

Capabilities and Conflict in the Cyber Domain

An Empirical Study

By

Anthony John Stuart Craig

Dissertation submitted to the School of Law and Politics, Cardiff University in requirement for the degree of Doctor of Philosophy (PhD) in Politics and International Relations.

January 2020

Acknowledgements

This PhD would not have been possible without the help of my family. I especially thank my wife Natalia for being so supportive and patient.

I am grateful to Cardiff University's School of Law and Politics for funding my PhD and to the Research School on Peace and Conflict in Oslo for the opportunity they gave me to develop professionally as a researcher and for introducing me to a network of similarly minded academics.

I thank my office colleagues and friends in Cardiff, my school friends in Glasgow, and Tattiana, Shaun, Edith and Andrea for their friendship and support during this time.

I would not have got to this stage without the encouragement of Dr. Brandon Valeriano, who has given me self-confidence in my abilities and has remained a mentor since my time as an undergraduate at Glasgow University. I also thank my Cardiff University supervisor Dr. Andrea Calderaro for his continual advice and guidance, and Dr. Campbell Craig for his valuable feedback.

Finally, I am grateful to my external reviewer, Dr. Tim Stevens and my internal reviewer, Dr. Claudia Hillebrand for their expert advice which helped me strengthen this thesis.

Summary

This dissertation is a mixed method, empirical study on the causes and consequences of the proliferation of cyber capabilities among nation states in the international system from 2000 to 2017. National cyber capabilities are defined as the resources and assets used by states to project and resist influence through computer network operations (CNO). They are conceptualised and operationalised from two perspectives. Latent cyber capabilities are the societal resources that governments can draw on, including the programming skill and computer science knowledge of a population. Active cyber capabilities are the institutional developments by governments and militaries to build cyber security preparedness. They include the establishment of a computer security incident response team, a military computer network operations unit, or a national cyber security strategy.

Via the quantitative analysis of an original data set (the national cyber capabilities data set), the distribution of latent and active cyber capabilities in the international system is first described and the rate at which active capabilities have been acquired over time is highlighted. By structuring the analysis according to the theory of opportunity and willingness, the findings demonstrate that the adoption of active cyber capabilities is enabled by a country's latent resources (opportunity) and motivated by its external threat and rivalry environment (willingness). Next, the relationship between capabilities and the occurrence of computer network operations between rival states is investigated. Rather than deter conflict, cyber capabilities are positively associated with cyber-attacks. Finally, a case study of Iran is employed to illustrate how the cumulative findings of the statistical analyses apply in a real-world example. The findings of this dissertation highlight the need to develop alternative strategies for securing cyberspace to those focusing on the pursuit of military based capabilities and threats.

Table of Contents

		<i>Page</i>
Acknowledgements		i
Summary		ii
List of Tables		vi
List of Figures		viii
<i>Chapter</i>		
I.	Introduction: The Purpose and Plan of the Thesis	1
	The issue	1
	The contribution	2
	Research questions and theory	3
	The structure of the thesis	5
II.	Conflict and Capability in the Cyber domain	7
	Introduction	7
	Cyber Conflict in International Relations	8
	Power and Capability	15
	What do we know about cyber power and capability?	19
	Theoretical Position of Thesis	24
	Conclusion	28
III.	A Theoretical Framework for Explaining the Causes and Consequences of Cyber Capability	30
	Introduction	30
	Part one: The determinants of cyber capability proliferation	31
	Opportunity-Willingness Theory	31
	Latent resources and military capabilities	33
	The resource requirements for cyber capability	36
	Security threats as a driver of military capability	38
	The cyber threat environment and proliferation	41
	Part two: The impact of cyber capability on cyber conflict	43
	Deterrence, capabilities, and conflict in international relations	44
	The failure of cyber deterrence	46
	Capabilities as a cause of conflict	51
	Opportunity-Willingness and cyber conflict	52
	Summary	55
IV.	Methods for Quantifying National Cyber Capability	57
	Introduction	57
	The scope and limits of the NCC dataset	58
	How is the data collected?	62
	Indicators of latent cyber capability	63

	Indicators of active cyber capability	69
V.	Research Design for Investigating the Causes and Consequences of Cyber Capability	75
	Introduction	75
	Establishing causality	76
	Methods of statistical analysis	77
	Part one: Describing the distribution and proliferation of cyber capability	78
	Part two: Identifying the determinants of cyber capability	79
	Part three: Investigating the impact of capabilities on cyber conflict	83
	Part four: Illustrative case study of Iran	90
	Summary	91
VI.	A Descriptive Analysis of Cyber Capability in the International System	92
	Introduction	92
	Latent cyber capabilities: where do countries stand?	92
	Active cyber capabilities and strategies: temporal and spatial proliferation	108
	Discussion	115
VII.	Determinants of Cyber Capability	116
	Introduction	116
	Hypotheses for capability adoption	116
	Bivariate analysis: latent capability and active capability	118
	Bivariate analysis: external threat environment and active capability	125
	Multivariate analysis: Opportunity and willingness theory tested	131
	Discussion	140
VIII.	Capability and Conflict: The Effect of Defensive Capabilities	142
	Introduction	142
	Research Design	143
	Defensive capabilities and cyber incidents at the system level	143
	Defensive capabilities and cyber incidents at the country level	146
	Multivariate analysis	150
	Defensive capabilities and the success of cyber incidents	152
	Discussion	155
IX.	Capability and Conflict: The Effect of Capability Parity and Preponderance on Cyber Conflict	156
	Introduction	156
	Parity and preponderance	157
	Research Design	158
	Relative latent cyber capability and cyber conflict	160
	Relative active cyber capability and cyber conflict	164
	Multivariate analysis	166
	Discussion	170

X.	Capability and Conflict: The Initiators Capability and Cyber Conflict	172
	Introduction	172
	System level capabilities and the initiation of cyber incidents	173
	The initiator's capability and the frequency of cyber incidents	176
	The initiator's capability and the likelihood of cyber incidents	179
	Rivalry intensity and cyber incidents	183
	Multivariate analysis	185
	The initiator's capability and the severity of cyber incidents	189
	Discussion	191
XI.	The Case of Iran: Illustrating the Findings	193
	Introduction	193
	Describing Iran's cyber capabilities	194
	How latent capability and rivalry has driven Iran's active cyber capabilities	195
	Has Iran's cyber defence succeeded?	202
	Iran's capabilities and offensive operations	205
	Discussion	209
XII.	Conclusion: What Do We Now Know About Cyber Capability and Conflict	211
	Introduction	211
	Summary of theory and approach	211
	What do we know about cyber capabilities now?	214
	Policy implications	217
	Caveats and future research	219
	List of References	222
	Appendix: Active Cyber Capability and Strategy Data	244

List of Tables

<i>Table</i>	<i>Page</i>
1. NCC dataset variables and measurement	74
2. Explanatory variables for investigating the determinants of active capability	83
3. Frequency of cyber incidents between rival dyads (2000-2016)	85
4. National performances at the IOI and IMO by country (2016)	93
5. Computer science publication output by country (2016)	95
6. Software companies by country (2016)	96
7. ICT service exports by country (2016)	97
8. Internet penetration, top and bottom 10 countries (2016)	99
9. Secure Internet servers, top ten countries (2016)	99
10. Latent cyber capability index country ranking (2018)	102
11. Correlation of latent cyber capability with cyber and material capability indices	106
12. Organisational age of national CSIRTs (2017)	110
13. Organisational age of military CNO units (2017)	112
14. Organisational age of national cyber security strategies (2017)	114
15. Summary statistics for opportunity-based variables	118
16. National resources and military CNO unit possession	120
17. National resources and national CSIRT possession	121
18. Conditional Probabilities of military CNO unit capability by resources	123
19. Conditional probabilities of National CSIRT capability by resources	124
20. Summary statistics for willingness-based variables	125
21. Threat environment and military CNO unit possession	126
22. Threat environment and national CSIRT possession	128
23. Conditional Probabilities of military CNO unit capability by threat environment	129
24. Conditional Probabilities of national CSIRT capability by threat environment	130
25. Logistic regression of military CNO unit possession	133
26. Logistic regression of national CSIRT possession	135
27. Effect of changes in independent variables on the probability of military CNO unit	137
28. Effect of changes in independent variables on the probability of national CSIRT	138
29. Likely next adopters of military CNO units	139
30. Likely next adopters of national CSIRT	139
31. Correlation between defensive cyber capability and cyber incidents	146
32. Correlation between secure servers (per million) and cyber incidents initiated (2000-2016)	147
33. Cross tabulation of secure servers (per million) and cyber incident initiation (2010-2016)	147
34. Cross tabulation of national CSIRT and cyber incident initiation (2010-2016)	149
35. Cross tabulation of NSCC and cyber incident initiation (2010-2016)	149
36. Logistic regression of defensive capabilities and cyber incident occurrence (2000-2016)	151
37. Defensive cyber capabilities and incident success	152

38.	Cyber incident occurrence among rival dyads (2000-2016)	159
39.	Summary statistics for relative latent cyber capability	159
40.	Frequency table of military CNO unit status amongst rival dyads (2000-2016)	160
41.	Relative latent cyber capabilities and incident onset among rival dyads (2000-2016)	161
42.	Conditional probabilities of cyber incident by relative power	162
43.	Combined capability and relative capability among rival dyads (2000-2016)	164
44.	Relative active cyber capabilities and incident onset among rival dyads (2000-2016)	165
45.	Conditional probabilities of cyber incident by relative active capability	165
46.	Logistic regression of relative capabilities and cyber conflict among non-directed dyads (2000-2016)	168
47.	Correlations between capabilities and incident frequency, 2000-2016	175
48.	Correlation between latent cyber capability and number of cyber incidents initiated (2000-2016)	178
49.	Initiator/defender preponderance in latent capability and incident initiation	180
50.	Initiator's latent capability and incident initiation.	181
51.	Initiator's military CNO unit possession and incident initiation	182
52.	Conditional probabilities of cyber incident by relative power	182
53.	Correlation of total MIDs with cyber incidents.	184
54.	Dispute frequency and cyber incidents between rival states (2000-2016)	184
55.	Number of MIDs from initiator and cyber incident initiation in directed rival dyads (2000-2016)	185
56.	Logistic regression of cyber incident initiation among directed dyads (2000-2016)	187
57.	Frequency of DCID incidents by severity scale	189
58.	Initiator's Military CNO unit status and incident severity	191

List of Figures

<i>Figure</i>	<i>Page</i>
1. Yearly Cyber Incidents, Coercive Intent: 2000–2014 (Valeriano, Jensen and Maness 2018)	14
2. IOI and IMO programming skill among top three (2000-2017)	94
3. Computer science publications among top three (2000-2016)	95
4. Number of software companies among top three (2000-2017)	97
5. ICT service exports among top 3 (2000-2017)	98
6. Secure Internet servers, top 10 countries (2010-2017)	100
7. Histogram of latent cyber capability (2018)	105
8. Difference between material and cyber capability among selected states.	107
9. Temporal proliferation of national CSIRTs (2000-2017)	109
10. Spatial proliferation of national CSIRTs (2017)	109
11. Temporal proliferation of military CNO units (2000-2017)	111
12. Spatial proliferation of military CNO units (2017)	112
13. Temporal proliferation of National Cyber Security Strategies (2000-2017)	113
14. Spatial proliferation of National Cyber Security Strategies (2017)	114
15. Secure Internet infrastructure and cyber incident frequency	144
16. National CSIRTs and cyber incident frequency	145
17. National Cyber Security Strategies and cyber incident frequency	145
18. Secure servers and total incidents suffered (2000-2016)	146
19. Average incidents experienced according to National CSIRT possession	148
20. Average incidents experienced according to NCSS possession	148
21. Average latent capability index by dyadic capability ratio size	163
22. Substantive impact of dyadic military CNO unit possession on cyber incident occurrence	170
23. Computer science article and incident frequency, 2000-2016	174
24. IMO and IOI medals and incident frequency, 2000-2016	174
25. Software companies and incident frequency	175
26. Military CNO unit countries and cyber incidents, 2000-2016	175
27. Scatter plot of latent cyber capability and incident initiation (2000-2016)	177
28. Density plot of cyber incident initiations by CNO unit status	179
29. Total MIDs and cyber incidents between rival dyads.	183
30. Ongoing cyber incidents against Iran (2000-2016)	205
31. Ongoing cyber incidents initiated by Iran (2000-2016)	208
32. The severity of Iran’s offensive cyber operations (2000-2016)	209

Chapter I

Introduction: The Purpose and Plan of the Thesis

The issue

This thesis advances our understanding of cyber capabilities and computer network-based conflict in international politics. The spread of Internet connectivity worldwide and the increased dependence of society on computer networks has led to the emergence of new national security threats. Traditional, territorial-based warfare has sharply declined since the end of World War II (Sarkees and Wayman 2010), but the digital revolution has given states new opportunities to pursue their strategic aims through virtual means (Valeriano, Jensen, Maness 2018; Kello 2018). Over the past twenty years, the Internet has become a new arena for interstate competition and conflict, and governments worldwide are reorganising, investing, and preparing accordingly.

The international system has occasionally witnessed the acquisition of weaponry and military capabilities during periods of significant technological change which has contributed to international competition and conflict. For instance, the development of steel hulled and steam powered battleships in the late 19th and early 20th century combined with great power competition over colonial acquisitions to create a naval arms race in the lead up to World War I. Furthermore, the invention of the atomic bomb by the United States during World War II led to its devastating application in 1945 and the subsequent proliferation of nuclear weapons to several other countries during the 20th century (Horowitz 2010). One of the key issues of today is how the emergence of computing technology will reshape international security.

Computer code is now employed for malicious purposes as a means of achieving influence in international relations. Many state and non-state actors are known to have conducted computer network operations (CNO) to undermine the interests of political rivals including the sabotage of critical infrastructure, disruption of Internet services, theft of classified government or industry data, or subversion of public opinion (Healey 2013). Even more actors are allegedly engaged in a global cyber “arms race” as they develop the means to carry out or defend against these threats (Diebert 2011; Craig and Valeriano 2016). States increasingly view cyberspace as the “fifth domain of warfare” after land, sea, air and space and are engaged in a rapid militarisation of this environment through the acquisition of cyber weapons and the establishment of military agencies aimed at deterring threats or harming their rivals (The Economist 2010).

This issue is of utmost policy relevance. The UK government, for instance, has classified cyber-attacks as a tier one threat to national security, claiming they are both highly likely and highly

destructive. It is investing £1.9bn from 2016 to 2021 to enact its national cyber security strategy (HM Government 2016, 10). The CIA's 2019 global threat assessment puts these threats on top of its priority list and warns that the United States' "adversaries and strategic competitors will increasingly use cyber capabilities – including cyber espionage, attack, and influence – to seek political, economic, and military advantage over the United States and its allies and partners" (Coats 2019, 5). Yet, despite frequent news stories in the west about the threat from states such as Russia, China, Iran, or North Korea, there has been very little empirical analysis of their capabilities or more generally of the adoption of capabilities worldwide.

Policy makers and stakeholders must urgently make sense of the proliferation of cyber capabilities to formulate appropriate responses and create a more stable and secure cyber domain. While cybersecurity is in one sense a highly technical area, it also involves political actors and processes. Experts at the technical level are needed to develop secure technologies and infrastructure, while at the policy level, International Relations (IR) scholars can help understand the behaviour of global actors and the conditions than lead to stability or conflict.

The contribution

Political scientists are clearly invested in this issue with increasing numbers of academic journal articles being published on cyber security (Gorwa and Smeets 2019). Yet, while there are certainly growing efforts to understand the implications of digital technology in international and domestic politics, there are limitations in the existing literature that this thesis addresses. For instance, the existing literature is to a large extent theoretical and speculative in its approach, as scholars have debated whether destructive cyber wars are a likely scenario of the future (Clarke and Knake 2010; Rid 2013). Despite the fact that these worse-case scenarios have not materialised, it is clear that states are investing in capabilities and are carrying out computer network operations that fall below the threshold of war (Valeriano and Maness 2014). This thesis moves beyond the debate of cyber war and examines the observable behaviour of states as they seek to secure cyberspace.

By doing so, this thesis also advances the role of quantitative based social science research in cyber security. With some exceptions (Valeriano and Maness 2014; Kostyuk and Zhukov 2017), most empirical research in this field is qualitative, meaning that studies are conducted on a few or even single cases rather than an extensive set of data points that can lead to generalisable findings. Although quantitative methods are commonplace in other areas of international studies, it is rarely applied to cyber security and the development of theory is lacking as a result because we have little understanding of the general causal trends characterising behaviour in this domain. Some scholars are highly sceptical of such efforts and suggest quantitative research is unfeasible given the secrecy

of cyber security activities (Kello 2018, 37-42). While it is indeed challenging, a quantitative assessment of the current cyber security landscape is both feasible and necessary to further our understanding of international politics in the digital era.

This thesis makes an original methodological contribution to the field by introducing the National Cyber Capabilities (NCC) dataset, compiled through open source information, which traces the growth in cyber capabilities of 194 nation states over the period 2000 to 2017. This data provides a valuable new resource to students and scholars of international cyber politics, and with this data set I help advance our knowledge of the causes and consequences of cyber capability proliferation. The thesis is also novel in that I apply longstanding IR perspectives concerning power, deterrence, and conflict to the cyber domain, thus furthering theory development in security studies.

National capabilities have long been considered key for explaining international conflict and are one of the most frequently used explanatory or control variables in quantitative research (Hensel 2012, 53). While national power in international relations, by many accounts, is evident only in the influence achieved by one state over another (Barnett and Duvall 2005), capabilities by contrast are the resources or assets that enable a state to project or resist influence in international politics. By extension, cyber capabilities are defined as the resources and assets to project or resist influence in the cyber domain, understood as the global environment of computer networks and systems through which international actors pursue their strategic aims.

This research is grounded in a positivist epistemology meaning that I treat the observed behaviour of political actors as the key means for acquiring knowledge about the world. My methods are primarily quantitative in that I use the NCC dataset alongside secondary data sources to conduct statistical analyses in order to establish causal relationships between variables. I then compliment my quantitative methods with an illustrative case study however to highlight the causal mechanisms and the processes of capability development and cyber conflict.

Research questions and the theoretical framework

The data is used to answer three specific questions. The first asks how capabilities have spread and been adopted in the international system. After empirically demonstrating the rapid proliferation of cyber capabilities in the international system, the second question asks what factors increase the likelihood of states adopting them. The third question then asks whether capabilities cause a reduction or increase in cyber conflict between states, and whether states are more likely to employ their capabilities offensively having acquired them.

I draw on a range of relevant literature to develop testable hypotheses about the causes of cyber capability adoption and conflict. To organise my explanatory variables and guide the investigation I apply an analytical framework known as Opportunity-Willingness Theory (Most and Starr 1989). Applying this to cyberspace, it suggests that a state's decision to establish active cyber capabilities, as indicated by the presence of military and governmental organisations that engage in computer network operations, should be driven by its motives and its capacity.

Opportunity describes what is possible for the state to achieve and is measured by the availability of resources. Scientific and technical knowledge is a particularly crucial resource in this context since cyber technologies are a knowledge-intensive rather than financially intensive capability. What matters most is whether a country possesses sufficient levels of computer programming skill and computer science knowledge, rather than how economically developed or it is.

Furthermore, the willingness to establish active cyber capabilities is shaped by the political pressures or incentives to build capability. More specifically, I test the proposition (derived from the neorealist concept of the security dilemma (Jervis 1976) that a state is more likely to adopt active cyber capabilities if it faces a more intense external threat environment. Countries facing greater insecurity, competition, and threat from their external rivals should be more likely to develop active cyber capabilities because they can provide the state with the means to better defend against threats or carry out offensive operations.

