jane's Defence Weekly*, March 2, 2017.

Toole, Laurence J. "Treating Networks Seriously: Practical and Research-Based Agendas in Public Administration." *Public Administration Review* 57, no. 1 (January 1, 1997): 45–52.

Traynor, Ian. "Russia Accused of Unleashing Cyberwar to Disable Estonia." *The Guardian*, May 17, 2007, sec. World news. https://www.theguardian.com/world/2007/may/17/topstories3.russia.

Tunnicliffe, Andrew. "NATO's Locked Shield Exercise: A Cybersecurity Success?" *Army Technology*, August 20, 2018. https://www.army-technology.com/analysis/natos-locked-shield-exercise-cybersecurity-success/.

UK FCDO. "Russia behind Cyber-Attack with Europe-Wide Impact an Hour before Ukraine Invasion." Press Release, May 10, 2022. https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion.

UK NCSC. "Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed." United Kingdom Nation Cyber Security Centre, October 3, 2018. https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed.

Underwood, Kimberly. “Initial Cyber Hardening Has Helped Ukraine.” AFCEA International, March 15, 2022. https://www.afcea.org/signal-media/cyber/initial-cyber-hardening-has-helped-ukraine.

UNGA. “Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.” United Nations General Assembly, June 24, 2013. https://undocs.org/A/68/98.

———. “Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.” United Nations General Assembly, July 22, 2015. https://undocs.org/A/70/174.

UNIDIR. "Cyber Policy Portal." United Nations Institute for Disarmament Research. Accessed March 23, 2023. https://cyberpolicyportal.org/.

United States Cyber Command. “Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command.” United States Cyber Command, April 2018. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

United States Department of Defence. “The Department of Defence Cyber Strategy.” United States Department of Defence, April 2015.

United Nations Officer of Disarmament Affairs (UNODA). “Developments in the Field of Information and Telecommunications in the Context of International Security.” United Nations Officer of Disarmament Affairs, n.d. https://www.un.org/disarmament/ict-security/.

———. “Open-Ended Working Group.” UN Office for Disarmament Affairs, December 2018. https://www.un.org/disarmament/open-ended-working-group/.

Vasovic, Aleksandar. “Russian Troops Seize Ukraine Marine Base In Crimea.” Business Insider, March 24, 2014. https://www.businessinsider.com/r-russian-troops-seize-ukraine-marine-base-in-crimea-soldiers-2014-24.

Vercellone, Chiara. “More Countries Participate in International Cyber Exercise.” C4ISRNet, January 29, 2020. https://www.c4isrnet.com/newsletters/daily-brief/2020/01/27/more-countries-participate-in-natos-cyber-exercise/.

Verton, Dan. “Serbs Launch Cyberattack on NATO.” FCW, April 4, 1999. https://fcw.com/1999/04/serbs-launch-cyberattack-on-nato/195288/.

Waltz, Kenneth N. *Theory of International Politics*. Addison-Wesley, 1979.

Wake, Damon. “NATO Exercises Cyber Defences as Threat Grows.” *Yahoo News*, November 30, 2018. https://sg.news.yahoo.com/nato-exercises-cyber-defences-threat-grows-161421627.html.

Weber, Valentin. “The Illusion of ‘Responsible’ Cyber Offense.” German Council on Foreign Relations, October 27, 2021. https://dgap.org/en/research/publications/illusion-responsible-cyber-offense.

Wenger, Etienne. *Communities of Practice: Learning, Meaning, and Identity*. Communities of Practice: Learning, Meaning, and Identity. New York, NY, US: Cambridge University Press, 1998.

Wentworth, Travis. “How Russia May Have Attacked Georgia’s Internet.” Newsweek, August 22, 2008. https://www.newsweek.com/how-russia-may-have-attacked-georgias-internet-88111.

Whitney, Lance. “Online Activists Fighting to Keep WikiLeaks Alive.” CNET, December 6, 2010. https://www.cnet.com/tech/tech-industry/online-activists-fighting-to-keep-wikileaks-alive/.

Williams, Brad D. “CYBERCOM Has Conducted ‘hunt-Forward’ Ops in 14 Countries, Deputy Says.” *Breaking Defense*, November 10, 2021. https://breakingdefense.com/2021/11/cybercoms-no-2-discusses-hunt-forward-space-cybersecurity-china/.