Once a state has acquired active capabilities, it then has the opportunity to engage in computer network-based conflict with its rivals. Given the failure of cyber-deterrence and the advantages that cyber capabilities provide in terms of avoiding attribution, overcoming geographical borders, and avoiding escalation into conventional military conflict, capabilities should promote rather than dissuade cyber conflict. Ultimately, I demonstrate the importance of accounting for cyber capabilities as a key explanatory variable for cyberspace activity.

My findings first of all confirm that the international system is witnessing a rapid proliferation of capabilities, including a strong trend towards militarisation. Secondly, the findings support the theory that the acquisition of capabilities is driven by a state's latent programming skills and computer science knowledge and by its international threat environment and rivalry context. Thirdly, my findings undermine deterrence as applied to the cyber domain and suggest to the contrary that the presence of capabilities promotes rather than reduces cyber conflict between states. Together the findings demonstrate that the adoption of capabilities and the incidence of cyber-attacks is likely to continue into the foreseeable future, at least at the relatively low levels of hostility currently experienced.

The structure of the thesis

The thesis is structured as follows: Chapter 2 is the literature review chapter and is used to establish the academic context of this research. This discussion is essential for the reader to understand the broader significance of this research and how it will build on existing knowledge on this subject. It includes a discussion of cyber conflict, of power and capability, the state of knowledge on cyber capabilities, and an explanation of where this thesis sits in the IR theory landscape.

Chapter 3 is the theoretical framework and is used to set out hypotheses that the proliferation of cyber capabilities is motivated by external threat environment and latent resources, and secondly that cyber conflict is more likely to be promoted rather than deterred by the presence of capabilities. In this chapter I establish Opportunity-Willingness theory (Most and Starr 1989) which guides my investigation.

The next two chapters discuss my methodology. Chapter 4 is the data collection methods chapter where I explain how I created the National Cyber Capabilities (NCC) dataset and derive the variables. Chapter 5 is the research design chapter where I explain how I use this dataset in subsequent chapters to answer my research questions. In these chapters I establish the scope conditions of my data and justify specific methodological choices. This is a key part of the dissertation because it gives readers a clear understanding of my approach and its validity.

Chapter 6 describes how capabilities have spread across the international system and across time and compares countries by their capability scores. This will highlight the current distribution of resources in the cyber domain and the rate at which countries are acquiring active capabilities. This chapter is also important for giving the reader a feel for the data used to answer the subsequent research questions.

Chapter 7 investigates the drivers of cyber capability proliferation. I use the Opportunity-Willingness framework to structure the analysis of how the state's latent resources and external threat environment influences its adoption of military and governmental computer network operations (CNO) units. The results show that a state's programming skill, computer science related knowledge, and its engagement in interstate rivalries provide the most robust explanations for the adoption of active capabilities.

Chapters 8, 9, and 10 examine the effect of cyber capabilities on conflict and draws on the theory of deterrence which suggests capabilities can be employed to dissuade offensive activity. Chapter 8 investigates the impact of defensive capabilities and policies on cyber incidents against the state, demonstrating that deterrence through denial is difficult to achieve. Chapter 9 further undermines deterrence by showing that the balance of preponderance of capability between two states does not reduce the likelihood that they will engage in cyber conflict. Chapter 9 investigates how the

capabilities of the initiator effect the likelihood of cyber operations being conducted. The results show that the presence of military capabilities increases the frequency of cyber conflict, while controlling for other factors.

Chapter 11 is the final chapter of analysis where I trace the process of capability adoption and conflict engagement in an illustrative case study of Iran. While quantitative methods can highlight the causal effects of variables, they cannot identify the causal mechanisms, or *how* opportunity and willingness factors have been translated by Iran towards greater cyber capability and proneness towards offensive activity.

Chapter 12 is the conclusion. In this chapter I summarise my approach and findings and discuss their theoretical and policy implications. I suggest a strategy of norms promotion rather than deterrence through militarisation as a more sustainable mechanisms towards building a more secure cyberspace. Lastly, I assess the limitations of my approach and suggest pathways for future research.

Chapter II

Conflict and Capability in the Cyber Domain

Introduction

International politics have often been impacted by technological change. History is replete with examples of how innovations in military technology like the longbow, the repeating rifle, long range airpower, or nuclear weapons were influential in reshaping the dynamics of the battlefield or even the stability of the international system (Herrera 2006). The information revolution beginning in the late 20th century describes the latest shift driven by “rapid technological advances in computers, communications, and software” which has resulted in a dramatic reduction in the cost of information communication (Nye 2011, 114). The impact of this revolution on international politics and military affairs is a source of fascination for many IR scholars who have turned their attention to explaining the spread and implications of digitally enabled military technologies such as drones, autonomous weapons, and cyber warfare capabilities (Furhmann and Horowitz 2017; Jensen, Whyte and Cuomo 2019; Schneider 2019).

Although the earliest form of communication through computer networks was established in the 1960s by the US Department of Defence, it was not until the 1990s when the invention of the World Wide Web (WWW) caused the expansion of Internet connectivity globally and gave rise to the phenomenon of Internet-based threats as we know them today. As Information Technology (IT) has proliferated, societies and governments have become increasingly dependent on the Internet which has brought great benefits in terms of economic growth and the spread of knowledge.

Unfortunately, the growth of cyberspace has also increased the risk of malicious cyber activity from state and non-state actors. From the financial loss to businesses through cybercrime, the theft of classified government or industry secrets, or the targeting of a country’s critical infrastructure, cyberspace poses a significant challenge to the economic and national security of states. As a result, cyber security has become a major source of concern for policymakers and IR scholars in the past twenty to thirty years.

Cyberspace, or the cyber domain¹, has been defined as “an operational domain framed by use of electronics to...exploit information via interconnected systems and their associated infrastructure” (Kuehl 2009, 24). Other scholars suggest the concept also encompasses political actors and users of cyberspace (Choucri 2012, 8). Alternatively, Libicki (2009, 12) describes cyberspace in terms of

¹ I use both terms interchangeably in this dissertation.

three layers beginning with a physical layer (computers) at the base, a syntactic layer (computer processes) above this, and a semantic layer (computer information) at the top. For the purposes of this thesis, cyberspace as defined as the international environment of Internet infrastructure, networks, and reliant systems through which political actors pursue their strategic interests. States in particular are currently developing the means to operate through this space in order to defend themselves against cyber operations, deter malicious cyber activity, or to carry out offensive or intelligence-gathering activity of their own.

The objective of this thesis is to explore this global build-up of cyber capability by states and investigate the causes and consequences of this process. I define cyber capability as the resources used to conduct Computer Network Operations (CNO) which I measure through the newly collected National Cyber Capabilities (NCC) dataset. The purpose of this chapter is to place this research within a broader academic and policy context to give the reader an understanding of its relevance and contribution to ongoing cyber security debates.

This chapter is divided into four parts. The first part reviews the literature on cyber war and conflict, which has been the most dominant theme in the emerging field of cyber security and international relations. This will help to highlight the theoretical and methodological gaps in the literature that this thesis seeks to address. Next, I explore the concepts of power and capability in the broader International Relations (IR) discipline which is key because many aspects of my approach are rooted in this literature. The third section then reviews the emerging literature on power and capability in the cyber domain specifically and assesses existing attempts at quantifying cyber capability. Finally, I end this chapter with a discussion of the importance of this research to policy and academic knowledge.

Cyber Conflict in International Relations

The literature on cyber security and its implications for world politics has been developing over roughly the past twenty-five to thirty years, but has grown particularly rapidly since the late 2000s. One of the key themes emerging from this literature is a debate over the meaning and significance of “cyber war” – a concept that has been used by scholars, policy makers, and the media as a catchall term for politically motivated cyber operations. Junio (2013, 126), for instance, defines cyber war as a “coercive act involving computer network attack”. A helpful, albeit oversimplified, way of understanding the cyber war debate is of the divide between cyber “revolutionaries” who believe cyber war is real and will destabilise international relations, and cyber “sceptics” who argue that cyber war is either not real, unlikely, or that its impact is grossly exaggerated (Lango 2016). To situate this thesis within the established body of literature, this section will explore the evolution of

the debate and define key concepts such as cyber war and cyber conflict that are central to any discussion of cyber security and international politics.

Cyber “revolutionaries” perceive cyber war as an urgent threat to international security that will transform the traditional dynamics of global politics. One of the earliest works from this perspective was by Arquilla and Ronfeldt (1993) when they proclaimed that “Cyber War is Coming!” and characterised the information age as the latest revolution in military affairs to reconfigure the power relations between nations. This article introduced two new concepts: “netwar” – the attempt to control the knowledge and beliefs of a target population through propagandist means, and “cyberwar” – military operations that aim to harm a rival’s information and communication systems and gain a relative advantage in knowledge on the battlefield.

The massive expansion of the Internet through the 2000s and the occurrence of high-profile cyber incidents such as Stuxnet (Zetter 2014) or the Estonian DDoS attacks (Lawlor 2014, 69-95) has led to renewed interest and debate on the meaning and implications of cyber war in the 21st century. The revolutionary perspective has been prominently advanced in writing by Clarke and Knake (2010) in their book, “Cyber War: The Next Threat to National Security”, which describes the devastating impact a cyber-attack could have on a nation’s critical infrastructure creating a potential for human fatalities. A major source of concern is the risk to a country’s Supervisory Control and Data Acquisition (SCADA) systems used to control the industrial processes of power plants, electrical grids, refineries, and pipelines etc (Peterson 2013) since these are usually connected to computer networks.

Some more critically minded IR scholars have traced the use of historical analogies which invoke fear to help build public support for national cyber security policy (Betz and Stevens 2013; Stevens 2016, 123-148). In these so called “cyber-doom scenarios” (Lawson 2013), analogies have been drawn between cyber war and the catastrophic events of Pearl Harbour (Ryan 2011) and 9/11 (Usborne 2012), as politicians have sought to draw attention to the issue and justify increased investment in cyber security. Research in this area has also shown how cyber threats are socially constructed and contingent on the changing ways they are framed by policy makers and interest groups over time (Cavelty 2008). Inaccurate metaphors and analogies however only hinder progress towards a clearer conceptualisation and understanding of cyber war (Betz and Stevens 2013, 148; Sulek and Moran 2009).

The sceptical perspective has been most prominently advanced by Thomas Rid who counters the threat inflation in an article and book titled “Cyber War Will Not Take Place” (Rid 2012; Rid 2013). Rid argues that cyber war is not real because cyber operations do not meet the criteria for warfare according to the military theory of Clausewitz. Since cyber-attacks have never resulted in casualties (are not violent), are not used to shape an opponent’s behaviour (are not instrumental), and are not

declared as acts of war by political actors (not political), Rid argues that cyber war is a misnomer, has not occurred, and is very unlikely to occur in the future. Betz (2012) supports the sceptical position and recognises that although cyber technology may change the way force is applied, acts of war require a declaration of will which has been absent from cyber incidents thus far. The rejection of cyber war is resisted by some scholars like Stone (2013) who responds that “Cyber War Will Take Place!” and argues that violence is not a necessary condition for war.

This literature highlights the need for clearer definitions of cyber-based activity. One limitation with this area of enquiry however is that it can get too bogged-down in questions of semantics that it often ignores the empirical reality that political rivals are increasingly using cyber tools against one another (Valeriano and Maness 2015). As Arquilla (2012) writes: “cyberwar has arrived. Instead of debating whether it is real, we need to get down to the serious work of better understanding this new mode of war-fighting.”

The other central aspect of the revolutionary/sceptic debate concerns the effect of cyber conflict on the international system. For instance, Kello (2013, 22) writes that “the virtual weapon is expanding the range of possible harm and outcomes between the concepts of war and peace, with important consequences for national and international security” given the inherent challenges of cyber defence, the advantages of cyber weapons, and disruption to the international distribution of power. Sceptics like Gartzke (2013, 42) on the other hand emphasise the limitation of cyber-attacks in contributing to military victory by noting that “the Internet is generally an inferior substitute to terrestrial force in performing the functions of coercion or conquest.” Similarly, Lieber (2014) highlights the inherent uncertainty over the effectiveness of cyber offence as tool for achieving military victory. Smeets (2018), on the other hand, argues that offensive cyber operations can have strategic value by increasing the range of foreign policy tools available to leaders, multiplying the effect of conventional military force, inflicting psychological harm on an enemy, and limiting casualties.

Another prominent hypothesis in this literature suggests that that cyber war poses an asymmetric threat (Koblentz and Mazanec 2013, 423) because the ease at which cyber technology can be obtained and harnessed will confer an advantage to conventionally weaker, less well-resourced states, and enable them to level the playing field with stronger states (Kello 2013, 31; Liff 2012, 409). Economically advanced states like the United States on the other hand are generally more reliant on computer networks which makes them relatively more vulnerable to cyber war (Valeriano and Maness 2015, 25; Libicki 2009, 32). Other authors counter these claims and argue that the ability to develop sophisticated cyber tools that could cause significant damage still lies in the hands of the most technologically advanced countries due to the high resource requirements in terms of intelligence gathering and technical ability (Lindsay 2013). While there is theory aplenty on cyber war and its effects, systematic empirical analysis is needed to substantiate or falsify these various claims.

As the study of cyber security has evolved, there is an increasing acceptance that competition and conflict in cyberspace, however it is defined, is a real phenomenon and its character and effects upon international relations ought to be investigated. Scholars now frequently use the term “cyber conflict” instead of “cyber war” to collectively describe the operations conducted through computer networks between political actors in cyberspace (Valeriano and Maness 2015). This term acknowledges that the vast majority of these interactions fall short of warfare strictly defined and are more accurately placed somewhere between the concepts of war and peace (Whyte and Mazanec 2019, 149).

The growth of cyberspace is significant to global politics because of the range of new avenues for interstate conflict that have arisen. Some of the effects that can be achieved through cyber operations include the defacement of web pages, disruption of Internet services, theft of confidential information, corruption or deletion of data, interruption of physical processes, or releasing of confidential information (Council on Foreign Relations n.d.).

A number of typologies of cyber conflict that fall below the threshold of warfare have been proposed. For example, Rid (2012) classifies politically driven offensive actions² into three categories: sabotage, espionage, and subversion. Sabotage is the “deliberate attempt to weaken or destroy an economic or military system” (2012, 16). This can occur alongside conventional military operations as on 6 September 2007 when Israel disrupted Syrian air defences with cyber tools to facilitate a subsequent and undetected airstrike against a nuclear facility. It can also be a stand-alone act, such as the infection in 2010 of the computer systems at a nuclear facility in Iran resulting in physical damage to the centrifuges used to enrich uranium (Zetter 2014).

Espionage is the “attempt to penetrate an adversarial system for purposes of extracting sensitive or protected information” and is the “most widespread use of state-sponsored cyber capabilities” thus far (Rid 2012, 20). China is accused of many intrusions into the networks of foreign governments and companies for espionage purposes dating back to at least 2003 (Lindsay and Cheung 2015, 58-59). These operations are often termed Advanced Persistent Threats, characterised by their sophisticated intrusion methods, stealth, and prolonged access (Tankard 2011). Between 2007 and 2009, Chinese hackers allegedly extracted terabytes of information relating to the designs of the latest American fighter jet, the F-35, which highlights the threat cyber espionage poses for the United States’ technological supremacy in world politics (Clarke and Knake 2010, 111).

Finally, subversion is characterised by a “deliberate attempt to undermine the authority, the integrity, and the constitution of an established authority” (Rid 2012, 22) as actors seek to advance their

² Most cyber incidents fall under the category of cyber-crime where the motive is not political but financial and is generally carried out by criminal groups or individuals. Because of the state-centric focus of this dissertation and the concern with political motivated cyber conflict, cyber-crime is not investigated here.

political or ideological agenda. During the 2016 U.S. presidential race, Russian government-sponsored hackers allegedly accessed and leaked tens of thousands of emails from the Democratic Party's National Committee and conducted a social media campaign of fake information to influence the election (Williams 2017).³ This incident could be placed under the subversion category.

In an alternative typology, Valeriano, Jensen and Maness (2018, 11-13) delineate three types of cyber strategy states adopt in trying to exercise power in cyberspace according to coercive intent. Disruption operations are a "low-cost, low-payoff form of cyber strategy designed to shape the larger bargaining context". Espionage describes the "efforts to steal critical information or manipulate information asymmetries in a manner that produces bargaining benefits between rival states engaged in long-term competition." Degradation refers to "coercive operations designed to sabotage the enemy target's networks, operations, or systems."

Another area of research has helped develop our understanding of how cyber conflict works at a more granular level. It is useful to review some of the technicalities of cyber conflict here. According to Nye (2016/2017, 50), the three main vectors for attack are through computer networks, the supply chain of software and hardware, or human insiders that have gained physical access to the target. One of the least sophisticated method is a Distributed Denial of Service (DDoS) attack whereby a computer network is overloaded with information sent simultaneously from several compromised computers – or botnet – which renders the service inaccessible to Internet users (Singer and Friedman 2014, 44).

More sophisticated methods attempt to infect a target computer or network with malware (malicious software) in the form of viruses, worms, Trojans, or spyware for example. Malware often infects a target through the process of phishing whereby an attacker deceives an unwitting user into opening an email attachment or link leading to the malware being installed. An alternative method is to insert the malware into a machine by physical means, like a USB drive. Once inside a computer system, malware can then disrupt, steal, or damage data as well as replicate and spread to other users (Singer and Friedman 2014, 58).

The term "cyber weapon" is closely synonymous with the concept of malware, and has been used by political scientists to refer to "computer codes that are used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings" (Rid and McBurney 2012, 6). In Herr's (2013) framework, cyber weapons contain a propagation method, an exploit, and a payload. The propagation method is how the malware is transmitted to a

³ This type of activity of seeking control over what an enemy knows and thinks through propaganda is also called information warfare (Libicki 2017).

target, the exploit is the code used to compromise the target's software and allow access, and the payload is the code which carries out the intended malicious aim.

Along similar lines, Buchanan (2016, 33) introduces an eight-stage model – a less technical version of the “Kill Chain” model used by cyber security professionals (Hutchins 2015) – to explain the key steps taken by attackers during a successful cyber operation. Attackers first gather intelligence about the target software then develop an exploit for that software, reflecting the fact that normally cyber weapons have to be developed with a specific target in mind.⁴ Attackers will often utilise “zero-day exploits” which are vulnerabilities that are unknown to the defender or software vendors, thereby increasing the chance of successful intrusion. Next the attackers may receive authorisation and further instruction from political decision makers and then find a way of delivering the malware to the target. After this, intruders establish command and control over the malware – unless there are pre-planned instructions written into the code. Finally, the intruders can verify they have the correct target and choose whether to add more malicious code before activating the payload and assessing and confirming the achievements of the mission.

Given the proliferation of offensive cyber operations (Smeets 2018), there is a growing body of policy-focused literature to explore how threats can be mitigated. For example, cyber defence has been conceptualised in terms of technological, operational, and policy innovations (Cyber Task Force 2017, 16-17). Technical innovations include intrusion detection systems, firewalls, antivirus software, encryption, and automatic security updates. Operational innovations include Computer Emergency Response Teams, cyber security training exercises, and security certifications. There is moreover a very active debate about the most effective international strategy for reducing cyber conflict including deterrence, active cyber defence, and norms (Nye 2016/2017; Gartzke and Lindsay 2019; Healey 2019; Harknett and Goldman 2016; Finnemore and Hollis 2016; Stevens 2012).

The emerging literature has done much to advance our understanding of the nature of cyber conflict. However, one of the main shortcomings is that while there are strong efforts at theorising about the issue, there is a deficiency in research that adopts the empirical methods of political science that are commonplace in the broader discipline. Gorwa and Smeets (2019) identified 70 cyber conflict-related articles published in top IR journals from 1990 to 2018 and find that the majority engage in theory-building rather than theory-testing and they identify only six articles that employ a large-N study or conduct experiments. Moreover, the case study research that exists predominantly focuses on a small number of dominant incidents such as the attacks against Estonia, Georgia, the Sony hack, and Stuxnet (Gorwa and Smeets 2019, 16).

⁴ Some cyber weapons are generic rather than targeted. For a more in-depth analysis of this distinction see Rid and McBurney (2012).

Although some have responded critically to the use of quantitative methods in cyber conflict (Kello 2018, 11), increased methodological diversity – which includes qualitative and quantitative research – should be welcomed in order to empirically test the growing number of hypotheses proposed about cyber security and international politics. One of the few examples of quantitative research in this area is by Valeriano and Maness (2014) who have compiled the first data set of cyber conflict incidents between pairs of rival states. In the most recently updated version of the dataset, they record a total of 266 cyber incidents from 2000 to 2016 between countries that perceive one another as strategic competitors and enemies. Figure 1 shows the annual number of incidents that have been carried out or sponsored by nation states against their rivals according to their coercive intent. The data suggests that while cyber incidents are on the rise overall, the more serious degradation type operations remains relatively low.

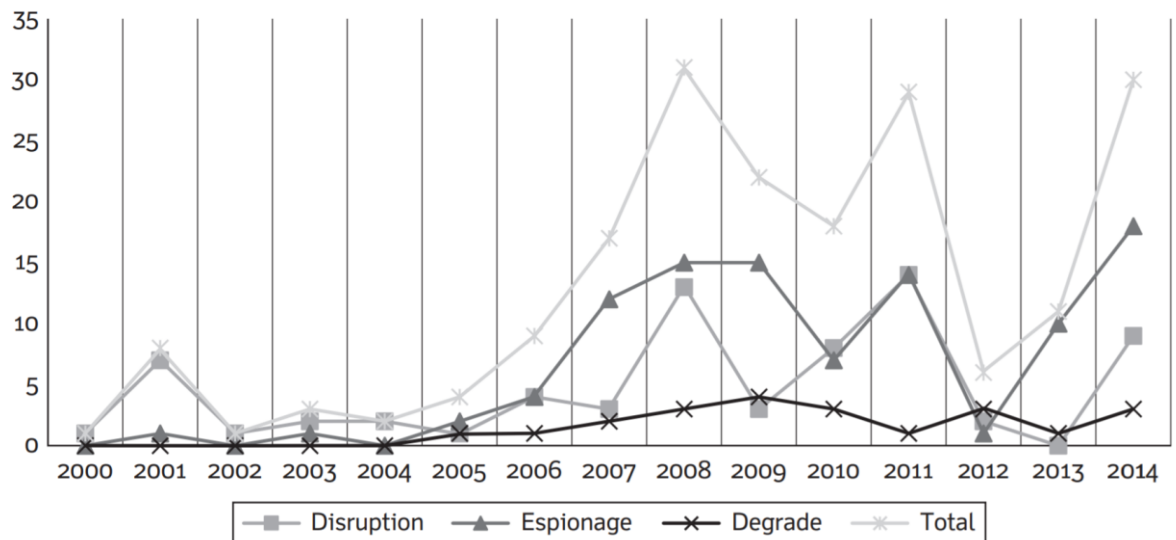


Figure 1. Yearly Cyber Incidents, Coercive Intent: 2000–2014 (Valeriano, Jensen and Maness 2018)

Other findings from this data show that in general cyber conflict is relatively uncommon, low in severity, regional in nature, yet increasing in frequency (Valeriano and Maness 2014; 2015; Valeriano, Jensen and Maness 2018). Furthermore, the data shows that only 6% of cyber operations have caused a change in behaviour in another state as intended by the initiator (Valeriano, Jensen and Maness 2018, 17), which directly engages with the debate about the strategic utility of cyber operations (Gartzke 2013; Smeets 2018). Another quantitative study by Kostyuk and Zhukov (2017) demonstrates that cyber incidents had very little effect on the broader battlefield events in the Ukraine and Syria conflicts. Quantitative research can therefore be useful in providing evidence

to address the prominent theoretical questions raised in the literature, including the prevalence and impact of cyber conflict.

There is need for further efforts in data gathering and analysis in this area because the issues about the likelihood and consequences of cyber conflict cannot be addressed fully through theoretical debate alone or through case studies of single events that are potential outliers. There is also much scope to move beyond investigation of cyber conflict to other aspects of international competition. As discussed later in this chapter, there is a dearth of empirical research on the rapid build-up of cyber weapons and capability globally (Deibert 2011). This thesis addresses these gaps by investigating the proliferation of cyber capabilities through quantitative methods. With newly collected data on the means to conduct computer network operations, new insights can be made into the future of cyber conflict.

Power and Capability

It is evident from the previous discussion that states are increasingly employing digital technologies to exert influence in the cyber domain. This begs the following questions: what gives political actors the ability in the first place to engage in cyber operations, and why are some states more active and effective in this domain than others? A central contention of this thesis is that to answer these questions, we must account empirically for the potential of states to pursue influence in the cyber domain, but this has not yet been achieved in the existing literature. The concepts of power and capability are highly relevant to this issue and must be discussed here to help define terms and clarify the approach taken in this thesis.

Power is a ubiquitous concept in IR scholarship. It is particularly central in the realist tradition which views the distribution of power in the international system as a key determinant of peace and war (Levy and Thompson 2010, 29). For classical realists, international politics is a struggle for power between nation states. As Morgenthau (1948, 13) writes: “whatever the ultimate aims of international politics, power is always the immediate aim.” For structural realists, power provides the means to ensure survival in the anarchical international system lacking centralised governance (Mearsheimer 2016). Although there is disagreement among structural realists over how much power should be obtained, they agree that international politics is a zero-sum game in which states calculate their power and standing in relation to one another (Waltz 1979; Mearsheimer 2001).

There are at least two ways of thinking about national power that are relevant to this research. The first is to equate power with resources. This approach, also known as the “elements of national power” (Morgenthau 1948, 80), conceptualises power in terms of the relevant resources, attributes, or assets the country possesses (Baldwin 2002, 237). This approach has generally been adopted by

realist thinkers. Morgenthau (1948) offers a set of material indicators of power: geography, natural resources, industrial capacity, military strength, population, and non-material indicators of power: national character, national morale, diplomatic skill, and quality of government. Similarly, Waltz (1979, 131) lists population, territory, natural resources, economic capability, and military strength, as well as political stability, and competence. The term, capabilities defined by Holsti (1964) as “any physical or mental object or quality available as an instrument of inducement” is largely synonymous with national resources.

In line with this tradition, Mearsheimer (2001, 57) conceptualises power purely as the state’s material capabilities, arguing that power represents “nothing more than specific assets or material resources that are available to the state”. He distinguishes between military power, indicated by active military forces and nuclear weapons from latent power, indicated by societal resources like wealth and population that can be converted into military capability over the longer term.

This power-as-resources approach is criticised by non-realist scholars who argue that power is not evident in any set of resources but through the relations and interactions between social actors (Baldwin 2002, 240). The most well-known definition of this “relational” approach to power analysis refers to the ability to influence and control others. This is often referred to as the “first face” of power articulated by Dahl (1957, 202-203) who argues that actor “A has power over [actor] B to the extent that he can get B to do something that B would not otherwise do”. Nye (1990, 155) argues along similar lines when he writes that the “proof of power lies not in resources but in the ability to change the behaviour of states”.

The concept of relational power has been expanded according to the scope and nature of influence that is being exerted. Bachrach and Baratz (1962) introduced the “second face” of power which is the ability to set the political agenda and suppress the policies available for consideration. Influence in this sense is achieved through the exclusion of certain issues from the policy table. Lukes (1974) later proposed the “third face” of power which refers to the ability to influence others’ beliefs and desires and shares similarities to Nye’s (1990) theory of soft power about shaping other states’ preferences so that they willingly change their behaviour. Finally, the “fourth face” of power, as developed by Foucault, refers to productive power. This is power that not exercised intentionally but resides within social structures and discourses and works to constitute social actors (Digeser 1992).

This concept has been developed further by Barnett and Duvall (2005, 39) who define power as “the production, in and through social relations, of effects that shape the capacities of actors to determine their circumstances and fate”. They propose that power can exist in the interactions between actors or can help to constitute actors and define their interests. Furthermore, power is either exercised directly and immediately, or diffusely at a “physical, temporal, or social distance” (Barnett and

Duvall 2005, 48). They introduce a typology delineating four types of power: compulsory power, institutional power, structural power, and productive power (2005, 49-55).

When it comes to empirical research, the relational, or power-as-outcomes approach has some disadvantages compared with the power-as-resources approach however. As Beckley (2018, 11-14) argues, the power-as-outcomes approach is difficult to apply to quantitative research because it requires the investigator to know each actor's preferences in order to ascertain whether preferred outcomes were achieved in each specific event, which is very challenging to do for many countries over many years. Tallying up each state's resources on the other hand is much easier to achieve across time and space. Secondly, the outcomes approach can only assess power that has been exercised in previous events and cannot be used to measure potential power that could be employed in the future. Third, it could lead one towards counterintuitive conclusions about the relative power of countries if, for instance, a country with much greater resources (e.g. the United States) was defeated in a war by a country with much fewer resources (e.g. Vietnam) because of other factors such as strategy, resolve, or luck.

Power and capabilities are clearly two distinct concepts, where power is a form of influence and capabilities are the resources that may help explain when political actors will achieve influence. Capability estimates should therefore be seen as "probabilistic predictions of outcomes under specified circumstances" (Baldwin 2016, 119). My approach centres on capabilities rather than outcomes. A focus on capabilities is advantageous as it allows power potential (Baldwin 2016, 68) to be assessed independently from foreign policy outcomes and allows questions such as the relationship between capabilities and conflict to be examined. Measuring capabilities allows the researcher to examine to what extent the means are instrumental to the end. However, the issue remains of defining what the end is. When assessing capabilities, one must still answer the question: the capabilities to do what (Baldwin 2016, 114)? As Sprout and Sprout (1965, 21) explain:

"without some set of given undertakings (strategies, policies), actual or postulated, with reference to some frame of operational contingencies, actual or postulated, there can be no estimation of political capabilities."

The Correlates of War data collection program measures power in terms of demographic, industrial, and military resources with reference to the ability to project or resist influence in international politics (Bremer 1980). Their data are primarily used to explain war or militarised dispute onset and outcome (Geller and Singer 1998). It is assumed that the more capabilities a country possesses, the better placed it is to exercise or resist influence in international conflict. In measuring national cyber capabilities, the types of outcome or influence that states want to achieve through their use of cyber capabilities will have to be specified. This step – taken in chapter 4 – is necessary before deciding upon the data indicators, otherwise one would be collecting data blindly without a frame of reference.

Creating a valid index of national capabilities is a question of first accurately identifying the key components of capability and of then combining them using a suitable methodology (Merritt and Zinnes 1988, 149). National capabilities can be measured by single variable indicators or a composite variable consisting of various indicators.⁵ Single variable measures are attractive because of their simplicity as they require less data sources and mathematical manipulation (Merritt and Zinnes 1988, 143). The single variable measures that have previously been used or proposed include economic and industrial indicators such as Gross National Income (GNI) (Knorr 1956), Gross National Product (GNP) (Organski 1968, 209), Gross Domestic Product (GDP) (Goldstein and Pevehouse 2007, 57), or fuel and electricity consumption (Russett 1968).

Other scholars argue that a single-variable approach fails to provide an accurate picture of the range of capabilities a state may possess. The most powerful countries, according to Waltz (1979, 131), are those that perform well across all areas, not just one. Brooks and Wohlforth (2016, 14) suggest that a multi-dimensional approach to assessing capabilities is crucial since a country with capabilities in only one area will not be able to pursue its full range of strategic interests as effectively as one with a comprehensive portfolio of capabilities. The multi-dimensional approach to measuring capabilities is common in the IR literature and involves combining various dimensions of capability under one composite variable.

By far the most widely used multivariate measure of capabilities in IR is the Composite Index of National Material Capabilities (CINC) developed by the Correlates of War Project (Singer 1988). The CINC was first created to investigate the link between capability distribution among states and the incidence of war (Singer, Bremer, and Stuckey 1972), and has been frequently used as a control variable in quantitative studies since (Hensel 2012, 53). The index measures the proportion of total capabilities in the international system held by a state and is constructed from six data components which together gauge the demographic, industrial, and military dimensions of material power. The composite variable is calculated by averaging a country's share of capabilities across each of the six components.

The logic behind the choice of indicators is to capture resources at the long term, intermediate term, and realised stages (Bremer 1980). The demographic variables (total and urban population) measure the manpower the state can convert to industrial or military capabilities over the long run, the industrial variables (iron and steel production and energy consumption) represent intermediate term capabilities as the state produces the tools of warfare, and the military variables (military spending and personnel) are the capabilities the state can put into action in the immediate term. Since it is a

⁵ There have been many of attempts at estimating national power. Hohn (2011), for instance, reviews fifty-one multivariate formulae used to rank and compare countries, too many to review here.

relative measure, an individual state's capability is dependent on the capabilities of other states. Each component is given equal weighting since there is no theoretical justification to the contrary.

Recent scholarship suggests that measures of power should be based on net assessments of capability rather than gross assessments of capability. Beckley (2018) criticises measures solely based on a state's total resources, like the CINC or GDP, because they overestimate the power of the most populous countries and fail to account for the costs of having a large population on the efficiency with which resources are used. He advises that capabilities are best measured by giving equal weight to a state's gross resources and its resources per capita to control for population. He multiplies GDP by GDP per capita to create a new measure of capability and shows that this method performs better at explaining international conflict outcomes (Beckley 2018, 38). As will be explained in chapter 4, I adopt a similar approach to Beckley (2018) to create an index of latent cyber capability. Now that the concept of capability and approaches for its measurement have been established, it is important to review how these concepts have been applied in the cyber security literature.

What do we know about cyber power and capability?

The study of cyber power is a relatively prominent area of research in the nascent cyber security and IR literature. Most of this work has sought to develop relational notions of cyber power, while much less effort has been undertaken on the power-as-resources approach including developing quantitative measures of cyber capability.

Some scholars have applied the concepts of relational power to the cyber domain. This includes Nye (2011, 130) who adapts the "three faces" of power to cyberspace with "hard" and "soft" variants of each face. The first face, which is about changing the behaviour of an opponent, can be exerted through hard means like DDoS attacks and malware infections, and through soft means such as information campaigns to change the behaviour of hackers. The second face, which involves removing the range of choices an opponent has, can be achieved through hard means such as firewalls and through soft means like introducing software standards. Finally, the third face, which is about changing preferences so that an opponent will not even consider certain options, can be produced through hard means such as threatening arrest to online bloggers and soft means like restricting information online.

Barnett and Duval's (2005) power typology has also been adapted for the cyber domain (Betz and Stevens 2011, 45-53; Stevens 2017). Compulsory cyber power involves direct coercive action to shape another actor's behaviour to one's own will, which might involve computer hacking but can also include non-cyber means such as sanctions to change behaviour in cyberspace. Institutional cyber power is about influencing the workings of institutions in a way that shapes the actions of

another actor. One example is the influence the United States has held over the global assignment of domain names through the Internet Corporation of Assigned Names and Numbers (ICANN) which until 2016 was part of the US Department of Commerce (Strickland and Hill 2017).

Thirdly, structural cyber power is evident in the ways that internet technology can “maintain” or “disrupt” structures of world politics, for instance, the reinforcement of the global capitalist system through information technology or the ability of citizens to challenge established authority through social media (Betz and Stevens 2011, 48). Finally, productive cyber power is about shaping narratives and discourses. An example is how the Tallinn Manual has changed the legal language surrounding cyber weapons which has since been incorporated into national cyber policies (Stevens 2017).

The cyber power literature has been highly useful in identifying the range of mechanisms by which influence can be exerted in cyberspace. There is a research gap nonetheless in an empirical assessment of the capabilities which could be employed to achieve these various effects. Scholars have theorised about the potential implications of the proliferation of cyber weapons (Liff 2012) and published policy guidance of how to manage this process (Bellovin, Landau and Lin 2017; Morgus, Smeets and Herr 2018). Yet, while there is recognition of a “substantial build-up of military cyber capabilities across the globe” (Stevens 2012, 166), there is very little knowledge of this phenomenon based on observation and systematic data collection.

Existing empirical studies, moreover, commonly employ single, qualitative case study methods. These cases have included the Stuxnet cyber operation to assess US capabilities (Lindsay 2013; Slayton 2017), China’s capabilities (Ball 2011; Inkster 2016), North Korea’s capabilities (Feakin 2013), or the growth of capabilities between two pairs of rival states (Craig and Valeriano 2016). Individual cases may be outliers and are insufficient for testing or developing a general theory about cyber capabilities.

Quantitative work is especially rare. The quantitative research that has been carried out is limited in sample size (Brantly 2014) or assesses cyber capacity more broadly in terms of societal resilience rather than at the level of cyber operations (Makridis and Smeets 2019). A recent study from the Harvard Kennedy School has attempted to quantify cyber power by combining a series of indicators of resources and intent, yet the study only covers 30 countries and includes no time series dimension (Voo, et al. 2020).

The lack of quantitative research could be down to the perception that data is inherently difficult to collect in the cyber domain, or the scepticism of many IR scholars to the significance of cyber security in global politics (Kello 2018, 9-11). Our knowledge of cyber capabilities is further limited by the fact that information often comes from non-academic sources such as the media, defence departments, or cyber security firms which might lack rigor or even introduce bias. Each of these

actors may have a financial or political incentive to hype or exaggerate the capabilities of various international political actors (Brito and Watkins 2011).

Measuring cyber capabilities is certainly a challenging endeavour. In the conventional military arena, rival governments can observe each other's military hardware or at least see evidence of their production with relative ease. Yet, many aspects of cyber capability are of a non-physical nature. An ideal indicator of offensive capability could be the amount and sophistication of malicious code each government has acquired, but these "cyber weapons" (Stevens 2017) exist as lines of code on a computer system and are unobservable and uninterpretable unless you are a trained technician and have access to the computer systems where they are stored. Walt (2010) makes a related point that one requires a deep technical understanding of computers to make meaningful threat assessments which most IR scholars presumably lack.

The difficulties are complicated by the secrecy that governments maintain over their precise capabilities. This is especially true for cyber weapons, which have a short shelf life. Once they are employed against a target the software vulnerability will then be identified and patched, rendering the cyber weapon useless for future operations. It may not even take until the zero day is employed before a system is updated or a vulnerability identified and patched. As a result, cyberweapons take on a "transitory nature" (Smeets 2018), making them incredibly difficult to measure in any systematic way.

Yet, there are other feasible methods for estimating capabilities as this thesis proposes. For instance, newly established government agencies dedicated to computer network operations are harder to hide, and information on their budgets and personnel are now often in the public domain. Furthermore, in trying to build a credible deterrent threat, governments may have a reason to be more open about their developments in capability. Although IR scholars may lack technical computer science knowledge, they can employ social science research methods to analyse these developments from a broader level of analysis (Valeriano and Maness 2018).

Aside from academic analyses, several think tanks and private companies have published assessments of cyber security preparedness that I review below. Many use synonyms for capability such as maturity, readiness, or power, but all broadly aim to measure the capacity for countries to be resilient to cyber threat. In these studies, countries are evaluated against several indicators which are often combined numerically into an index or ranking system.