Wilner, Alex, and Casey Babb. “New Technologies and Deterrence: Artificial Intelligence and Adversarial Behaviour.” In *NL ARMS Netherlands Annual Review of Military Studies 2020: Deterrence in the 21st Century—Insights from Theory and Practice*, edited by Frans Osinga and Tim Sweijs, 401–17. NL ARMS. The Hague: T.M.C. Asser Press, 2021.

World News. “NATO to Set up Rapid Reaction Teams against Cyber Threats.” Hürriyet Daily News, June 5, 2013. https://www.hurriyetdailynews.com/nato-to-set-up-rapid-reaction-teams-against-cyber-threats-48292.

Wu, Qi, Qiang Li, Dong Guo, and Xiangyu Meng. “Exploring the Vulnerability in the Inference Phase of Advanced Persistent Threats.” *International Journal of Distributed Sensor Networks* 18, no. 3 (March 1, 2022): 15501329221080416. https://doi.org/10.1177/15501329221080417.

YLE News. "Helsinki to Host Hub Aimed at Curbing Cyber Warfare Threats." *YLE News*, November 21, 2016. http://yle.fi/uutiset/osasto/news/helsinki_to_host_hub_aimed_at_curbing_cyber_warfare_threats/9307244.

8.2 – Western Research Ethics Board Approval Letters

8.2.1 Western Research Ethics Board Initial Approval, February 17, 2021

Western Research

Date: 17 February 2021

To: Dr. Erika Simpson

Project ID: 118236

Study Title: Interviews for Research on NATO's Cyber Defence Strategy, Deterrence, and Hybrid Warfare

Short Title: Interviews on NATO's Cyber Defence Strategy

Application Type: NMREB Initial Application

Review Type: Delegated

Full Board Reporting Date: 05/Mar/2021

Date Approval Issued: 17/Feb/2021 22:54

REB Approval Expiry Date: 17/Feb/2022

Dear Dr. Erika Simpson

The Western University Non-Medical Research Ethics Board (NMREB) has reviewed and approved the WREM application form for the above mentioned study, as of the date noted above. NMREB approval for this study remains valid until the expiry date noted above, conditional to timely submission and acceptance of NMREB Continuing Ethics Review.

This research study is to be conducted by the investigator noted above. **All other required institutional approvals and mandated training must also be obtained prior to the conduct of the study.**

Documents Approved:

Document Name	Document Type	Document Date	Document Version
Interview Guide	Interview Guide	18/Dec/2020	1
Third Party Recruitment	Recruitment Materials	18/Dec/2020	1
Clean Recruitment Email	Recruitment Materials	02/Feb/2021	4
Clean Letter of Information and Consent	Written Consent/Assent	02/Feb/2021	4
Clean Letter of Information and Consent	Verbal Consent/Assent	02/Feb/2021	4

No deviations from, or changes to the protocol should be initiated without prior written approval from the NMREB, except when necessary to eliminate immediate hazard(s) to study participants or when the change(s) involves only administrative or logistical aspects of the trial.

The Western University NMREB operates in compliance with the Tri-Council Policy Statement Ethical Conduct for Research Involving Humans (TCPS2), the Ontario Personal Health Information Protection Act (PHIPA, 2004), and the applicable laws and regulations of Ontario. Members of the NMREB who are named as Investigators in research studies do not participate in discussions related to, nor vote on such studies when they are presented to the REB. The NMREB is registered with the U.S. Department of Health & Human Services under the IRB registration number IRB 00000941.

Please do not hesitate to contact us if you have any questions.

Sincerely,

Ms. Katelyn Harris , Research Ethics Officer on behalf of Dr. Randal Graham, NMREB Chair

Note: This correspondence includes an electronic signature (validation and approval via an online system that is compliant with all regulations).

8.2.2 Western Research Ethics Board Updated Approval, February 17, 2023

Western Research

Date: 7 February 2023

To: Dr. Erika Simpson

Project ID: 118236

Study Title: Interviews for Research on NATO's Cyber Defence Strategy, Deterrence, and Hybrid Warfare

Application Type: Continuing Ethics Review (CER) Form

Review Type: Delegated

Date Approval Issued: 07/Feb/2023 22:11

REB Approval Expiry Date: 17/Feb/2024

Dear Dr. Erika Simpson,

The Western University Non-Medical Research Ethics Board has reviewed this application. This study, including all currently approved documents, has been re-approved until the expiry date noted above.