Some of these indices are confined to specific geographical areas and as such limited in the number of countries assessed. These include the Cyber Maturity in the Asia-Pacific Region index, which includes 23 countries from the South East Asia and the Pacific region. Maturity here is defined as "the presence, effective implementation and operation of cyber-related structures, policies, legislation and organisations" and measured with eleven indicators across five categories:

governance, cybercrime enforcement, military application, digital economy and business, and international engagement. This index mostly gauges broad societal indicators and makes only a scant evaluation of the military dimension of national cyber security. The index puts the United States, South Korea, and Japan as the top three most capable countries in the South East Asian and Pacific region (International Cyber Policy Centre 2017).

Other regional based assessments include the EU Cyber Security Dashboard (BSA: The Software Alliance 2015) and the Asia-Pacific Cyber Security Dashboard (BSA: The Software Alliance 2015). The EU Cyber Security Dashboard contains 25 indicators for the 28 EU members classified into legal foundations, operational entities, public-private partnerships, sector-specific cybersecurity plans, and education. The Asia-Pacific Cyber Security Dashboard has 31 indicators with the addition of the cyber law indicators category. These assessments provide helpful information on a wide range of policy developments such as the creation of national cyber security strategies and national computer incident response teams, although the military dimension is ignored. These efforts are limited because unlike the other assessments reviewed here the indicators are not quantified and combined into an index to give an overall assessment of cyber capability.

The National Cyber Security Index has been developed by the Estonian E-governance Academy since 2012 and by 2017 it included 47 countries in its assessment of the ability of countries to “prevent cyber threats and manage cyber incidents.” It puts much emphasis on the government mandated steps taken to protect against cyber threats using 46 indicators grouped into 12 types of capacity. It provides an extensive breadth of indicators and has a national focus, but it can sometimes produce counterintuitive results given that at the time of writing Greece, Czech Republic, and Estonia were ranked as the top three countries (E-Governance Academy n.d.).

Containing a much larger group of countries is the Global Cyber Security Index first published in 2015 and updated in 2017 by the International Telecommunications Union (ITU). It covers 193 UN member states plus Palestine and uses 25 indicators to measure their cyber security development in the areas of legal measures, technical measures, organisational measures, capacity-building, and cooperation. Its main strengths are its global coverage of countries and breadth of information. The index is strong on the policy and legal developments, but much less so on the military and operational aspects of cyber security. According to this index, Singapore is ranked highest followed by the United States and Malaysia (International Telecommunications Union n.d.).

The 2015 Cyber Readiness Index by the Potomac Institute for Policy Studies considers cyber security to be essential for preventing damage to economic development and aims to provide policy makers with a framework for assessing capabilities and a pathway towards full cyber readiness. It assesses the cyber capabilities of 125 countries across seven categories: national strategy, incident response, e-crime and law enforcement, information sharing, investment in research and development,

diplomacy and trade, and defence and crisis response. Within each category are several sub-indicators. Each component of readiness is classified as either insufficient in evidence, partially operational, or fully operational, yet despite this scoring mechanism there is no country ranking like other indices. There is a selection bias towards countries with higher levels of economic development. However, unlike the ITU indices, it gives substantial treatment to military cyber capabilities and accounts for the presence of national cyber defence units (Potomac Institute for Policy Studies 2015).

The final index reviewed here is The Cyber Power Index. It measures the resilience of states and their economies against cyber-attacks across four categories: Legal and Regulatory Framework, Economic and Social Context, Technology Infrastructure, and Industry Application. The index is notable in its use of several quantitative indicators to assess IT infrastructure, although it has much less emphasis on government-led cyber security policies and capabilities. The greatest limitation of the index however is its confinement to the G20 countries. The United Kingdom, United States, and Australia are ranked as the top three most capable countries respectively (Economist Intelligence Unit 2011).

These efforts are of varying value to policy makers and researchers. Their methods and data vary widely in terms of the number of countries analysed, indicators used, and their scoring and indexing methods. As a result, so do their conclusions about the most capable countries. Unlike this research, they do not provide a time series dimension to their rankings, making it impossible to assess how capabilities have changed over time. They provide only a snapshot of information from one point in time rather than across time and are therefore of limited value to scholars who require a greater number of data points to make stronger conclusions about the dynamics of cyber power. Furthermore, while these assessments take a holistic approach to cyber power, they lack grounding in established IR theory and approaches to power and capability and as a result are limited in their applicability to answering the key debates in the cyber security literature. To engage with foundational IR theories related to capabilities and conflict, we need information on what capabilities states have established to conduct and defend against cyber operations.

Most importantly, these efforts lack a common and precise definition of the concept of cyber capabilities which is an essential step towards building a body of empirical knowledge on this issue. Nye (2011, 123) defines cyber power in two ways. Firstly, from the relational perspective he defines cyber power as “the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain.” From the power-as-resources perspective, he writes that cyber power is based upon “infrastructure, networks, software [and] human skills” (Nye 2011, 123). While the latter definition hints at the concept of cyber capabilities developed in this thesis, the concept requires a clearer specification and operationalisation.

Overall, there is a gap in the literature in understanding the sources of cyber capability and in developing an empirical measure of the concept. As will be explained in greater depth in chapters 4 and 5, I operationalise cyber capabilities first in terms of latent skills and knowledge, industry, and infrastructure in a society and secondly in terms of the governmental and military agencies tasked with conducting defensive or offensive computer network operations. I make this distinction because the former should be one of the key explanations for the development of the latter.

Theoretical position of thesis

At this stage it is necessary to provide an explanation of where this thesis sits within the broader IR theoretical landscape. My approach is mostly aligned with the work of quantitative international security scholars who emerged out of the debate between the “traditionalists” and “behaviouralists” in the 1960s. The behaviouralists aimed to study international politics in a more scientific and systematic manner (Schmidt 2002, 19; Vasquez 2004, 39-43). This is traced back to scholars like J David Singer and the Correlates of War project which sought to develop the discipline’s knowledge of the causes of conflict through the quantification of concepts such as war, capability, and alliances (Singer 1979; Singer and Small 1966; Singer, Bremer and Stuckey 1972).

In general, this approach to the study of IR seeks to collect data on the attributes and behaviour of political actors (Mitchell, et al. 2012, 7), but does not wed itself to any particular IR paradigm such as realism, liberalism, or constructivism. Instead it empirically tests hypotheses drawn from a range of perspectives. My aim here is similarly to collect and analyse data on the concepts of cyber capabilities and conflict, but I am not arguing that one IR theory is more useful than another. Rather my approach is inductive, and my conclusions are guided by the empirical findings.

Having said that, theoretical decisions must be made to focus the study and many aspects of my approach and the arguments I test do derive from the “constellation” of realist theories (Levy and Thompson 2010, 28). For instance, my analysis takes the state as its unit of analysis, assesses national capabilities, and derives some hypotheses from the notion of the security dilemma. In many ways this reflects the realist assumptions of international politics as a struggle for power and security between groups (in this case nation states) operating in an anarchical environment (Wohlforth 2008, 133), and where explanations for state behaviour are found in the international system rather than the domestic sphere (Vasquez 2004, 37).

One of the main reasons why realist ideas are drawn upon in this thesis is that they have a lot to say about the causes of arms build-ups and conflict in the international system in terms of testable hypotheses that relate directly to my research questions. Realism, with its emphasis on “states’ competition for power and security in a high-threat international environment”, has traditionally

proposed answers to these questions more so than other perspectives (Levy and Thompson 2010, 28; Bennet and Stam 2004, 37).

Given its dominance over these issues, there is a longstanding engagement with realism in the quantitative literature on the causes of war. Yet these scholars are not necessarily proponents of realism. They are instead engaged in “systematizing realist work according to their own criteria of adequacy and then quantitatively testing the hypotheses they derived from the paradigm” (Vasquez 2004, 42). Some are critical of realist prescriptions including Senese and Vasquez (2008) whose “steps-to-war” theory suggests that many realpolitik foreign policy practices such as building arms, forming security alliances, and taking a hard-line stance to threats, do not deter but in fact increase the probability of conflict.

I am likewise interested in exploring whether realist-based explanations have empirical validity in the cyber domain. Many assessments of capabilities and conflict in cyberspace have their roots in realist theories including the security dilemma (Buchanan 2016), balance of power (Klimburg and Faesen 2018), or the offense-defence balance (Lieber 2014). It is necessary therefore to discuss realist theory here to highlight its relevance to debates about cyber power.

The basic tenet of realism is the assumption that the anarchical international system creates pressure on states to adopt self-help measures to assure their security (Wohlforth 2008). The adoption of military capabilities is the key tool for a state to ensure its survival as they enable a state to defend itself and to deter foreign aggression.

The security dilemma describes the phenomenon whereby efforts by one state to enhance its security, through the development of military capabilities, decrease the security of others (Herz 1950; Jervis 1978, 169; Booth and Wheeler 2017). Actions such as military build-ups are often perceived as threats by other states who then take similar measures to enhance their own security. This process is often termed the spiral model with each build-up forcing a counter reaction (Glaser 2004, 44). The spiral model is at the heart of traditional conceptualizations of an escalating arms race which are said to cause rapid shifts in the distribution of power, an increase in international tension, and a greater risk of miscalculation and conflict (Richardson 1960). IR scholars have studied the effects of arms races for decades and there is a large body of evidence suggesting that arms races contribute to conflict escalation (Wallace 1979; Sample 1998; Gibler, Rider and Hutchison 2005).

Security dilemmas are said to be more intense and arms races more likely when 1. The advantage lies with the offence, and 2. When offensive and defensive weapons are indistinguishable from one another. Some have suggested that the cyber domain is inherently predisposed to these phenomena. As Lord and Sharp (2011, 28) write:

“Offensive dominance creates a great risk of cyber arms races. States ... are likely to view the prevalence of offensive cyber threats as a legitimate rationale for bolstering their own capabilities, both defensive and offensive, thus fuelling an action-reaction dynamic of iterative arming”.

The offence-defence balance has been considered by some realists to be a “master key to the cause of international conflict” (Van Evera 2001, 190). Offence-defence balance theory predicts that if offensive capabilities are deemed cheaper, easier, and more effective than defensive capabilities, states will be incentivised into developing offensive capabilities and engaging in offensive operations (Jervis 1978; Van Evera 1998). It is commonly believed that cyber offence has the advantage over cyber defence due to the perceived low cost of offensive action and the inherent difficulties of defending in cyberspace (Lieber 2011, 100-101).

Secondly, offensive cyber capabilities are hard to differentiate from defensive capabilities in cyberspace. As Buchanan (2016, 7) points out, the security dilemma is particularly strong in cyberspace given the virtual and unobservable nature of cyber weapons, the overlapping skill-set is for offence and defence, and because a country’s cyber warfare agencies cannot easily be distinguished into offensive and defensive roles. This would suggest that a state cannot build-up its cyber security without inadvertently threatening other states and sparking a cyber arms race.

An intense cyber security dilemma may be driving the proliferation of cyber capabilities, but this needs to be empirically tested. Deibert (2011) discusses the emergence of the cyber arms race characterised by the increased “militarisation” of cyberspace, or “the growing pressures on governments and their armed forces to develop the capacity to fight and win wars in [the cyber] domain” (Deibert 2011, 2). The action of the United States in 2010 to unify military cyber capabilities under a new military organisation called Cyber Command will in his view motivate other states to develop similar capabilities (Deibert 2011, 2).

State activity in cyberspace is also frequently framed within the context of balance of power theory. Balance of power is a longstanding hypothesis in the realist paradigm that suggests states will automatically develop their military capabilities or form alliances to counterbalance the dominant power in the international system (Waltz 1979; Schweller 2016). Some have applied this idea to the cyber domain to suggest that weaker rivals to the United States invest in cyber capabilities as a cheaper method of challenging its dominance in international politics (Feakin 2013, 68). The US military claims that “a wide range of actors use ICT and advanced technologies as a relatively inexpensive way to gain parity with the US as compared to buying tanks and aircraft or training thousands of soldiers” (The United States Army 2010, 11).

For realists, the acquisition of military capabilities is key to deterring aggression from other states and maintaining national security (Morgenthau 1948, 14). Deterrence through punishment aims at

discouraging attacks through a demonstration of one's military capacity and willingness to respond in kind. Deterrence theory rose to prominence during the Cold War because of the threat of mutually assured destruction from nuclear weapons (Quackenbush 2011, 751). Deterrence logic also influences cyber strategy. For example, in its national cyber security strategy, the U.S. government policy is aimed at "convincing a potential adversary that it will suffer unacceptable costs if it conducts an attack on the United States" (Department of Defense 2015, 11) and the UK government too has spoken explicitly about the need to respond to cyber incidents with offensive actions (Elgot 2016).

Scholars that are critical of realism argue that military build-ups are likely to lead to an escalation of conflict and deepening of rivalry (Senese and Vasquez 2005; Valeriano 2013). Analysing data on cyber capabilities is therefore crucial to determine whether they can in fact deter cyber conflict, or whether they instead increase the probability of cyber capabilities being used offensively.

As this is one of the earliest attempts at a quantitative assessment of cyber capabilities and conflict, drawing hypotheses from IR theories that have been most frequently applied to these issues both in the non-cyber and cyber environments is an appropriate starting point. The analysis can help show whether these approaches have validity or whether different perspectives are warranted for future research.

That being said, many aspects of my approach are not realist. Where possible, I attempt to control for competing explanations for an outcome. For instance, I frequently control for the impact that domestic regime type may have on the development of capabilities or engagement in cyber conflict. The argument that domestic politics influences international conflict is a liberal not a realist theory (Russett and O'Neal 2001). An in-depth analysis of domestic based explanations is not undertaken, however, in this thesis. For instance, harkening back to Eisenhower's idea of the military-industrial complex (Ledbetter 2011), Deibert (2011, 5) attributes the acquisition of capabilities to a nascent "cyber-military complex" whereby defence contractors and other private cyber security firms promote their products to military and intelligence agencies. Others have raised the issue of the military-Internet complex, or the conjunction of a military establishment and large cyber security industry selling cyber weapons to governments (Singer and Friedman 2014, 162), which raises interesting questions about external versus internal drivers of cyber build-ups. Unfortunately, not all explanations can be examined in this study.

Many of the resource-based concepts I derive (such as scientific and technical knowledge) are furthermore not the domain of realism. These factors are relevant across a wide range of academic disciplines including economics or science and technology studies (Comin and Mestieri 2014). The concept of interstate rivalry, which forms part of my explanation for the diffusion of cyber capabilities and conflict, is also not a realist perspective. Rivalry research developed as a methodological tool to help explain the causes of interstate violence, given the finding that most

interstate conflict is fought between states that have engaged in repeated disputes over extended periods of history (Hensel 1999, 178).

Some readers may argue that by conceptualising capabilities in terms of national resources and focusing my analysis at the level of the state I am adopting a realist standpoint. While this approach may align itself with realism, these decisions were made for pragmatic reasons rather than because they are realist. As I explain later in this chapter, I focus on capabilities as state resources and assets rather than power as outcomes or influence (Baldwin 2002). This is because firstly resources can be more feasibly measured and compared across countries - unlike the concept of influence - and secondly because by measuring capabilities independently from outcomes, I can test how capabilities affects the outcome (engagement in conflict) which is one of my research questions (Beckley 2018, 11-14).

I take a state-centric perspective partly because of data availability. There is a much greater wealth of data available for state than non-state actors. While non-state actors are undoubtedly important in cyberspace (Stevens 2012, 8; Whyte and Mazanec 2019, 169-200), the IR field has yet to compile a historical record of non-state cyber incidents for analysis as it has for interstate conflict (Council on Foreign Relations n.d.; Valeriano and Maness 2014). To quantitatively assess the impact of capabilities on cyber conflict, a large sample of previous instances of this phenomenon is required.

To integrate a wide body of literature and give the analysis structure, I adopt a broad theoretical framework known as Opportunity-Willingness (Most and Starr 1989) which is explained in the upcoming discussion. This framework helps derive hypotheses and select indicators for the proliferation of capabilities and conflict in cyberspace. Part one of this chapter will develop the explanation for the determinants of cyber capability proliferation and part two will develop the explanation for the effect of capabilities on conflict.

Conclusion

This research is important from both policy and academic perspectives. As Singer, Bremer and Stuckey (1972, 21) write, “the foreign policy elites of all national states are, at one time or another, concerned with their nation’s standing in the power and/or prestige pecking order.” Today, governments are increasingly concerned about the diffusion of cyber capabilities to rival states. The 2017 Worldwide Threat Assessment by the US Director of National Intelligence notes that “many countries view cyber capabilities as a viable tool for projecting their influence and will continue developing cyber capabilities” and lists Russia, China, Iran, and North Korea as the largest state-based threats (Coats 2017). Tracking the growth and spread of cyber capabilities globally is of strategic importance to governments which can be aided through empirical data and analysis.

Capability rankings have been a source of intense speculation among media, industry, and government, but very few assessments are empirically substantiated. For instance, one report suggests the United States has fallen behind Russia (SC Media 2015). Another article claims Russia and China are “leading the way” with their “catastrophic” capabilities (Seals 2018). One news source asserts that North Korea’s cyber capabilities are greater than their nuclear threat (Wright 2018). These speculations cannot be taken seriously without rigorous analysis. Cyber security policy, like other areas of national security policy, should be informed by accurate assessments of relative capabilities and threat.

As this chapter has demonstrated, there is a gap in the existing literature in measuring the concept of cyber capability and examining its role in cyber conflict. Two questions in particular emerge: Firstly, what motivates and enables states to build cyber capability, and secondly, how do established cyber capabilities affect patterns of cyber conflict internationally. Capabilities are therefore examined as both a dependent and independent variable in this thesis in order to give a broad assessment for the role of this concept in international relations. This chapter has situated this research within the existing literature and highlighted its relevance. The next chapter sets out the specific theoretical framework used to investigate my main research questions on the causes and consequences of cyber capability proliferation.

Chapter III

A Theoretical Framework for Explaining the Causes and Consequences of Cyber Capability

Introduction

The previous chapter established the general context for this research. In this chapter, I establish a more structured theoretical framework to guide my empirical investigations. With the newly collected NCC dataset, this thesis addresses three research aims: to investigate how capabilities have proliferated, identify the determinants of capability proliferation, and assess the effects of capability proliferation on cyber conflict.

The first research objective involves assessing patterns of capability adoption over time and the geographical distribution of capabilities in the international system. This is achieved through an inductive, descriptive assessment of the NCC dataset rather than by studying correlations between variables. The second objective involves identifying the country-level factors that increase the likelihood of the state acquiring active cyber capabilities. Active cyber capabilities are measured by the presence of governmental and military organisations dedicated to offensive or defensive computer network operations. The third objective involves investigating the relationship between capability and the frequency or likelihood of computer network operations being conducted between rival states.

The latter two research aims require an analysis of the causal factors and mechanisms behind a process or phenomenon for which theory is needed to help choose the relevant explanatory variables. State behaviour is shaped by countless factors and it is not feasible to account for them all in a single study. The purpose of theory is to simplify the explanation of a phenomenon down to a few key variables that should matter most. I develop my theory for the causes of capability adoption and their consequences by applying Opportunity-Willingness theory (Most and Starr 1989) which helps explain the creation of active cyber capabilities through a country's capacity and motivation to acquire them. I then draw on the relevant empirical literature on military build-ups and arms proliferation as well as the emerging cyber security literature to produce testable hypotheses.