REB members involved in the research project do not participate in the review, discussion or decision.

The Western University NMREB operates in compliance with the Tri-Council Policy Statement Ethical Conduct for Research Involving Humans (TCPS2), the Ontario Personal Health Information Protection Act (PHIPA, 2004), and the applicable laws and regulations of Ontario. Members of the NMREB who are named as Investigators in research studies do not participate in discussions related to, nor vote on such studies when they are presented to the REB. The NMREB is registered with the U.S. Department of Health & Human Services under the IRB registration number IRB 00000941.

Please do not hesitate to contact us if you have any questions.

Sincerely,

The Office of Human Research Ethics

Note: This correspondence includes an electronic signature (validation and approval via an online system that is compliant with all regulations).

Page 1 of 1

8.3 – Western Research Ethics Board Approved Interview Questions

1. How does NATO's Cyber Defence Strategy utilize deterrence as an extension of its Strategic Security Doctrine?
2. How is deterrence applied in the cyber domain, and is cyber deterrence an appropriate strategy for addressing the challenges posed in this threat landscape?
3. Has NATO's implementation of deterrence in the cyber domain changed how the Alliance applies deterrence?
4. How do you respond to critical challenges of classical deterrence in the cyber domain?
5. Is Article V applicable in the cyber domain, and how is it applied?
6. Given the unique nature of threats in the cyber domain, do cyber weapons require a nonconventional threshold for triggering Article V? Is such a threshold appropriate?
7. If triggering Article V based on attacks in the cyber domain is based on a case-by-case basis, what are some central characteristics that would trigger Article V in the cyber domain?
8. What is the relation between the NATO Cyber Defence Pledge and individual member state national cyber defence strategies? How does NATO promote member states to align national cyber defence policies with the consensus-based pledge?
9. Does NATO's Cyber Defence Strategy set policy benchmarks for states to abide by? What are these benchmarks, and how is national implementation of them enforced?
10. How does NATO assess the cyber capabilities of member states? Is there a specific international framework that NATO uses to quantify the maturity of HQ and member state national cyber defence policy? Such as the frameworks outlined by NIST, ISO, or ENISA.

8.4 – List of Research Participants

Last Name	First Name	Title	Unit	Location	Date
Alberque	William	Director (2012-2020)	Arms Control, Disarmament and WMD Non-Proliferation NATO	Video Call	August 2, 2022
Angell	David	Ambassador and Permanent Representative	Joint Delegation of Canada to NATO, Government of Canada	Brussels, Belgium	January 24, 2022
Black	Dan	Principal Threat Analyst	Cyber Threat Assessment Branch, Joint Intelligence and Security Division, NATO	Brussels, Belgium	March 9, 2022
Brust	Frederick	Policy Officer	Enablement and Resilience Section, Defence Policy and Planning Division, NATO	Brussels, Belgium	March 7, 2022
Cairns	Julia	Policy Officer	Enablement and Resilience Section, Defence Policy and Planning Division, NATO	Brussels, Belgium	March 7, 2022
Di Paolo	Marc	Director	Defence, Institution, and Capacity Building, Operations Division, NATO	Brussels, Belgium	March 3, 2022

Last Name	First Name	Title	Unit	Location	Date
Lacko	Larysa	Policy Officer	Counter Hostile Information, Strategic Communications, Public Diplomacy Division, NATO	Brussels, Belgium	March 9, 2022
Liflander	Christian-Marc	Section Head	Cyber and Hybrid Policy Section, Emerging Security Challenges Division, NATO	Video Call	July 5, 2022
Metka	Stefanie	Branch Head	Cyber Threat Assessment Branch, Joint Intelligence and Security Division, NATO	Brussels, Belgium	March 4, 2022
Minnion	Megan	Policy Officer	Defence and Related Capacity Building, Operations Division, NATO	Brussels, Belgium	March 1, 2022
Prata	Francisco	Policy Officer	Climate and Energy Security Section, Emerging Security Challenges Division, NATO	Brussels, Belgium	March 8, 2022
Richmond	Iain	Policy Officer	Crisis Response Systems and Exercises, Operations Division, NATO	Brussels, Belgium	March 3, 2022