I structure this chapter by first situating my theoretical approach in the broader context of IR theory, then I set out the theoretical framework for the determinants of cyber capability acquisition based on Opportunity-Willingness theory. I then discuss the IR literature on the adoption of military capabilities from the opportunity and willingness perspectives, apply these concepts to the cyber

domain, and then create hypotheses for the proliferation of cyber capabilities which are tested in chapter 7.

Following this, I expand the theoretical framework to the effect of cyber capabilities on cyber conflict and also draw on the arguments of deterrence versus escalation (Jervis 1978; Glaser 1992). Specifically, I explore whether the presence of cyber capabilities will dissuade cyber incidents or whether they will promote an escalation in cyber conflict. I begin by reviewing these approaches in the context of traditional conflict before applying them to the cyber domain and setting out my hypotheses to be tested in chapters 8, 9, and 10.

Part one: The determinants of cyber capability proliferation

What theories help us explain if and when a state will establish the institutional capacity to engage in defensive or offensive computer network operations? There is no well-developed theory of cyber capability proliferation in the existing literature. As such I draw insight from IR theory and previous empirical studies on the proliferation of military technology to develop a theoretical framework for understanding the determinants of active cyber capability. Given that cyberspace is often viewed by governments as a “warfighting” domain (Department of Defense 2018, 1), it is reasonable to ask whether these approaches are also helpful for explaining the drivers of cyber capabilities.

A multitude of system-level, interstate-level, and domestic-level factors have been used previously to explain arms or capability build-ups. For instance, theories relating to the balance of power (Waltz 1979), system polarity (Goldsmith 2003), the offence-defence balance (Van Evera 1998), international norms and prestige (Sagan 1996; Jo and Gartzke 2007), the security dilemma (Jervis 1978), interstate rivalry (Rider, Findley and Diehl 2011), revisionist intent (Glaser 2004), civil war and domestic repression (Buzan and Herring 1998) the military-industrial complex (Buzan and Herring 1998), the technological imperative (Evangelista 1989; Buzan and Herring 1998), and a state’s financial and organisational capacity for adoption (Horowitz 2010) have previously been used to explain increased military investments or the adoption of specific military technologies.

Opportunity-Willingness Theory

A more parsimonious theoretical framework is needed to simplify this range of possible explanations and provide clear structure to the investigation. The framework I adopt to explain the drivers of active

cyber capability is known as Opportunity-Willingness Theory⁶ (Most and Starr 1989). The framework has been applied to a wide range of issues in international politics including interstate war (Siverson and Starr 1990), democratic peace theory (Gartzke 1998), civil conflict (Furlong, Gleditsch and Hegre 2006), and is commonly used to explain the proliferation of military technologies (Early 2014; Fuhmann and Horowitz 2017; Jo and Gartzke 2007). It is advantageous because it can incorporate a range of relevant factors into a simple framework thus allowing a relatively broad-based exploration of cyber capability to be undertaken.

Opportunity-Willingness Theory was introduced formally by Harvey Starr (1978) as an analytical tool for “ordering”, or categorising, the range of hypotheses on international conflict found in the diffuse literature. It should not be seen as a theory that explains a phenomenon through any single variable or set of variables but as a framework that helps “bringing disparate phenomena together in an orderly manner”, including different levels of analysis (Most and Starr 1989, 24). The central idea of the theory is that the behaviour of a political actor can be explained in terms of its capacity to act given its environment, and its goals or motives given its perception of its environment (Starr 1978, 366). The theory derives from the work of Harold and Margaret Sprout (Sprout and Sprout 1969) on the way a political actor’s environment (for instance, a state’s geographical location or industrial resources and ingenuity) sets the scope of action it can possibly take.

The theory prompts us to consider two broad types of explanation when asking why a state takes a particular action. Opportunity is a structural based explanation for state behaviour and is defined as “the possibilities that are available to any entity within any environment, representing the total set of environmental constraints and possibilities” (Siverson and Starr 1990, 48). The opportunity perspective explains state behaviour based on what is the possible scope of action for a state. A state’s opportunity for waging war for example will be shaped by its geographical proximity to a rival and its material capabilities (including its level of technology to overcome geographical space) (Most and Starr 1989, 31). Capabilities, or resources, are of central importance because they “permit the creation of opportunities” (Most and Starr 1989, 31).

In this study, the state behaviour I am first explaining is the adoption of active cyber capabilities (measured by whether the country has established an incident response team or a military computer network operations unit⁷). To explain this from the opportunity perspective, I argue that the creation of active capabilities will be determined in part by the country’s latent capability or resources (skill, knowledge, wealth, industry etc.). In this sense, I am explaining how one aspect of capability shapes another aspect of capability. As explained in chapter 4, it is for this reason that I distinguish between

⁶ This has alternatively been called the “interest and capacity” theory (Fuhmann and Horowitz 2017) where interest refers to willingness and capacity refers to opportunity.

⁷ The specific variables are explained in chapter 4.

latent and active cyber capabilities, where the former is the explanatory or independent variable and the latter is the outcome or dependent variable to be explained.

Willingness, on the other hand, is an explanation at the decision-making level and concerns the preferences of policy makers. It refers to “the willingness to choose (even if the choice is no action), and to employ available capabilities to further some policy option over others” (Most and Starr 1989, 23). In the context of war, the willingness to go to war is influenced by “real (relatively accurate) perceptions, or distorted and selective perceptions of security and insecurity, threat, hostility, fear or anxiety” (Most and Starr 1989, 35). In the context of this research, willingness is similarly gauged by the state’s threat environment that should motivate it towards adopting a capability. In sum, opportunity relates to a state’s inherent ability to act based on its capabilities, while willingness relates to its motivation to act based on political incentives and pressures.

My central contention is that as the willingness and opportunity of a state increases, the likelihood of active cyber capabilities being adopted will also increase. Opportunity and willingness therefore provide the independent variables to help explain variation between countries in the adoption of active cyber capabilities. In the upcoming discussion, I set out an explanation for the determinants of cyber capability based on opportunity and willingness arguments by first showing how they have been used to explain the proliferation of military technology in the broader IR field and then applying this to the idiosyncrasies of the cyber domain.

Latent resources and military capabilities

The opportunity-side of the theory makes the simple proposition that for a given action to take place, that action must be “at base, physically, technologically, or intellectually possible” (Siverson and Starr 1990, 48). A theory of proliferation based on opportunity would argue that the state’s inherent capacity to adopt capabilities provides the best explanation for why it does so rather than the state’s specific interests. These explanations are generally based on the state’s latent resources that provide the state with the capacity to adopt a policy. Theories of technological determinism are an opportunity type explanation for the adoption of military capabilities because they assume that states will automatically engage in arms acquisitions given that they possess the underlying capacity. These theories suggest that the pressure placed on states to keep up with the continual qualitative advance in technology often initiated in the private sector makes the adoption of military technology by governments an inevitable process, rather than one driven by immediate policy choices (Evangelista 1989; Buzan 1987; Buzan and Herring 1998).

Horowitz’ (2010) “adoption-capacity” theory also explains the spread of military technology primarily in terms of opportunity-based explanations. He argues that willingness-based explanations,

including strategic competition, are not by themselves sufficient to explain technological acquisition because they do not account for whether the state has the capacity to adopt an innovation. Using the cases of carrier warfare, battlefleet warfare, nuclear weapons, and suicide bombing, his theory suggests that the rate and extent of proliferation of a military innovation is determined by each technology's financial and organisational requirements.

Horowitz argues that the financial intensity of an innovation is determined by the unit cost of the technology and whether it is commercially available with dual-use with applications beyond that of the military. Nuclear weapons for example require substantial financial resources because of the high unit cost of the nuclear warheads and their delivery vehicles and because nuclear technology, at least when the weapons were originally developed, was in the purview of the military and not dual-use (Horowitz 2010, 103). Secondly, proliferation depends on the scale of the organisational changes that would need to be overcome to adopt an innovation. Horowitz suggests that the rigidity in how military organisations view their goals, their willingness to experiment, and the age of an organisation are plausible ways of conceptualising organisational ability.

There are a range of relevant resources for explaining the acquisition of military technology. Previous studies have particularly focused on the state's financial resources, industrial capacity, or science and technical knowledge as a reflection of the state's underlying potential to design and produce a military technology. In this study, I will also explain cyber capability adoption based on these types of resources.

The first type of resource required for capability adoption is financial. Every technology, whether domestically produced or purchased, has a financial cost. It follows that wealthier states have more opportunity than less wealthy states to afford a capability. A country's economic capacity in the context of nuclear proliferation has been measured by Gross Domestic Product (GDP) or GDP per capita – an appropriate method for controlling for a country's population (Singh and Way 2004, 867-868; Horowitz 2010, 111). GDP based measures have also been used to explain the acquisition of UAVs (Furhmann and Horowitz 2017, 409) and space launch and satellite capabilities (Early 2014, 58). In these studies, a country's financial resources in terms of GDP are consistently found to be good predictors of the adoption of technologies.

Industrial capability is another type of resource identified in the literature, which refers to the country's ability to convert raw materials and technical knowledge into goods and services. A state cannot become a top-tier power in international politics without a domestic manufacturing base because without the industrial capacity of its own, a country will be dependent on inferior imported military hardware while the privileged countries at the forefront of technological innovation can develop the most advanced tools for warfare (Buzan and Herring 1998, 30).

Industrial-based resources have long been established as an indicator of a state's latent capability in IR theory (Morgenthau 1948, 87) and quantitative research (Singer 1988). According to Morgenthau (1948, 87), the "leading industrial nations have been identical with the great powers." The Composite Index of National Capabilities (CINC) gauges industrial resources by iron and steel production and energy consumption as these are the relevant industrial activities for producing military hardware which in turn can be harnessed to project and resist influence in international politics. In the nuclear literature, industrial capability has also been approximated by steel and iron production and energy consumption (Singh and Way 2004, 868; Jo and Gartzke 2007, 173; Horowitz 2010, 112)⁸. Kinsella (2000, 265) uses the value added by industry to GDP to help explain the production of military hardware for the global arms trade. Industrial indicators often correlate with measures of economic capacity given the contribution of industrial activity to economic output reflected in GDP measures. However, there is a distinction between the ability to manufacture technological products and the country's overall wealth.

A third type of resource or capability is scientific and technical (S&T) knowledge. A country cannot produce technology without the sufficient level of know-how, expertise, or skills in the relevant fields. Knowledge is in fact central to many definitions of technology. For instance, Brooks (1980, 66) defines technology as the "knowledge of how to fulfil certain human purposes in a specifiable and reproducible way." This understanding of technology is distinct from technology as manufactured outputs, or in the military context the "actual instruments or artefacts of warfare" (Ross 1993, 110). This distinction, as Skolnikoff (1993, 13) writes, is "whether technology should be thought of as a piece of physical hardware...or whether it should rather refer to the knowledge base that made the hardware possible." In any case, underlying skills should clearly provide a state with the opportunity to produce capabilities.

The concept of S&T knowledge has been operationalised very inconsistently in empirical studies. In the nuclear literature, scholars often rely on a nuclear weapons production capability index composed of seven components: uranium deposits, metallurgists, chemical engineers, and nuclear engineers/physicists/chemists, electronic/explosive specialists, nitric acid production capacity, and electricity production capacity (Sagan 2011, 230). While this proxy measure partly helps to gauge technical knowledge related to nuclear weapons, it is unsuitable as a general measure of S&T knowledge. Moreover, the index does not separate indicators of scientific knowledge (the presence of scientists and technicians) from raw materials (uranium deposits) or industrial activity (production capacities).

Access to knowledge has been operationalised alternatively by the time that has passed since the technology was first invented under the assumption that knowledge will eventually and inevitably

⁸ Jo and Gartzke refer to this as economic capacity, and it is likely the two are correlated.

diffuse to more countries over time (Early 2014, 61; Jo and Gartzke 2007, 173). Furthermore, Early (2014, 61) uses educational attainment rates to approximate the S&T human capital required for the creation of space-based capabilities. Despite the variation in how this concept is operationalised, these studies have generally found this factor to be an important predictor of the adoption of capabilities. The next step is to apply these concepts and approaches to the cyber domain.

The resource requirements for cyber capabilities

What resources enable a state to establish the capability to conduct cyber operations? There is a widespread assumption that the cyber domain has low financial requirements (Kello 2018, 165). As Nye (2011, 124) notes “the barriers to entry in the cyber domain are so low that non-state actors and small states can play significant roles at low levels of cost.” Although the most sophisticated cyber operations may be financially costly (Lindsay 2013), the basic operational capability is not. The hardware and infrastructure needed to engage in cyber operations consists essentially of a computer and an Internet connection. This is a stark contrast to the high cost of conventional military hardware like aircraft carrier fleets, submarines, tanks, or missiles.

Furthermore, cyber related technology may be relatively cheaper to acquire because of its dual-use nature which also fuels a “technological imperative” (Buzan and Herring 1998, 50) to the adoption of cyber capabilities. Many advances in computer hardware and software are made in the private sector, undirected by governments. The size of the annual US market for cybersecurity reportedly ranges from between \$50 billion and \$80 billion, which according to Deibert (2011, 5), “not only creates a kind of feeding frenzy among defence contractors, but also propels the development of more refined techniques of monitoring, exploitation, and attack.” Since the technology is easily obtainable to the whole of society, states will automatically seek to integrate it into their cyber operations to maintain their status and ability to protect national security.

Given the low unit cost and commercial availability of computer software and hardware, even governments with a modest budget should be able to acquire at least the basic infrastructure and technology. However, an assessment of the cost of cyber capabilities must distinguish between the unit cost of the basic infrastructure and the cost associated with obtaining the skills to develop defensive or offensive cyber technology and to carry out operations. While the basic technology of cyber operations may not be financially costly or difficult to acquire, the real cost comes from the skills of the trained developers and operators of cyber operations. As Slayton (2017, 82) remarks, the “cost of cyber operations will depend not on the features of technology alone, but instead on the skills and competence of the actors and organisations that continually create, use, and modify information technology.”

Skills should be a particularly essential asset in developing CNO capacity because of the low shelf life of cyber weapons. Cyber weapons are highly perishable and can become obsolete over time (Bartos 2016). They are perishable in that once used defenders become aware of the security flaws in their systems and patch the exploited vulnerability. They are at high risk of becoming obsolete because defenders are always looking for vulnerabilities in their systems to fix even before it is attacked. Therefore, adequate levels of technical skill are needed for a state to continually develop malware for new targets. It goes without saying that the development of cyber security software and operations to keep ahead of advances in offensive capabilities should also depend on a state's access to technical skill and knowledge (New York Cyber Task Force 2018).

Less developed states can engage in cyber operations if they invest disproportionate amounts in training their population in the necessary skills. With a GDP per capita of just 1,800 US dollars, North Korea is not an advanced economy, yet has frequently engaged in malicious cyber operations so clearly has some level of capability. From the opportunity perspective, this is explained by the fact North Korea has put great effort into developing hacking skills among its students. Feakin (2014, 72) documents the process by which the North Korean government seeks out talented school pupils skilled in mathematics and sends them to the country's universities to be trained in computer science. These students can then eventually be employed in one of the military's cyber units (Stephen and Lindsay 2015, 4). This point is echoed by Lee (2005, 104-106) who notes that there are over 200 universities in North Korea specialising in computer science and software development, noting that the government funds national Olympiads in these fields.

With its latent skill, North Korea been able to develop active cyber capability as reflected in the "Unit 121" which was created in 1998 and by some reports has between 500 and 6000 professional hackers operating out of it (Mulrine 2015; Lee and Kwek 2015; Hewlett Packard 2014). It is from agencies such as these that North Korea has allegedly carried out its cyber-attacks. These include the hack of Sony Pictures in 2014 where confidential documents were accessed and publicly released in response to the new film "The Interview", which portrayed an assassination plot against North Korean leader Kim Jong Un (Peterson 2014).

The global demand for cybersecurity professionals underlines the importance of technical skill to cyber capability, driven in part by prominent cyber-attacks like the 2007 Estonian DDoS incident (Libicki, Senty and Pollak 2014, 43). The urgent need for skills is apparent in national cyber strategies. In December 2018, the UK government launched a Cyber Security Skills Strategy to help prepare the country against cyber threats. The policy intends to ensure that "the UK has a sustainable supply of home-grown cyber skilled professionals to meet the growing demands of an increasingly digital economy, in both the public and private sectors, and defence" (HM Government 2018, 16). The efforts of the UK government to train and educate society in cyber security are discussed at

length by Stevens (2016, 167-176). Technical skill and knowledge should therefore be one of the key resources that explain proliferation from the perspective of opportunity. States that can draw greater levels of expertise from their population will be better placed to develop operational cyber capabilities than states lacking skill.

The strength of a country's cyber-related industry should also be an important resource in building capability. The software industry is especially relevant to cyber capabilities as it is involved in the designing, developing, manufacturing, and supplying of computer and Internet related technology and services which can be adopted across society by individuals, the private sector, and governments to improve cyber security. One of the reasons Israel is considered a powerful country in cyberspace for example is down to the prominence of its software industry and cyber security start-ups (Tabansky and Israel 2015, 27). The private sector is an important source of the technology and expertise that governments require to build active cyber capabilities. Nonetheless, there are several very active countries in cyberspace that do not have strong industrial bases in software like North Korea or Iran, so it is not a necessary condition.

In light of this discussion, I argue that a country's latent capability, particularly that which is derived from the country's skill and knowledge base, will create the opportunity for action and thus be a key explanation for whether a country acquires active cyber capability. This leads to my first hypothesis:

Hypothesis 1: Countries with greater latent resources, especially the relevant skill and knowledge, will be more likely to acquire active cyber capabilities.

Latent resources are only part of the explanation for proliferation. As discussed in the next section, a country's external threat environment should also be a driver of capability adoption.

Security threats as a driver of military capabilities

The second half of the Opportunity-Willingness theory suggests that a state will be more likely to develop capabilities if it has the willingness to do so. According to Most and Starr (1989, 23), "willingness is a shorthand term for the choice (and process of choice) that is related to the selection of some behavioural option from a range of alternatives". Opportunity-Willingness theory conceptualises willingness in terms of perceived or real security threats (Most and Starr 1989, 35) and posits that the willingness created by insecurity can drive the creation of new capabilities, thus establishing greater opportunity (Most and Starr 1989, 43). This explanation is aligned with realist accounts of military build-ups. According to realism, a state's choice to adopt military capabilities is a function of its international threat environment, and the desire to build-up military capabilities fundamentally arises from the need to deal with aggression in international politics (Jervis 1978).

The anarchical structure of the international system means that states are highly sensitive to threats to their survival and respond to these by enhancing their own power (Waltz 1979).

Security threats can be conceptualised at varying levels of analysis. At the system-level, states are pressured to maintain a balance of power between them and other states because it is against their security interests to allow another state to dominate the international system. Some predict that states will increase their military capabilities (internal balancing) or form alliances (external balancing) to challenge a dominant power or rising hegemon and restore a balance of power in the system (Levy and Thompson 2010, 40). Given that the current international system is considered unipolar (Wohlforth 1999), a key question is how weaker states will attempt to challenge US preponderance given they lack the conventional means to do so (Pape 2005).

The international security literature commonly focuses on external threats to explain the build-up of arms or the acquisition of military technology. In the nuclear literature, for instance, Singh and Way (2004, 872-873) find a positive and significant association between threat (measured by the presence of rivalry and the frequency of militarised interstate disputes) and the exploration, pursuit, and acquisition of nuclear weapons on the other. In addition, Fuhrmann and Horowitz (2017, 410-411) show that a state's acquisition of armed UAVs is positively correlated to its involvement in territorial disputes or experience of terrorism, a logical finding given the application of drones to interstate border surveillance and anti-terrorist operations.

The security dilemma hypothesis suggests that it is the threat represented by the military capabilities of other countries that motivate the arming process. The security dilemma refers to the phenomenon whereby "many of the means by which a state tries to increase its security decrease the security of others", causing an action-reaction pattern of iterative arming (Jervis 1978, 169). A country is likely to perceive the military build-up of a rival country as a potential threat because it cannot be certain that there is no aggressive intent behind the action and will itself be more likely to build-up capability in response. This secondary arms build-up however will increase the insecurity of the original country which will then be motivated further to build arms to restore prior levels of security. The security dilemma drives the action-reaction process of iterative arming among states which is at the heart of traditional conceptions of an arms race (Richardson 1960).

The intensity of the security dilemma, and thus the willingness to develop military capabilities, is increased under two conditions according to Jervis (1978, 186-187): if offensive and defence are hard to distinguish, and if the offence-defence balance favours the offence. If a state cannot tell whether its rival's capabilities are offensive or defensive, and if an offensive strategy is seen as more cost effective and advantageous than a defensive strategy, then uncertainty regarding its rival's intentions will be heightened further and the pursuit of military capabilities intensified.

Identifying the action-reaction process in reality is difficult. Studies have shown for instance that the military spending of the United States and the Soviet Union during the Cold War did not fit this pattern (Organski and Kugler 1980), while another study has shown that military spending (as a proportion of GDP) is explained better by domestic political and economic factors than by interstate competition (Goldsmith 2003). However, there is empirical evidence to suggest major powers are more responsive to their rivals' weapons systems (such as capital ships), as opposed to their military expenditures (Bolks and Stoll 2000).

In examining the determinants of nuclear capability proliferation, Jo and Gartzke (2007, 173-174) measure a state's conventional threat environment based on a country's level of material capabilities compared with the capabilities of its rivals and measure its nuclear threat environment based on whether the state has any rivals with nuclear weapons. While they find that a higher conventional threat is significant linked to further nuclear proliferation, the presence of nuclear-armed rivals appears to deter rather than promote the development of nuclear weapons by a state. Similarly, Early (2014, 64) finds limited evidence that the establishment of space exploration capabilities (civil space agencies, national satellite capability, and domestic space launch capability) are driven by a rival's possession of these assets.

Interstate rivalry presupposes the existence of many of the issues that heighten a country's external threat environment and motivate the arming process. Strategic rivalries are defined in quantitative research as "relationships in which decision makers have singled out other states as distinctive competitors and enemies posing some actual or potential military threat" (Colaresi, Rasler and Thompson 2008, 3). Rivalry is characterised by perceptions of competition and mutual threat between two states, competition over incompatible goals, a continuous pattern of conflict yet with variation in intensity over time, and a propensity for events to escalate into a more serious situation than would be expected outside a rivalry context.

Vasquez (2009, 79) defines rivalry as "a competitive relationship between two actors over an issue that is of the highest salience to them". The most prominent issues at stake in rivalries are territorial disputes (spatial rivalries) and conflict over relative power and influence (positional rivalries). Historically, interstate rivalry, like that between the United States and Soviet Union during the Cold War, has been an important factor in the development of military technology because it enhances the drive to gain and maintain a military advantage over a competitor. Indeed, the empirical evidence confirms that military build-ups are much more likely to occur in the context of enduring rivalry (Rider, Findlay, and Diehl 2011). In the next discussion, the role of threats and rivalry in promoting cyber capability are explored.

The cyber threat environment and proliferation

Explanations for proliferation based on security threats can be equally applied to cyberspace. So, how do cyber threats motivate a state to develop the capability to conduct cyber operations? There are several reasons to believe states will perceive cyberspace as a particularly insecure environment. First, the effects of anarchy may be particularly intense in the cyber domain because of the lack of institutional governance over the proliferation of cyber weapons (Stevens 2017). Liberal institutionalist theory argues that the insecure and conflict-prone nature of the international system can be reduced through the greater engagement of states within international organisations (IOs). By providing information, promoting mutual gains, developing norms, and punishing norm-breakers, IOs can help dissuade states away from conflictual and militaristic policies towards more cooperative behaviour (Russett and Oneal 2001, 161-166). As Nye (2014, 5) points out however, “over the past 15 years, the advances in [cyber] technology have far outstripped the ability of institutions of governance to respond”. While some organisations do exist and some agreements have been reached there are few relating to cyber conflict management or the non-proliferation of cyber warfare technologies, which may result in an unconstrained spread of capabilities.

Secondly, cyber capabilities are considered difficult to distinguish as unambiguously offensive or defensive which entails a more intense security dilemma and greater probability of arms racing behaviour (Rueter 2011, 4; Buchanan 2017, 7; Slayton 2017, 86). At the level of the technology, some tools like firewalls or antivirus software have no offensive component to them and can be classified as defensive, while computer code written to carry out malicious intent is clearly offensive in nature. At the level of operations, however, distinguishing offence from defence is difficult because cyber operations are often ambiguous in their role and the skills set of the operators overlap. Scanning networks for potential threats is seemingly defensive but the same tactic could be used to prepare the groundwork for an offensive action (Buchanan 2017, 112).

Thirdly, there is also a widespread perception that the cyber domain is offence-dominant which may explain the rise in offensive cyber capabilities and operations in the international system. On the one hand, cyber offensive weapons are supposedly very cheap to acquire or develop, technically easy to implement, need only target specific weak spots, act at very high speeds, can have a potentially crippling impact on network dependent infrastructure, and provide attackers with anonymity allowing them to avoid retribution. On the other hand, defensive measures against cyber-attacks are considered expensive, complex, unfeasible in scope, time-consuming, and of little use as a tool for achieving military victory (Lieber 2011, 100-101; Liff 2012, 415; Kello 2013, 22-30). According to Libicki (2009, 39): “another dollar’s worth of offence requires far more than another dollar’s worth of defence to restore prior levels of security”. The effect on policy making could be significant. As

Lynn (2010) argues: “in an offence-dominant environment, a fortress mentality will not work ... the United States cannot retreat behind a Maginot Line of firewalls or it will risk being overrun.”

Several IR scholars dispute the offence-dominance hypothesis (Lieber 2011, Slayton 2017, Gartzke 2013, Lindsay 2014). For example, Lindsay (2014, 385) points to the high costs involved in the Stuxnet operation, which involved considerable efforts in planning and access to the target, as evidence that conducting sophisticated and strategically effective offensive operations is more challenging than it seems. Similarly, Lieber (2011, 103) argues that the inherent uncertainty over the effectiveness of cyber offence as tool for achieving military victory poses a challenge to offence-defence theory in cyberspace. The basic malware and physical infrastructure for conducting operations may well be cheap, but if cyber-attacks cannot be used to do damage to an opponent in any consistent way it may not be meaningful to say the cyber domain favours attacker.

Yet policy makers’ perceptions of the offence-defence balance should logically have a greater impact on their decision making than the actual balance (Van Evera 1998, 6; Gortzak, Haftel and Sweeney 2005, 75). Threat perceptions of offensive cyber activity are clearly on the rise. According to a Pew Research Centre global threats survey, an average of 54% of people in each country in a sample taken in 2017 viewed the threat of cyberattacks from other countries as a serious concern, which increased to 61% in a 2018 survey (Carle 2015). These threat perceptions may be sufficient to motivate states into cyber capability investments.

Another potential source of increased willingness is the country’s experience of cyber-attacks as these highlight the country’s vulnerability and should prompt subsequent efforts to build preparedness against future attacks or to develop offensive cyber tools to retaliate. In the UK’s National Cyber Security Strategy, cyber security capability is frequently discussed in the context of managing cyber-attacks. Here the government sets out its defensive policy of ensuring “UK networks, data and systems in the public, commercial and private spheres are resilient to and protected from cyber-attack”.

The number of cyber-attacks experienced offers a way to operationalise this explanation. Previously collected data shows that cyber incidents have on average been increasing over time (Valeriano, Jensen and Maness 2018, 67), which may provide an explanation for the proliferation of cyber capabilities. Iran for example embarked on a build-up of offensive and defensive cyber capacity in direct response to the Stuxnet operation which caused physical damage to one of its uranium enrichment plants in 2010. This cyber-attack highlighted Iran’s vulnerability and likely motivated it to establish organisations such as the Supreme Council of Cyberspace, a cyber military command, and to develop its own national Internet (Craig and Valeriano 2016, 150).

Threats can also come from the perceived or misperceived capabilities of rival states. According to security dilemma theory, the threats that drive a military build-up arise from the capabilities of rival

states due to the fear that they could be used to conduct offensive action against a state. This suggests that states will develop cyber capabilities when their rivals possess cyber capabilities. The idea of the security dilemma has already been applied to cyberspace (Reuter 2011; Cavelti 2014; Buchanan 2017; Brantley 2014; Craig and Valeriano 2016), although not as a testable hypothesis in a statistical study for the adoption of cyber capabilities.

Applying this action-reaction logic to cyberspace however may be flawed. Lieber (2011, 104) argues that cyber build-ups are not observable like most conventional military build-ups, meaning that there would be no evidence of a country making the kind of preparations that would motivate another state into a reactive cyber build-up. He suggests that only actual cyber incidents provide evidence of threat. Yet in these cases, the states are not reacting out of mutual insecurity as the security dilemma model describes; instead, there is only one state initiating cyber-attacks against another. While Lieber's point is true for some inherently undetectable aspects of cyber capability development, such as the acquisition of malware, there are observable actions that could be perceived as a potential threat. For example, the development of cyber warfare units or commands for instance will be less likely to go unnoticed by rival governments and these entities could provide a source of threat.

Drawing on balance of power theory, some commentators suggest that the reason why some states develop their offensive cyber capabilities is that they are seeking low-cost means to challenge the United States – the unipolar power in international politics. As stated by the US military, “a wide range of actors use ICT and advanced technologies as a relatively inexpensive way to gain parity with the U.S. as compared to buying tanks and aircraft or training thousands of soldiers” (United States Army 2010, 10). A potential explanation is that the rivalry of these countries with the United States motivates them to develop capabilities.

Given the inherent insecurities associated with the cyber domain, states should be sensitive to their external threat environment and their rivalry context and will pursue capabilities as a means of managing their external relations. Previous research has already documented the engagement of rival states in cyber operations against one another (Valeriano and Maness 2014). This leads to the second hypothesis for the determinants of cyber capabilities from the willingness perspective:

Hypothesis 2: Countries with a more intense external threat environment are more likely to adopt active cyber capabilities

Part two: The impact of cyber capability on cyber conflict

Having established an explanation for the spread of capabilities, the next task is to develop an explanation for the impact of cyber capabilities on the occurrence of cyber conflict (i.e. the computer

network-based operations carried out between states). Policy makers urgently want to know why states are engaging in cyber conflict, how it is likely to change in the future, and how to curtail it. Moreover, IR theory is advanced by discovering if capabilities have any explanatory power in relation to a new form of interstate conflict. To be clear, capabilities represent the resources states can potentially use to engage in computer network operations, while conflict refers to the application of cyber capabilities in computer network operations against their opponents.

Capabilities either make conflict more likely, less likely, or have no impact. By drawing on the relevant theoretical IR literature, two basic and opposing arguments can be developed for the impact of cyber capabilities on the incidence of cyber conflict. The first, drawn from deterrence theory, suggests that the signalling of capabilities may reduce cyber conflict through the mechanisms of denial and punishment. The second, derived from the spiral model of arms build-ups and conflict, suggests that the growth and adoption of capabilities by states will promote the use of these capabilities in cyber operations.

Whether the presence of capabilities deter and therefore reduce the occurrence of cyber incidents is an open, empirical question. While there is a large body of theoretical literature on cyber deterrence (Libicki 2009; Stevens 2012; Nye 2017; Brantly 2018), there is a dearth of empirical analysis on the relationship between capabilities that could be used to signal credible levels of resolve and threat and the initiation of cyber incidents between states. I address this question empirically for the first time using the NCC dataset and combining it with previously published data on cyber conflict (Valeriano and Maness 2014).

Based on Opportunity-Willingness Theory increases in capability in the international system should lead to an increase in the likelihood and frequency of cyber conflict. Once states acquire active cyber capabilities, they have increased opportunity to engage in cyber operations, thus making cyber conflict more likely. Moreover, the failure of cyber deterrence and the incentives to employing cyber capabilities will lead to increased willingness to engage in cyber operations, again leading to a greater propensity for cyber conflict to occur. In this section, I first explain the concept of deterrence in IR theory and highlight the difficulties when applying it to cyber conflict. Secondly, I discuss the argument that military build-ups cause an escalation in interstate conflict and then apply these to the cyber domain to argue that increases in cyber capability should be associated with an increase in cyber incidents.

Deterrence, capabilities, and conflict in international relations

Deterrence can be understood as the avoidance of war through causing a change in the cost-benefit calculations of a potential aggressor. If an attacker can be made to believe that the costs of their

military action will outweigh the benefits, they can be dissuaded from initiating conflict. Although deterrence-based logic has always implicitly underlined international relations, deterrence theory came to the forefront of national security policy after the employment of nuclear weapons in World War Two given their immense destructive capacity and the need to formulate strategies that would prevent their use in the future (Brodie 1946).

Some scholars argue that nuclear weapons are paradoxically a weapon of peace and stability since they dramatically raise the costs of conflict escalation through the mechanism of Mutually Assured Destruction (Waltz 1990; Mearsheimer 1990, 19-20). Assuming a state possesses the ability to survive an initial nuclear strike and retaliate with its own nuclear arsenal, war between nuclear-armed states is inconceivable and a scenario to be avoided at all costs. Deterrence is not only relevant to the nuclear domain. It provides a plausible causal mechanism between capabilities and conflict in general, and is increasingly alluded to in the cyber security discourse.

There are two key mechanisms by which deterrence can operate. The first is *deterrence through punishment* which can be defined as “the use of a threat (explicit or not) by one party in an attempt to convince another party to maintain the status quo” (Quackenbush 2011, 741). A defender can reduce the cost-benefit ratio for aggressors and deter conflict by convincing its rivals that it possesses adequate military capabilities to respond to an attack, that it will inflict unacceptable costs through its retaliatory action, and that it would carry out this threat if attacked. Credibility is the key determinant of the success or failure of deterrence (Huth 1988). Nuclear deterrence, for instance, was underpinned by the certainty that nuclear weapons would impose overwhelming levels of destruction.

The second mechanism is *deterrence through denial*, which works by “reducing the perceived benefits an action is expected to provide a challenger” (Wilner 2015, 28). This is achieved through frustrating the attacker’s efforts, rather than threatening punishment in response to an attack. A defender can reduce the cost-benefit ratio for aggressors and deter conflict by building defensive capability and resilience to signal to a would-be attacker that that military action will not succeed and will be costly and time consuming. If offensive action is no longer considered worthwhile, the likelihood of conflict initiation against a state with high defences should decline.

While nuclear deterrence operates through the principle of punishment, conventional deterrence generally operates through the principle of denial (Mearsheimer 1984; Shimshoni 1988; Quester 1966). The key assumption of this theory is that when states are considering engaging in warfare, they are incentivised by the prospect of a rapid and easy victory, and disincentivised by the prospect of a drawn-out war of attrition. Conventional deterrence is therefore about convincing a potential enemy that it will likely fail in achieving a rapid victory, rather than necessarily threatening punishment in response to an attack.

Deterrence can provide a plausible causal mechanism between the relative capabilities of states and their conflict-proneness. Specifically, scholars have debated whether a preponderance or balance of capabilities between pairs of states is more likely to deter conflict. Balance of power theorists argue that a parity (balance) in capabilities will make conflict less likely because each state will perceive victory as being less certain against an equally powerful rival and be deterred from initiating conflict (Wright 1964; Waltz 1979). They argue that conflict is more likely when one state is substantially stronger than the other because victory will be perceived as feasible by the stronger state against its weaker foe who lacks the capability to deter its stronger adversary.

Alternatively, power preponderance theorists argue that a capability balance increases the likelihood of war because both states recognize an opportunity for victory. They argue that a condition of preponderance (one state has substantially more capabilities) is less war-prone because only the most powerful state has the capability to wage war but is more likely to be satisfied and have no need for war (Blainey 1973). Moreover, the likely outcome of conflict in such circumstances will be clear-cut and so the would-be disputants are more likely to settle their issues peacefully rather than engage in war. Most empirical evidence points towards conflict being more likely between equally capable states (Bremer 1992, 337; Geller 1993; Bennet and Stam 2004, 137).

Military capabilities are not the only relevant factor in deterrence, which is equally about signalling resolve and credibility. Nevertheless, capabilities are a necessary condition for successful deterrence because they provide the means to deny or punish an actor. Without offensive or defensive capabilities, a country will not be able to carry out deterrent threats or defend against attacks. If deterrence is successful, one should observe a negative relationship between capabilities and conflict. Yet as the next section will discuss, deterrence faces significant challenges in cyberspace which means capabilities might not cause a reduction in conflict.

The failure of cyber deterrence

The concept of deterrence, or as Nye (2016/2017, 45) puts it, “dissuading someone from doing something by making them believe that the costs to them will exceed their expected benefit”, is frequently applied to the cyber domain⁹ as a mechanism for reducing cyber-attacks. The concept has existed since at least the early 1990s, but moved to the forefront of the national security discourse in the late 2000s in response to several prominent cyber incidents during this period (Stevens 2012, 151).

⁹ In this thesis I am referring to intra-domain cyber deterrence which is the prevention of cyber incidents through threat of cyber operations or build-up of cyber defences.

Some governments make it clear that their acquisition of cyber capabilities serves the purpose of deterring malicious cyber operations. For instance, the United Kingdom declares in its 2016 National Cyber Security Strategy that “the full spectrum of [its] capabilities will be used to deter adversaries and to deny them opportunities to attack us” (HM Government 2016, 47). IR scholars have also suggested that capabilities are being developed for this purpose given the lack of global cyberspace governance. As Stevens (2012, 166) writes:

“there is a substantial build-up of military cyber capabilities across the globe, which perhaps indicates that states see little real utility in global cyberspace agreements to deter or prevent cyber conflict, or are attempting to develop punitive capabilities through demonstration of massive offensive capabilities and force structures and posture.”

But can cyber capabilities deter cyber-attacks either through the threat of punishment or the denial of gains? This is perhaps the most prominent yet challenging policy issue in the area of cyber policy as experts try to formulate strategies to reduce digital threats. Some commentators believe they can. For instance, Healey (2018) argues that the United States was deterred from responding to Russian interference in the 2016 presidential election out of fear of Russian cyber power, particularly their ability to disrupt the US electricity grid.

States that possess greater cyber capabilities may be able to disincentivise the use of cyber operations against them either by threatening punishment in the form of a retaliatory cyber operation or by denying their adversary gains. There are strong theoretical challenges to this notion however, and there is widespread scepticism of the applicability of deterrence to cyberspace. According to Clarke and Knake (2010, 32), “of all the nuclear strategy concepts...deterrence theory is probably the least transferable to cyber war”. Indeed, the concept is fraught with difficulties when applied to the cyber domain.

Some scholars argue that denial is the most feasible system of deterrence in cyberspace like Arquilla (2015) who draws an analogy between cyber conflict and airpower in WWII where it was the denial of German victory through superior air defences rather than the threat of punishment that deterred Germany’s bombing of British cities. Nye (2016/2017, 56) suggests that “good cyber defenses can eliminate the majority of potential attacks from unsophisticated users”. Through stronger private sector regulation, encryption, cyber security awareness and practices, intrusion detection and anti-virus products, and automatic software updates, and basic “hygiene”, perhaps the rate of successful cyber-attacks can be reduced.