Last Name	First Name	Title	Unit	Location	Date
Roberts	Clare	Policy Officer	Cyber and Hybrid Policy Section, Emerging Security Challenges Division, NATO	Video Call	July 15, 2022
Robinson	Neil	Policy Officer	Data and AI Policy Unit, Emerging Security Challenges Division, NATO	Brussels, Belgium	March 1, 22
Rodriguez-Arroyo	Jose	Section Head	CIS and Cyber Capabilities Branch, NATO Office of Resources, NATO	Brussels, Belgium	March 2, 22
Ruehle	Michael	Section Head	Climate and Energy Security Section, Emerging Security Challenges Division, NATO	Video Call	July 28, 2022
Shea	Jamie	Deputy Assistant Secretary General (2010-2018)	Emerging Security Challenges Division, NATO	Video Call	July 28, 2022
Slack	Chelsey	Deputy Section Head	Cyber and Hybrid Policy Section, Emerging Security Challenges Division, NATO	Video Call	July 19, 2022

Last Name	First Name	Title	Unit	Location	Date
Stanley-Lockman	Zoe	Policy Officer	Innovation Unit, Emerging Security Challenges Division, NATO	Brussels, Belgium	March 2, 2022
Thankey	Hasit	Section Head	Enablement and Resilience Section, Defence Policy and Planning Division, NATO	Brussels, Belgium	March 4, 2022
Tsangaros	Spyridon	Information Management Officer	Archives and Information Management, Executive Management Division, NATO	Brussels, Belgium	March 8, 2022

8.5 – Phases A-D Collected Critical Junctures and NATO Policy, 1999-2022

8.5.1 Phase A

Kosovo, 1999

Critical Juncture 1 (Phase A)	Kosovo 1999
Events	Cyber attacks targeted NATO during Operation Allied Force.
Critical Juncture	Unprecedented attacks demonstrated the value and dangers of cyber capabilities.
NATO Policy or Institutional Change	The first cyber language was included in the 2002 Prague Summit Communiqué. The additional cyber language was added at the 2006 Riga Summit.

8.5.2 Phase B

Estonia, 2007

Critical Juncture 2 (Phase B)	Estonia 2007
Events	Cyber attacks targeted Estonia after the removal of a Soviet-era statue.
Critical Juncture	Unprecedented cyber incidents included website defacements and disruptions, temporarily taking Estonian web pages offline.
NATO Policy or Institutional Change	The first cyber language was included in the 2002 Prague Summit Communiqué, and additional cyber language was added at the 2006 Riga Summit.

Georgia, 2008

Critical Juncture 3 (Phase B)	Georgia 2008
Events	Cyber attacks targeted Georgia, which shaped the threat landscape for Russia's conventional invasion in August 2008.
Critical Juncture	Unprecedented coordination between cyber capabilities and conventional forces was observed as a dangerous use case for the first time.
NATO Policy or Institutional Change	Major NATO cyber institutions were created in 2008, around the time of the cyber incidents in Georgia. NATO Cyber Coalition exercise took place for the first time. At the 2009 Strasburg/Kehl Summit, Allies agreed to strengthen cyber defence collaboration.

Iran, 2010

Critical Juncture 4 (Phase B)	Stuxnet 2010
Events	Stuxnet is launched on the Iranian nuclear enrichment facility in Natanz.
Critical Juncture	The unprecedented cyber weapon demonstrated that malicious software caused real-world physical destruction to critical infrastructure.
NATO Policy or Institutional Change	At the 2010 Lisbon Summit, NATO agreed on a Strategic Concept. Stuxnet was a major cyber attack in the threat environment in the months of debates leading up to the Summit. The precedents set by Stuxnet influenced decision-makers to develop policy, given advancements in cyber weapons to cause physical destruction.

NATO 2010 Strategic Concept

Internal Adjustment (Phase B)	NATO 2010 Strategic Concept
Events	The Alliance agreed to a new Strategic Concept at the Lisbon Summit.
Internal Adjustment	The document included language for the first time on cyber security and related threats.
NATO Policy or Institutional Change	Cyber-related language in the Strategic Concept and Summit Documents opened the door to significant funding, investment, and other institutional policy initiatives in 2011 and 2012. The cyber language signalled that NATO acknowledged its interests in cyberspace to develop defensive capabilities.

8.5.3 Phase C

Crimea 2014

Critical Juncture 6 (Phase C)	Crimea, 2014
Events	Russia's annexation of Crimea involved significant cyber incidents and hybrid threats.
Critical Juncture	Unprecedented events involved cyber capabilities and other unconventional tactics that attained strategic objectives.
NATO Policy or Institutional Change	Policy changes at the NATO 2014 Wales Summit, where cyber-attacks became part of Article 5. Further changes at the 2016 Warsaw Summit included the formation of NATO Enhanced Forward Presence.

Ukraine 2015-2016

Critical Juncture 7 (Phase C)	Ukraine, 2015-2016
Events	Ukrainian energy plant Ukrenegro was targeted by Russian BlackEnergy malware to take power offline.
Critical Juncture	The unprecedented use of malware to target critical national infrastructure in the energy sector took power offline in numerous cases to cause further disruption.
NATO Policy or Institutional Change	The European Union passed significant legislation on cyber reporting requirements. NATO established an Industry Cyber Partnership—increased cyber exercises with affiliated Centres of Excellence.

United States, 2016

Omitted Critical Juncture (Space Limitations)	Democratic National Committee, 2016
Events	Hack and leak operations conducted by Russia during the 2016 US Presidential Election.
Critical Juncture	The unprecedented use of combined hybrid threats using cyber capabilities to access DNC officials' networks to hack and leak documents to influence the United States 2016 Federal Election at such a high level.
NATO Policy or Institutional Change	NATO's Warsaw Summit 2016 recognized cyber as a domain of military operations. Further development related to the rapid response teams, cyber defence and capacity building, Cyber Defence Pledge, partnerships, and affiliated Centres of Excellence.

Global 2017 - EternalBlue, WannaCry, NotPetya

Omitted Critical Juncture (Space Limitations)	EternalBlue and WannaCry, 2017
Events	The Shadow Brokers hacker group stole National Security Agency hacking tools, which included the EternalBlue computer exploit, which they released to the internet.
Critical Juncture	Over months EternalBlue was weaponized. North Korean threat actors used the EternalBlue exploit to launch the WannaCry ransomware attack. Russian threat actors used the same to launch the NotPetya attack, which caused $10 billion in damage globally.
NATO Policy or Institutional Change	The 2018 NATO Summit in Brussels included significant developments in cyber defence policy in the years following WannaCry. The Alliance agreed to form the Cyber Operations Centre with institutional changes partly because cyber was recognized as a domain of military operations.

8.5.4 Phase D

Global 2020 - COVID-19 Pandemic

Critical Juncture 8 (Phase D)	COVID-19 Global Pandemic, 2020
Events	The global COVID-19 pandemic erupts cyber attacks and malicious cyber activities taking advantage of the chaos caused by the pandemic.
Critical Juncture	Hackers took advantage of the fear and uncertainty of the pandemic to target individuals with significant increases in phishing and ransomware. State-sponsored cyber capabilities targeted vaccine-related research for theft.
NATO Policy or Institutional Change	NATO expertise in crisis management and disaster relief addressed the pandemic to present a model to adapt past expertise to future challenges arising faster than countermeasures can adapt.

Global 2021 - Ransomware Surge

Omitted Critical Juncture (Space Limitations)	Ransomware Surge, 2021
Events	Significant increase in the use of ransomware in late winter and spring 2021, targeting numerous organizations across North America and Europe.
Critical Juncture	Hackers took advantage of the fear and uncertainty of the pandemic to target individuals with significant increases in phishing and ransomware. State-sponsored cyber capabilities targeted vaccine-related research for theft.
NATO Policy or Institutional Change	NATO expertise in crisis management and disaster relief addressed the pandemic to present a model to adapt past expertise to future challenges arising faster than countermeasures can adapt.

2022 Strategic Concept

Internal Adjustment (Phase D)	NATO 2022 Strategic Concept at Madrid
Events	The Alliance agreed to a new Strategic Concept at the Madrid Summit, which included further developments related to cyber defence at NATO.
Internal Adjustment	Future research will question whether these events are a critical juncture akin to the 2010 Strategic Concept.
NATO Policy or Institutional Change	Future research will answer related questions.