The active cyber capabilities and policies that I measure in this project which represent efforts to improve cyber defence include the presence of a national incident response team and a national cyber security strategy. These efforts are undoubtedly motivated by the need to reduce the country’s

vulnerability to cyber threats, but can such capacities and policies increase the cost-benefit ratio of the attacker and deter cyber incidents? In theory, denial can reduce the expected gains of the attacker in two ways: by defending against an attack as it occurs or through rapid recovery and damage limitation. Some have suggested that denial is, by definition, not deterrence because an attack has already taken place rather than been outright prevented (Stevens 2012, 153). Nonetheless, if defensive capacities in general reduce the frequency of future attacks (once attackers have become aware of their futility), this relationship should show up in a data analysis.

Deterrence by denial is faced with such significant challenges however that the institutional capabilities and policies established by the state are unlikely to reduce cyber incidents, particularly those from sophisticated state actors (Nye 2016/2017, 57). First, the range of possible intrusion vectors available to the attacker is very large making it hugely costly for the defender to map and patch all possible vulnerabilities and routes of entry (Kello 2013, 29). Even if a state establishes a national incident response team, for example, they will be unable to detect vulnerabilities or intrusions across the entire country simultaneously in order to prevent an incident. Secondly, many offensive operations target zero-day vulnerabilities in software which by definition are unknown to the defender until they are exploited, making it difficult to foresee and detect intrusions (Stevens 2017, 8). The nature of cyber threats means that many cyber incidents cannot be dealt with before they occur, suggesting capabilities will not reduce incidents.

The difficulty of defence and denial is confounded by the fact that responsibility for securing networks lies mostly in the private sector, not in central government (Carr 2016). This is because of the widespread nature of computer networks connecting private businesses, organisations, and individuals within and between countries. Unless a state creates a national intranet that can be disconnected from the Internet (Mueller 2017), state level policies and capabilities will not have much success in deterring cyber incidents. For these reasons, preventing the weaponized code of an attacker reaching its target is a very challenging policy to implement successfully (Kello 2018, 68-74).

Since the potential attacker knows that it has a good chance of achieving its aims, it is unlikely to be dissuaded from acting despite the capability of the defender. I therefore argue that efforts to build defensive capability or policy at the institutional level (through initiatives such as a national CSIRT or a national cyber security strategy) will not be associated with a reduction in cyber conflict against the defending state. This is summarized by hypothesis 3.

Hypothesis 3. Active cyber capabilities for defensive purposes will not cause a reduction in cyber incidents against the defender.

This is not to say cyber security measures should not be promoted. Easily preventable incidents should be tackled through basic cyber hygiene practices enacted within organisations including

regular data back-ups, software updates, and regularly changes in passwords. Moreover, there should be an acceptance that sophisticated actors will find a way in and the focus should be on becoming resilient to cyber threats by reducing the damage done and recovering quickly. While institutional developments (CSIRTs and strategies) are also important, their effect is not likely to be observed in the rate of cyber incidents suffered.

Deterrence through punishment equally faces problems, undermining the hope that offensive cyber capabilities could be brandished against potential aggressors as a means of reducing the occurrence of cyber conflict. The problems of attributing cyber-attacks and the uncertainty over the effects of cyber weapons are the key factors undermining the credibility of deterrence by punishment in this domain (Whyte and Mazanec 2019, 133).

The first problem is attribution and establishing political responsibility for a cyber-attack (Rid and Buchanan 2015; Lindsay 2015). For a state to be able to credibly threaten punishment against an attacker, it must confidently be able to identify and trace the attacker. Guitton (2012) has carried out one of the few statistical analyses on the effect of attribution on the successful deterrence of cyber criminals using cyber-crime data from the UK, France and Germany from 2003 to 2010. His findings provide some evidence that a lack of attribution is associated with an increase in attacks, suggesting deterrence is more likely to fail if cyber criminals believe they will evade punishment.

In the international cyber domain, attribution is difficult because of the non-physicality of cyber weapons and the elusive methods by which actors can carry out attack. With a nuclear strike, it is usually clear where the weapon came from given its physical nature and the narrow range of potential attackers. Cyberattacks however are much more difficult to track to an origin and political actor because of their virtual nature and because attackers can conceal their identities online and do not have to operate out of the country that sanctioned the attack. Moreover, the barriers of entry are lower and so a much larger group of state and non-state actors can develop or purchase malware than they can nuclear weapons (Nye 2011, 124), thereby increasing the group of possible attackers.

It is possible for forensic experts to link malware back to an original computer, but there is still great uncertainty over who was responsible. Attackers can cover their tracks by using botnets (remotely controlled and compromised computers) that can be located across numerous countries and jurisdictions (Singer and Friedman 2014, 44). Moreover, attackers are not necessarily state actors but criminals operating within a country's territory or civilian hacking groups used by the state to deny responsibility (Whyte and Mazanec 2019, 135). Deterrence is therefore difficult because of the challenge of establishing political responsibility giving attackers the confidence to act with impunity.

This means that even if the initiator of a cyber operation is aware that the defending state has well developed capabilities that it could apply for offensive purposes, it can be more confident that the

defender will be unable to identify it as being responsible, thus undermining the threat of punishment. The initiator therefore is unlikely to be dissuaded from conducting operations against the defender.

Some scholars argue that the attribution problem is overstated and that eventually the initiator of a cyber incident is identified (Valeriano and Maness 2015, 82). Even if attribution is eventually achieved, the credibility of a deterrent threat is undermined by the uncertainty that the initiator has of the defender's capabilities. Governments tend to be very secretive of their offensive capacity in cyberspace because cyber incidents can reveal one's malware, render it no longer useful, and allow the target to learn from it (Gartzke 2013, 60). If the potential attacker has a lack of evidence about the defender's capabilities, it is less likely to be convinced that the defender has the capacity to retaliate in the event of a cyber-attack. The defender's creation of a military cyber unit, for instance, may signal to the attacker that the defender has some degree of operational capacity, but it offers very little evidence of precisely the types of damage the defender could inflict through a retaliatory cyber operation.

Credibility is also undermined by the lack of destructive potential that cyber capabilities can inflict in general. The damage that could possibly be done through a computer network operation is clearly on a much lower level than a nuclear or conventional military strike. As Rid (2013, 18) argues, cyber-attacks are highly unlikely to ever inflict violence against humans. At most cyber-attacks can achieve the defacement of websites, disruption of Internet services, theft or destruction of data, and perhaps the sabotage of industrial controllers affecting some physical infrastructure. Yet these are limited effects compared to that of conventional or nuclear actions. Moreover, the effect of a cyber-attack can usually be reversed relatively quickly (Gartzke 2013, 57). The level of hostility achieved through cyber operations to date therefore falls far below what is considered an act of war. This means that the attacker will be aware that the damage the defender could inflict will inherently be limited and therefore may be willing to bear any potential costs of its actions.

Given the problems of applying traditional deterrence models in cyberspace, some scholars have expanded the scope of deterrence to include other strategies such as the development of international norms to constrain state behavior (Stevens 2012; Nye 2016/2017). Nye (2016/2017, 58) adds the policy of entanglement to the strategic options, whereby tight interdependencies between states and their economies are reinforced so as to make cyber-attacks a counterproductive action. Given the unique, interdependent structure of cyberspace, Harknett et al reject deterrence outright and argue that states are operating in an "offence-persistent" environment where cyber conflict will continue below the threshold of where deterrence would become relevant. The appropriate strategy should therefore be a blend of active defence and offence where the state continually seeks to anticipate attacks and degrade enemy capabilities (Harknett, Callaghan and Kauffman 2010; Harknett and Goldman 2016).

Valeriano and Maness (2014) introduce a theory of restraint to explain the lack of destructive cyber-attacks so far, which draws on a blend of deterrence and norms-based arguments. For instance, they write that states are restrained from conducting “devastating Internet operations focused on power systems and health services...through fears of retaliation and escalation of the conflict beyond control” (2014, 350). They also cite the fear of breaking the normative taboo against collateral damage (Romanosky and Goldman 2016) – given the tendency for malware to spread beyond its intended target – and the unwillingness to reveal one’s capabilities, since rivals can learn from the computer code used in an operation to improve their own capability (Valeriano and Maness 2014, 358).

The lack of destructive cyber-attacks to date may be evidence that deterrence is working at least at some level – although the precise mechanism (norms, denial, or fear of reprisal) is unknown. Low-level incidents, on the other hand, are generally tolerated by states as acts of disruption or espionage that fall below the threshold for retaliation and war. Deterrence may be feasible in relation to high-level cyber conflict rather than the low-level cyber incidents that we currently observe between rival states. Nevertheless, at the level of cyber conflict currently experienced, capabilities that could be applied towards punishment are not likely to have an impact on the occurrence of cyber incidents. What this means at the dyadic level of cyber conflict is that a country’s level of cyber capability vis a vis its rival will not change the attacker’s cost-benefit calculation, and therefore will not deter (prevent) cyber conflict. A preponderance or balance of capability between two states will not limit the initiation of cyber incidents because deterrence is undermined by plausible deniability through the attribution problem, the lack of credible threat, and the tolerance of low-level cyber conflict. This results in hypothesis 4.

Hypothesis 4: Neither a preponderance nor balance of capabilities among two states will be associated with a reduction in cyber incidents between them.

Capabilities as a cause of conflict

Alternatively, capabilities can be viewed not as a tool of deterrence and stability, but as a cause of conflict. To gain security in a self-help international system, a realpolitik foreign policy calls for the augmentation of military power, reflected in the Latin proverb: *Si vis pacem, para bellum* – if you want peace, prepare for war. Yet there is a body of empirical studies suggesting that military build-ups in fact contribute to the onset of war.

In the anarchical international system states are forever fearful of the intentions of others and so military capabilities provide a means to defend and deter. The downside, however, is that one state’s

military build-up pressures other states to invest in capabilities which in turn increases uncertainty and insecurity amongst all. This is the spiral model of conflict, whereby the arms competition increases the risk of warfare by creating uncertainty over whether a rival state is going to initiate conflict and therefore makes states more willing to attack pre-emptively to eliminate that country's ability to attack (Jervis 1976, 62-67). Capabilities are therefore themselves the key driver of uncertainty which lead states down the path to war.

The literature on arms races suggest that arms races are a factor increasing the probability of disputes. Scholars have found that militarised interstate disputes preceded by an arms race are more likely to escalate into war (Wallace 1979; Sample 1997). Steps-to-war theory integrates military build-ups into a set of realpolitik actions that together increase the probability of war including alliance formation and the presence of hardliners in government, and empirical testing of the theory shows that mutual military build-up increases the probability of war and disputes amongst rivals involved in a territorial dispute (Senese and Vasquez 2008). It seems the fluctuation in capability between competitors increases the general level of rivalry and hostility and risk of a crisis escalating.

However, Vasquez (2009, 127) notes that "increases in military expenditures and calculations about capability immediately prior to the outbreak of a war should be seen more as an attempt to prepare for a coming war and to time it to one's advantage, rather than as a 'true cause' of war". In this sense, capabilities reflect a deeper willingness to engage in conflict and are a necessary part of the preparation to engage in it. This is an example of how an initial willingness to engage in conflict can lead to greater opportunity to do so, through the acquisition of military capabilities, whereupon both factors combine to make war more likely (Most and Starr 1989, 43).

Cyber conflict operates in a very different way to traditional warfare, however. The spiral model – which is based on the logic of pre-emptive war – does not translate well to the domain of cyber conflict because cyber capabilities lack the capacity to inflict decisive defeat upon an enemy, achieve territorial domination, or shift the balance of power permanently in one's favour unlike a conventional, kinetic military campaign (Gartzke 2013). The causal mechanism linking cyber capability to conflict is based on different logic, as will be discussed next.

Opportunity-Willingness and Cyber Conflict

An increase in cyber capability is more likely to promote than to deter cyber conflict, although this is not to say that they it will transform the traditional dynamics of the international system or replace more effective forms of military capability. Rather than be used to achieve military victory, cyber operations are conducted to either cause disruption or harassment to a rival and influence the broader political bargaining context, alter the balance of information through espionage in the context of

long-term competition, or, at its most severe, sabotage a country's critical infrastructure (Valeriano, Jensen, and Maness 2018, 11-13).

Cyber operations may involve the hacking of enemy computer systems to disrupt communications, alter data, or tamper with systems of critical infrastructure like electricity grids, but states are likely to recover from these effects in a relatively short amount of time. This undermines the utility of cyber operations as a tool for achieving political impact unless they are used in tandem with kinetic or other methods of attack (Gartzke 2013, 44). If states do not believe that cyber capabilities will help them achieve their political aims, some scholars argue that the presence of capabilities are unlikely to increase the likelihood of cyber war. As Gartzke (2013, 57) writes:

“The mere ability to cause harm over the Internet does not suffice to predict that cyberwar will substitute for terrestrial conflict, or even that it will be an important independent domain for the future of warfare”.

The same logic of fear that might drive states locked into a security dilemma into a pre-emptive war in the non-cyber realm does not apply in cyberspace, because the weapons are limited in impact and threat. Two countries that are engaged in a process of building up cyber capability may be more fearful of one another and anticipate possible aggressive action, but they are unlikely to believe that they ought to initiate a cyber operation before their rival does in order to decisively defeat their enemy or prevent them using their cyber capabilities. Cyber technology cannot achieve this sort of lasting victory. The limited utility of cyber weapons leads Liff (2012, 426) to conclude that “although gradual proliferation of cyberwarfare capabilities may be inevitable, the widespread use of CNA is probably not.”

That being said, while decisive and lasting victory¹⁰ is not possible with cyber capabilities, there are several reasons to believe there are incentives and thus willingness to carrying out cyber operations. Glaser (2000, 254) argues that the spiral model assumes both states are benign security seekers and ignores the presence of greedy, offensive states, and this is useful for understanding cyber conflict also. In the cyber domain, cyber incidents occur because some states are motivated towards conducting offensive operations.

Because of the failure of deterrence mechanisms, and the incentives for carrying out cyber-attacks and espionage, the willingness to conduct cyber operations is generally high. Moreover, by providing the state with the opportunity for action, capabilities will be a key factor in enabling or impeding its engagement in cyber conflict. The acquisition of cyber capabilities creates opportunity and should therefore lead to increased levels of conflict at the currently observed low levels of hostility. To be

¹⁰ Victory in cyber conflict has been explored by Valeriano, Jensen and Maness (2018) who base it on whether a cyber operation leads to a concession or change in behaviour of the defender.

clear, I am not talking about devastating acts of cyber war which are unlikely for reasons of restraint articulated by other authors (Valeriano and Maness 2015, 61-64), but of the hundreds of cases of cyber incidents involving rival states over the past few decades that have never escalated into war.

So, what are the incentives to the employment of cyber capabilities? According to Kello (2018, 67), cyber capabilities “expand the available methods of harm that do not fit established conceptions of war but may be no less harmful to national security”. While I am sceptical about their revolutionary impact, it is clear that cyber capabilities have provided states with more avenues to disrupt, steal information from, or degrade their rivals that would not have been possible before the advent of cyber weapons. As explained by Smeets (2018), offensive cyber operations give leaders more tools for resolving diplomatic crises and managing escalation, help increase the effectiveness of conventional military operations by disrupting communications, inflict psychological damage, and limit casualties.

Moreover, offensive-oriented strategies are increasingly being viewed as a means of attaining cyber security. This creates an added willingness to engage in cyber operations. According to Harknett and Goldman (2016, 86) cyberspace is an “offense-persistent” environment where defenders cannot sit back and rely on a strategy of deterrence but must continually seek to anticipate attacks and gain advantages over adversaries. This is reflected in the United States’ 2018 Cyber Strategy which aims to “persistently contest malicious cyber activity in day-to-day competition” through the “development of cyber capabilities for both warfighting and countering malicious cyber actors” (Department of Defense 2018, 4).

Structural factors are also important in reducing the barriers and increasing the opportunity for cyber conflict. For instance, a commonly cited reason for the increase in offensive cyber operations is that the ability for attackers to penetrate their opponents’ networks compared to the defenders’ ability to prevent or respond is greater. Proponents of this idea (Kello 2018) draw on the offence-defence balance theory (Jervis 1978; Van Evera 1998; Glaser and Kaufmann 1998) which posits that when technological change improves the cost effectiveness of offensive technology and action relative to defence, the willingness for engaging in offensive activity increases. Since offensive cyber weapons can be developed relatively cheaply, travel at rapid speed with no geographical hindrance – combined with the fact the defender is impeded by the difficulty of securing every network and system vulnerability – attackers have advantages over the defenders and we should see a proliferation of cyber-attacks in line with increases in the resources to carry them out.

Another structural condition is the lack of deterrence in the cyber domain for the reasons mentioned previously. States engage in cyber operations precisely because they will not be faced with a deterrent threat or effective denial. Moreover, there are few institutional barriers to conducting cyber operations. One reason pointed out by Junio (2013, 130) is that there is little bureaucratic “friction”

in place when it comes to conducting computer network operations. In this environment the norm is for cyber operators to be constantly penetrating the networks of their rivals (Buchanan 2016)

Taken together, the heightened level of opportunity and willingness to conduct offensive cyber capability, especially in an environment where deterrence fails, suggests that states are likely to engage in cyber operations, given they possess adequate capability. Capability is an enabler for conflict and its presence may also reflect a deeper willingness to engage in cyber activity against rivals. The only thing preventing a state that is interested in conducting cyber operations from doing so is whether a country possesses the capability. This suggests capabilities should be a key variable for explaining cyber conflict. As a country's latent and active cyber capability grows, they become more skilled and organised for conducting computer network operations and therefore are more likely to engage in it. This leads to hypothesis 5:

Hypothesis 5: As the capability of the state increases it is more likely to conduct cyber operations against another state.

Capabilities are a key explanation for cyber conflict, yet they offer only a partial explanation. States also require a target for their politically motivated acts of cyber aggression or espionage. While capabilities increase the opportunity for carrying out cyber operations, the intensity of rivalry and the pre-existing level of tensions and conflict between states should increase the willingness to conduct cyber operations at the interstate level.

I therefore argue that pairs of states with more rivalrous relations are more likely to engage in cyber conflict because they have an increased motive. Cyber operations provide a way for a state to harm its external competitors or gain relative advantages through disruption, espionage, or degradation. Hypothesis 6 therefore tests whether the willingness side of the opportunity and willingness framework can help explain not just the proliferation of active cyber capabilities but the use of capabilities against another state.

Hypothesis 6: Rivalry intensity will increase the likelihood of cyber conflict

Summary

In sum, the theoretical framework of Opportunity-Willingness helps explain two steps in a process of emerging cyberspace activity by state actors. The process begins with a country's possessing varying levels of latent cyber capabilities, which are defined as the set of societal based resources that the state can draw on to establish active capabilities.

The most important type of latent capability is technical skill and knowledge relevant to computer networks and systems. This is crucial because cyber capability is inherently about the creation of

computer code and the knowledge of computer systems, which requires expertise more so than money or other resources. Although wealth is helpful in growing this type of talent in a country, skill and knowledge should be the proximate cause of cyber capability from the opportunity perspective. Some level of latent cyber capability is necessary for the proliferation of domestically established active cyber capabilities.

The decision to pursue active capabilities will also be sensitive to threats such as the existence of rivalry, cyber-attacks, and the perceived capabilities of rivals, because of the anarchical and insecure nature of cyberspace which lacks global governance. Capabilities provide them with new tools to deter, defend threats or pursue strategic interests against rivals. These include developments like military organisations dedicated to computer network operations or national incident response teams.