Russia's Invasion of Ukraine

Critical Juncture 9 (13)	Russian Invasion of Ukraine Early, 2022
Events	Russia amassed troops on the border of Ukraine over months prior to a full military invasion on February 24, 2022. Numerous cyber attacks occurred in January and February prior to the invasion.
Critical Juncture	Cyber and related attacks set new precedents for the joint use of cyber and conventional capabilities. The example of Viasat demonstrated a dangerous display of cyber capabilities when combined with supporting conventional military operations.
NATO Policy or Institutional Change	Lessons learned during Russia's war in Ukraine occurred between February and June 2022, according to an interview for this study. Related initiatives were part of deliberations in the months leading up to the Madrid Summit and Strategic Concept.

Russia's War in Ukraine

Critical Juncture 10 (Phase D)	Russia's War in Ukraine, February 24, 2022-
Events	According to Wired Magazine's Andy Greenberg, Russia's war in Ukraine has involved many cyber attacks and the most wipers used ever in history.
Critical Juncture	New tactics, techniques, and procedures were observed, including coordination between cyber capabilities and conventional operations. Specific cyber attack use cases involve wiper attacks to erase government data.
NATO Policy or Institutional Change	Future research to answer questions about what NATO policy or institutional change resulted from Russia's use of cyber capabilities during the war in Ukraine.

8.6 – Open Street Map

The Open Street Map Foundation provided maps by open-source licence detailed at the following webpage: https://www.openstreetmap.org/copyright. All figures and diagrams are created and owned by the author of this manuscript Ryan J. Atkinson. All figures in this manuscript that include maps were based on screenshots taken from the OpenStreetMap tool. This subsection includes screenshots related to the OpenStreetMap copyright and license, which granted open-source use of the maps in the present manuscript.

8.6.1 Copyright and License - OpenStreetMap

OpenStreetMap is "open data, licenced under the Open Data Commons Open Database Licence by the OpenStreetMap foundation."[605] The OpenStreetMap Copyright and Licence webpage states that authors are "free to copy, distribute, transmit and adapt our data, as long as you credit OpenStreetMap and its contributor. If you alter or build upon our data, you may distribute the result only under the same licence."[606]

OpenStreetMap Copyright and License

Copyright and License

OpenStreetMap® is *open data*, licensed under the Open Data Commons Open Database License (ODbL) by the OpenStreetMap Foundation (OSMF).

You are free to copy, distribute, transmit and adapt our data, as long as you credit OpenStreetMap and its contributors. If you alter or build upon our data, you may distribute the result only under the same licence. The full legal code explains your rights and responsibilities.

Our documentation is licensed under the Creative Commons Attribution-ShareAlike 2.0 license (CC BY-SA 2.0).

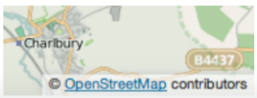
How to credit OpenStreetMap

Where you use OpenStreetMap data, you are required to do the following two things:

- Provide credit to OpenStreetMap by displaying our copyright notice.
- Make clear that the data is available under the Open Database License.

For the copyright notice, we have different requirements on how this should be displayed, depending on how you are using our data. For example, different rules apply on how to show the copyright notice depending on whether you have created a browsable map, a printed map or a static image. Full details on the requirements can be found in the Attribution Guidelines.

To make clear that the data is available under the Open Database License, you may link to this copyright page. Alternatively, and as a requirement if you are distributing OSM in a data form, you can name and link directly to the license(s). In media where links are not possible (e.g. printed works), we suggest you direct your readers to openstreetmap.org (perhaps by expanding 'OpenStreetMap' to this full address) and to opendatacommons.org. In this example, the credit appears in the corner of the map.



[605] OpenStreetMap, "OpenStreetMap Copyright," OpenStreetMap, n.d., https://www.openstreetmap.org/copyright.
[606] Ibid.

8.6.2 License and Attribution Guidelines - OpenStreetMap

The OpenStreetMap text attribution is conducted by including "©OpenStreetMap Contributors" in the bottom right-hand corner of all figures that include related maps. The license attribution requirement includes the link: https://www.openstreetmap.org/copyright and is also included as a hyperlink beneath each map diagram. The following screenshots depict these details further.[607]

Attribution Text

Attribution text

Attribution must be to "OpenStreetMap".

Attribution must also make it clear that the data is available under the Open Database License. This may be done by making the text "OpenStreetMap" a link to openstreetmap.org/copyright, which has information about OpenStreetMap's data sources (which OpenStreetMap needs to credit) as well as the ODbL.

The text must be easily readable and understandable, taking into consideration the font, size, colour, contrast, positioning and amount of time that it is visible. We recommend you follow accessibility guidelines such as WCAG, and any other locally relevant regulations.

OSM does not wish to claim credit for data or other material that did not come from it, so feel free to qualify the credit to explain what OSM content you are using. For example, if you have rendered OSM data to your own design, you may wish to use "Map data from OpenStreetMap."

The historical forms of attribution "© OpenStreetMap contributors" or "© OpenStreetMap" are acceptable.

Books, Magazines, and Printed Maps

Books, magazines, and printed maps

For a printed map and similar media (that is ebooks, PDFs and so on), the credit must appear beside the map if that is where other such credits appear, or in a footnote/endnote if that is where other credits appear, or in the "acknowledgements" section of the publication (often at the start of a book or magazine) if that is where other credits appear. The URL to openstreetmap.org/copyright must be printed out.

[607] OpenStreetMap Foundation, "Licence/Attribution Guidelines," n.d., https://wiki.osmfoundation.org/wiki/Licence/Attribution_Guidelines#Why_attribution_is_important

8.6.3 Open Data Commons Open Database License - Open Data Commons

The OpenStreetMap tool is licenced under the Open Data Commons Open Database License by the Open Knowledge Foundation.[608]

Open Data Commons

LEGAL TOOLS FOR OPEN DATA

Open Data Commons Open Database License (ODbL) Summary

This is a human-readable summary of the ODbL 1.0 license. Please see the disclaimer below.

You are free:

- *To share*: To copy, distribute and use the database.
- *To create*: To produce works from the database.
- *To adapt*: To modify, transform and build upon the database.

As long as you:

- *Attribute*: You must attribute any public use of the database, or works produced from the database, in the manner specified in the ODbL. For any use or redistribution of the database, or works produced from it, you must make clear to others the license of the database and keep intact any notices on the original database.
- *Share-Alike*: If you publicly use any adapted version of this database, or works produced from an adapted database, you must also offer that adapted database under the ODbL.
- *Keep open*: If you redistribute the database, or an adapted version of it, then you may use technological measures that restrict the work (such as DRM) as long as you also redistribute a version without such measures.

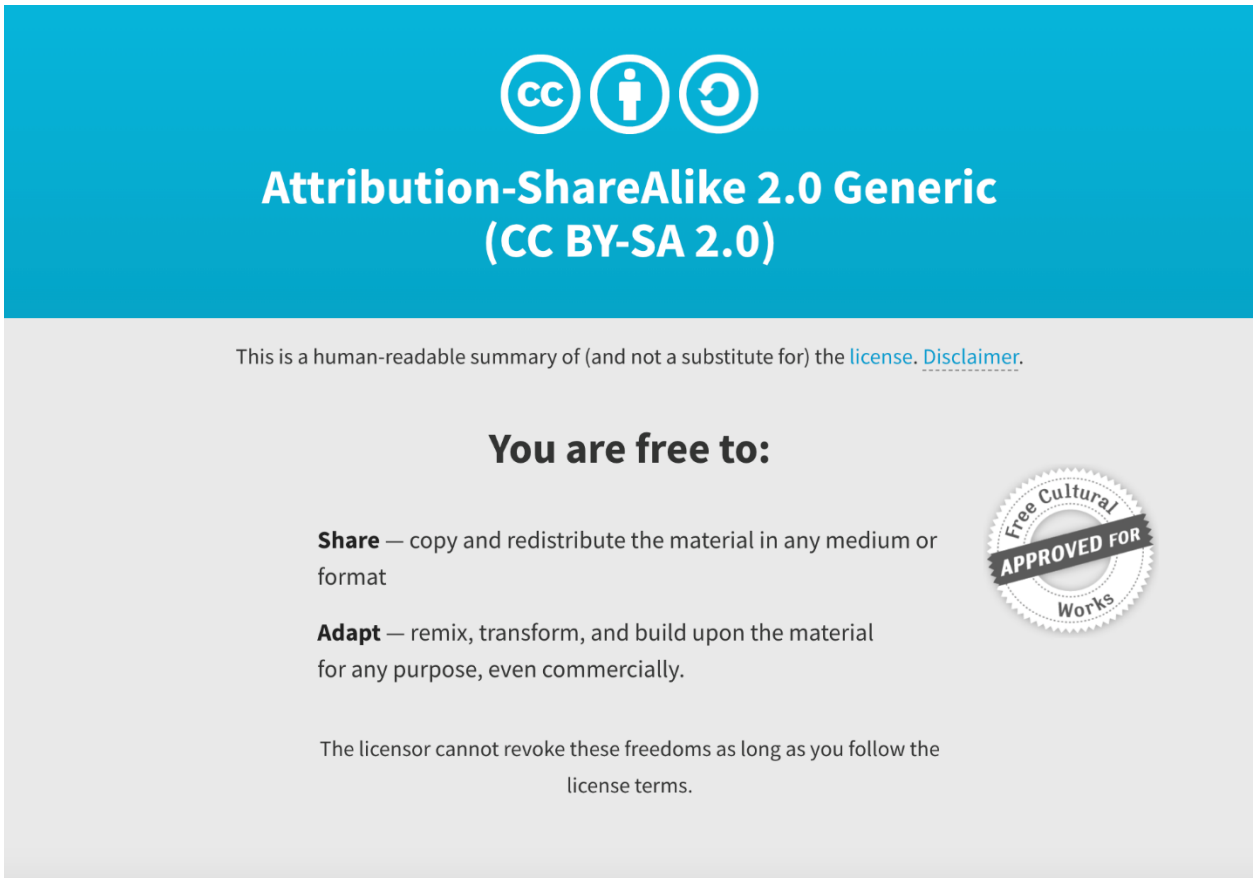
Disclaimer

This is not a license. It is simply a handy reference for understanding the ODbL 1.0 — it is a human-readable expression of some of its key terms. This document has no legal value, and its contents do not appear in the actual license. Read the full ODbL 1.0 license text for the exact terms that apply.

[608] Open Data Commons, "Open Data Commons Open Database License," n.d., https://opendatacommons.org/licenses/odbl/

8.6.4 Documentation License - Creative Commons

The OpenStreetMap Foundation provided all documentation open-source under the Attribution-ShareAlike 2.0 Generic license.[609]



[609] Creative Commons, "Attribution-ShareAlike 2.0 Generic," n.d., https://creativecommons.org/licenses/by-sa/2.0/.

8.7 – Curriculum Vitae of Ryan J. Atkinson

Department of Political Science, Western University, London, Ontario, Canada, N6A5C2

Education

2019-2023, Ph.D. Candidate in Political Science, Western University, London, Canada
2017-2018, M.A. Political Science, University of Toronto, Toronto, Canada
2010-2015, B.A. (Hons.) Political Science and Philosophy, University of Toronto, Canada

Honours and Awards

2023, Congress of the Humanities and Social Sciences, Graduate Student Merit Award
2023, Western University, Department of Political Science, Research Training Fund
2021-2022, Government of Ontario, Ontario Graduate Scholarship Research Funding Package
2019-2023, Western University, Department of Political Science, Doctoral Scholarship
2021, Western University, Department of Political Science, Research Training Fund
2020, Western University, Department of Political Science, Graduate Research Fund

Presentations

2023, Panel Presentation, "Key Events in NATO Cyber Defence Policy, 2000-2022," Congress of the Humanities and Social Sciences, York University, Toronto, Canada
2023, Guest Lecture, "Global Cyber Threats," Global Violence and Injustice, Dr. Erika Simpson, Department of Political Science, Western University, London, Canada
2022, Guest Lecture, "Future of Cyber Warfare," International Crises, Dr. Erika Simpson, Department of Political Science, Western University, London, Canada
2022, Guest Lecture, "NATO's Cyber Defence Policy and Evolution," NATO Consultation, Command, and Control Course, NATO School, Oberammergau, Germany
2021, Panel Presentation, "NATO Cyber Defence Debates on Deterrence and Defence," Internet and Cyber Challenges, Canadian Peace Research Association, Alberta, Canada

Professional Experience

2021-2022, Intern, Emerging Security Challenges Division, NATO HQ, Brussels, Belgium
2019-2021, Teaching Assistant, Western University, London, Ontario, Canada
2021, Cyber Policy Consultant, Ryerson Leadership Lab, Toronto, Canada
2019, Cyber Security Consultant, KPMG Canada, Toronto, Canada
2018-2019, Program Manager and Research Analyst, NATO Association, Toronto, Canada
2016 and 2018, Research Assistant to Dr. Erin Tolley, University of Toronto, Toronto, Canada