Once active capabilities are established, the next step in the process is their application in conflict against rivals. Capabilities will not deter conflict, rather they enable states to carry out cyber operations. While there are clear incentives for the engaging in cyber conflict generally, not all countries with this capacity will necessarily do so. A secondary factor therefore is the intensity of the rivalry context. Countries with more conflict-prone relations will be most likely candidates for carrying out cyber-attacks against their rivals.

Overall, I suggest that cyber capability is a key variable for understanding the growth of cyber conflict in the international system because it gives countries the opportunity to engage with their rivals, in an environment where deterrence is ultimately bound to fail. The importance of rivalry also demonstrates that cyber conflict is ultimately related to pre-existing international tensions. These relations must first be improved, or else capabilities and conflict will continue to proliferate. Having set out the theoretical framework used to structure the analysis the next chapter will describe my methods for measuring my variables and testing these hypotheses.

Chapter IV

Methods for Quantifying National Cyber Capability

Introduction

In this chapter I outline my methodology for creating the National Cyber Capabilities (NCC) dataset which I use to test my hypotheses about the proliferation of cyber capabilities. The creation of the dataset – which involves turning theoretical concepts into quantitative indicators – is a prerequisite for empirical analysis. This chapter therefore explains and justifies the choices and approaches I take in creating a set of quantitative indicators.

The dataset of national cyber capabilities describes the resources and assets belonging to each state in the international system from the year 2000 through 2017 that relate to the pursuit of strategic interests in cyberspace. This is essential for the quantitative examination of the proliferation of active capabilities and conflict. The dataset represents significant progress in the existing scholarship in this area by introducing a time series dimension to the data and accounting for military capabilities.

This study is based on a positivist epistemology and quantitative methodology.¹¹ Positivism is the philosophical standpoint – underpinning the scientific method – that valid knowledge of the world is best acquired through our examination of observed phenomena rather than a priori reasoning (Sanders 2010, 23). The methods are mainly quantitative meaning that observed phenomena are measured in a numerical fashion and analysed statistically. Unlike qualitative research where the goal is often to analyse a limited number of cases of a phenomenon in depth, quantitative research analyses a large number of cases. This makes it possible to generalise on patterns of state behaviour and its drivers using statistical techniques (Mansfield and Pevehouse 2008). Quantitative methods are most appropriate method for my research aims which are to identify causal effects that can be generalised to the entire population of countries. The quantitative component however is complimented with a qualitative case study to illustrate the processes of cyber capability adoption and conflict.

In this chapter, I establish the scope and limits of the dataset in terms of what the data can and cannot achieve. Afterwards, I explain the specific variables that compose the dataset beginning with a discussion of latent capabilities, which are the resources that exist within society, and then active capabilities which are the government centred capabilities.

¹¹ Epistemology relates to the discussion of what counts as valid knowledge of the world, and methodology relates to the discussion of what type of methods ought to be used to acquire knowledge.

The scope and limits of the National Cyber Capabilities dataset

The variables discussed here are aimed at approximating a state's ability to pursue its strategic interests in cyberspace through societal resources and government level initiatives. Specifically, national cyber capabilities are defined as *the national resources and assets that a state can draw on or use to resist or exert influence in cyberspace via the means of computer network operations (CNO)*. This definition requires several further assumptions, specifications, and caveats for a clearer understanding.

First, cyber capability is not synonymous with cyber power as defined in terms of influence (Betz and Stevens 2011, 43; Nye 2011, 123). That type of power is evident through outcomes while capabilities refer only to the resources used to achieve outcomes. Capabilities can therefore be thought of as potential power. Just as a country with a large army has greater potential to win wars than a country with a small army, a country with more cyber capabilities may be better able at carrying out successful cyber operations. A state with more resources is more likely to achieve its goals, although this is not always true due to other factors such as force employment tactics (Biddle 2005). One of the benefits of defining capabilities as resources rather than outcomes is that it allows the link between the two concepts to be investigated to determine, for instance, the effect of superior capabilities on the outcome of cyber operations.

Another reason why I take the power-as-resources approach is that one cannot deduce a country's capability from its activity in cyber operations alone. One of the mistakes some commentators make is that they observe a high level of offensive cyber activity from a country, like Russia or North Korea, and conclude that its capabilities are advanced compared to other countries (SC Media 2015; Wright 2018). This logic is flawed because a country may have advanced capabilities yet not use them. Conversely, although a country that frequently engages in offensive operations is clearly capable to some extent, the cyber-attacks themselves cannot provide a full picture of a country's range of capabilities. Instead they say as much about its political motivations and intentions than what resources are available to it, hence the importance of measuring a country's capabilities independently from outcomes.

Capabilities must be defined with reference to some intended outcome that a state using capabilities wants to achieve. For simplicity's sake, strategic goals in cyberspace can be categorised into defence and offence. States fundamentally acquire capabilities to deter cyber operations or carry out cyber operations. Studies of national cyber strategies have shown that defensive strategies often aim at protecting national assets from cyber-attacks including the defence of critical infrastructure, of confidential government or industrial data, and of military networks (Luijff, Besseling and de Graff 2013; Azmi, Tibben and Win 2016). Although governments will not usually admit to the usage of offensive capabilities, some states clearly have offensive intent and the historical record of cyber

conflict shows that several countries have utilised offensive cyber technology and methods to harm their rivals interests or gain economic or informational advantages (Valeriano and Maness 2015).

I choose *Computer Network Operations* as a suitably comprehensive framework for capturing most of the methods by which states pursue these strategic goals in cyberspace. The concept of Computer Network Operations (CNO) consists of three types of activity: Computer Network Attack (CNA), Computer Network Defence (CND), and Computer Network Exploitation (CNE), which have been defined by the United States military as follows: CNA is defined as “actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.” Computer Network Defence (CND) is defined as: “Actions taken through the use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within Department of Defense information systems and computer networks.” Computer Network Exploitation (CNE) is defined as “Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.” Placing cyber capabilities within the context of CNO is aligned with previous research on this topic (Liff 2012; Brantly 2014).

In recent years, the term “cyber operations” has superseded the term CNO. Cyber operations include “offensive cyber operations”, “defensive cyber operations”, “cyber intelligence, surveillance and reconnaissance”, and “cyber operational preparation of the environment” (Ministry of Defence 2016). These two sets of concepts largely share the same meaning and are used interchangeably in this thesis.

Nevertheless, I need to exclude several types of cyber activity that do not fit into this framework. Firstly, my concept of cyber capability does not directly relate to a country engaging in propaganda or information warfare activities unless computer networks or systems were themselves hacked. Social media activity as part of operations to shape public opinion are not part of the analysis. For the same reason as above, electronic warfare (EW) capabilities are also excluded as this involves attacking and defending electromagnetic radiation signals and infrastructure, but not computer networks.

My capability data measures the institutions that have been formally established by governments or the latent resources existing in society. The NCC dataset therefore cannot account for the entire portfolio of national cyber capabilities because states can also derive capability from other sources which I do not directly measure. For instance, I do not measure proxy actors (Maurer 2018) that operate out of the broader society such as the “Iranian Cyber Army” (Anderson and Sadjadpur 2018, 11). However, my assessment of latent knowledge in society helps to capture the potential for cyber operations existing in society regardless of whether it is a government institution or proxy actor instigating them.

Secondly, the capabilities I measure refer to domestically produced capabilities. I do not account for the sale of off-the-shelf malware to repressive governments by foreign IT companies such as NSO group in Israel or Hacking Team in Italy (Brewster 2016). This activity is far too secretive to collect reliable data on. That being said, I argue that the most sophisticated and capable states are those that have the domestic capacity and skill to develop their own malware. In this sense, having to acquire capabilities from a foreign third party is an indicator of weakness rather than strength.

The data set assesses capability from various perspectives, reflecting the idea that a state's ability to project and resist influence in cyberspace is a function of several factors. As some scholars have noted, "Chinese analysts assess that the United States holds the advantage in cyber capabilities in terms of overall IT industry dominance, malware design, training of cyber forces, and control of Internet infrastructure" (Lindsay, Cheung, and Reveron 2015, 146). A multi-dimensional approach is common in IR research too (Singer 1988), and as Wohlforth and Brooks (2016, 14) argue, a "broad-based" approach to assessing capabilities is crucial since a country with capabilities in only one area will not be able to pursue its full range of strategic interests as effectively as one with a comprehensive "portfolio" of capabilities.

This research categorises capabilities into two broad categories – latent and active capabilities. The decision to distinguish between these two types of capability has precedence in IR theory and prior empirical research. The widely used Composite Index of National Capabilities (Singer 1988) distinguishes between the broader demographic and industrial resources a state can draw on over the longer term from the military capabilities that the state can put into use in the immediate term for strategic gain. Mearsheimer (2001) argues that a state possesses military power and latent power. Military power is represented by the quality and quantity of a state's active armed forces while its latent power reflects "the raw potential it can draw on when competing with rival states" (Mearsheimer 2001, 55), or the "societal resources that a state has available to it to build military forces", which for Mearsheimer are its economic wealth and population (Mearsheimer 2001, 60). This thesis adopts a similar approach by thinking about cyber capabilities in terms of the broad societal resources and the military or governmental units used to carry out cyber operations.

Latent cyber capabilities represent the state's long-term cyber potential and exist throughout broader society such as in the business and academic sectors rather than being centralised within government structures. They can nevertheless be drawn on or utilised by government to achieve strategic objectives in cyberspace through defensive or offensive cyber operations. Societal resources are an essential consideration given that so much of cyberspace infrastructure, expertise, industry, and technology exists outside government control. I have hypothesised that these resources help to supply the state with the means to establish active cyber capability and are used as independent variables to explain the proliferation of active capability.

To achieve strategic aims like protecting critical infrastructure or causing political or economic disruption to rival states, governments must also develop the organisational capacity and policy to operate through cyberspace defensively and offensively. Unlike latent cyber capabilities, active cyber capabilities are under the direct control of government and embedded within government structures. This information is essential for gauging how governments are preparing for cyber conflict and for examining the relationship between latent potential and active units. The active capability indicators are used as the dependent variables in the analysis on the drivers of capability proliferation.

Measuring active cyber capabilities requires an examination of a state's observable and documented policy developments. Ideally, offensive cyber capabilities would be measured by the number and sophistication of the malicious code and zero-day exploits governments possess. This would be analogous to quantifying and qualifying a country's military systems – warships, planes, tanks, or nuclear weapons – to measure conventional or nuclear capability. Unfortunately, cyber weapons are near impossible to account for because they are by nature non-physical and only observable if one were to gain access to governmental computer systems.

Governments, moreover, are highly secretive over their cyber weaponry because once a cyber-weapon is revealed to the world, others can learn from its design and defenders can patch their vulnerabilities, thus lowering its strategic value. In 2016, a hacking group known as the Shadow Brokers stole and publicly released an 'arsenal' of software exploits developed by the NSA, which included those used in the WannaCry incident (Solon 2016). Of course, this is neither a feasible nor ethical approach for a systematic data collection effort.

This research takes the alternative approach of considering the structures where a state's cyber capabilities are organised and centralised, and these are often within government units functioning at the level of computer network operations. Active capability gauges the capacity to conduct cyber operations as a means of achieving strategic goals. Operational government units, with their active involvement in CNO, embodies the state's active cyber capabilities. Strategy formulating entities, on the other hand, are tasked with defining the goals rather than engaging in CNO themselves. My inclusion of an indicator of national cyber security strategy, which I organise under the active capability category, is an exception to this rule.

Active capabilities are differentiated into civilian and military aspects. A 2013 assessment by the United Nations Institute for Disarmament Research (UNDIR) found that forty-seven states involved the military in their cyber security programmes while sixty-seven states had purely civilian cyber security programmes (UNDIR 2013, 1) The civilian organisations assessed here are those purely dedicated to defence and incident response. It is at least possible, if not likely, that units in the military domain can and do engage in offensive missions on the other hand. This may allow some tentative

judgements to be made about countries' relative investments in offence and defence, although it is more accurate to refer to this as a civilian and military distinction.

How is the data collected?

The research involves a mixture of original data collection and collection from pre-existing databases. Specifically, the active cyber capability component is collected originally¹². While the latent capability indicators are derived from pre-existing databases, the active capability component of the NCC dataset involves the collection of information on the military cyber units, national CSIRTs, and national cyber strategies established by states. The key information that is sought is the presence of each of these types of units and the year the structure was created, or strategy document published. This allows the creation of a time series-cross sectional data set which provides information on which countries have active cyber capabilities and when these were present.

The presence of military units, national CSIRTs, and strategies is confirmed through comprehensive desk-based research on a wide range of publicly available sources. Evidence is first collected from government and military websites, resources from international organisations non-governmental organisations and think tanks, academic literature and books, journal articles, and cyber security company reports.

Then a systematic internet search is carried out to find data from other sources such as media reports. To do this, Google's search engine is used with search terms including the name of the country, the terms 'cyber', and either 'military unit', 'strategy', or 'CSIRT'. Since the data also needs to vary across time, the searches are also conducted for each specific year from 2000 to 2017, using Google's historical search tool to specify the year. This helps to capture historical units or strategies that may have since been overshadowed by new organisations or documents. Google translate is used extensively to translate foreign language sources.

Where evidence is found of an active cyber capability, the relevant country-year row in the dataset is coded with the number '1' indicating the presence of capability. If an exhaustive search of the sources results in no evidence for a particular capability, this will be judged as sufficient evidence that the country did not possess this capability and the country-year row is coded as '0' indicating the absence of capability.

¹² There are some pre-existing repositories of cyber security strategies, for example from the ITU (International Telecommunications Union n.d.), but these were found to be incomplete and so further research was needed to identify additional strategies, or to ascertain whether a particular document met the coding criteria for a national cyber security strategy.

Unless the source is the official website of the CSIRT or the military unit, or the strategy document itself, I require two independent sources corroborating the same information before I code a capability as present. If this evidentiary standard is not met, or if the year of a unit or strategy cannot be established, then the country is coded as missing in the data set and will not be included in the analysis. Romania, Cuba, Ukraine, and Bangladesh are coded as missing for the military CNO unit variable because of insufficient evidence. But given that these cases constitute just 4 out of 194 countries (2% of the dataset), this is not expected to have a significant effect on the findings.

The specific coding criteria for each active capability indicator are described in the relevant sections of this chapter. The indicators of latent capability and other control variables used in the analysis are collected from pre-existing data sources, which are also detailed further in the relevant sections of this chapter.

This process took months to be sufficiently confident that all relevant sources had been consulted for all 194 countries. Although all efforts were taken to be comprehensive, one cannot rule out the possibility of missing data due to government secrecy. Given that it was possible to collect information on national CSIRTs and military cyber units for highly secretive countries like Russia, Iran, and North Korea this problem is likely overstated. It is important to make clear that the following analysis is conducted on known capabilities, although the data set will be continuously updated in the future as new information comes to light.

The next part of the discussion sets out each component of latent and active cyber capability and explains how the concepts are quantified. This also includes a discussion of reliability and validity issues and potential weaknesses.

Indicators of latent cyber capability

Latent cyber capabilities are assessed across the dimensions of technical skill, knowledge, industry, and infrastructure. Unlike the active cyber capability data, these data come from pre-existing databases or sources. In many cases, the data had to be reformatted considerably to create the specific variables for this study. Either Excel or Stata was used for this purpose.

It is important to note that many of the following variables should be seen only as approximations, or proxies, of the concept they intend to capture. For instance, the concepts of skill and knowledge are of quite an intangible nature and hard to gauge directly. Instead I rely on quantitative indicators which should reflect these underlying and unobservable characteristics of the state.

Programming skill

The first two components of latent capability capture the technical ability available in a country in areas applicable to CNO and thus an important aspect of the latent potential of the state to pursue and resist influence in cyberspace. Software skills are critical for developing malware and defensive cyber technologies. Since cyber weapons often become redundant after they have been used, skills are essential for continually developing new weapons. For this reason, Slayton (2017, 85) argues that “*cyber weapons are inseparable from skills*”. These types of capability are not only required to develop technology but to conduct computer network operations. As the Military Balance (2014, 19-20) notes:

“the ability to operate in cyberspace requires skills and experience sometimes beyond the traditional competencies of armed forces’ personnel; these include advanced computer analysis and programming abilities and forensic IT skills”.

The urgent demand by governments for skilled operators who can often earn substantially more in the private sector is well documented and provides evidence of the importance of skill to cyber capabilities (Singer and Friedman 2014, 237). All else being equal, a country with a larger pool of talent should have an advantage over a country with less of this resource. It should be better able to develop the tools of cyber warfare and establish operational cyber units. The data set contains one indicator of skill and one indicator of knowledge.

Programming skill is measured by the country’s performance in the International Olympiad of Informatics (IOI) (International Olympiad of Informatics n.d.) the IOI was established in 1989 and involves high school pupils competing in computer programming and coding challenges. Out of all the international Olympiads, is it the most relevant for cyber activity. Computer programming is the activity of writing computer code which is essential in cyber security and offensive cyber operations and therefore a key component of cyber capability.

But because many countries have never competed in the IOI there are substantial missing data. To overcome this, I draw on the results of another competition called the International Mathematics Olympiad (IMO) (IMO n.d.). The IMO was established in 1959 and involves high school pupils from each country competing in mathematical challenges. This is justified because maths is the fundamental intellectual tool underpinning computer science, as it is for all sciences, and a country with greater maths skill amongst its students has more potential to train them into cyber security professionals or hackers. North Korea’s strategy of training the country’s best mathematics students as government hackers, for instance, is well documented (Feakin 2013, 72). IMO performance is

highly correlated with IOI so serves as a suitable substitute to fill in the missing data (correlation = 0.81).¹³

The information on national performance is obtained from the IOI and IMO websites which provide a breakdown of medals won by each country by year. The variable is operationalized as the three-year moving average of medals won over the current year and the previous two years in these two competitions averaged together. First the value of medals in each competition in each year is calculated. In order to give higher medals a stronger weighting than lower medals, bronze medals are given a value of 0.25, silver 0.5, and gold 1. The IMO and IOI results are then averaged to create one overall skill variable for each country.¹⁴

A country may have a medal count of zero not because of low skill but because it chose not to compete for other reasons. An extra step was therefore to identify the countries that had never competed and record their values as missing, rather than to assume they had low skill, resulting in these countries being removed from the analysis. Some countries had competed in some years but not in others. In order to estimate their missing values, I forward filled their medal count from previous years where they had attended.

I use the 3-year moving average to smooth out short term fluctuations in performance and to give each state a more stable skill score. An advantage of these data sources is that the IOI and IMO have the highest participations rates compared with other international Olympiads which helps to maximize the data set's scope. Moreover, as these prestigious competitions are held annually and are attended by many countries worldwide, it is a useful resource for use in the time series-cross sectional dataset.

Computer Science Knowledge

Related to skill is the concept of knowledge. My second indicator of latent capability is the cyber-related knowledge from a more theoretical, academic level and is assessed by the publication output in computer science coming from the state. This data reflects an ability to produce new research that could be applied in cyber operations. The SciMago website (Scimago n.d.) provides a breakdown of documents published by each country by year. Out of the 27 academic fields available from this source, computer science is selected as it is deemed the most applicable to the ability to engage in cyber operations (Kallberg and Bhavani 2012). An alternative field like engineering may capture some computing related knowledge but would be too broad because it also includes many research areas not directly related to computing. The yearly data is downloaded from this website then combined to complete the 2000 to 2017 time series. I create another version of this variable that is

¹³ Calculated by author using Stata 15©.

¹⁴ Another method that I use for some analyses is to divide the weighted medal count by the number of times the country has participated. The results do not change substantially under this alternative method.

the computer science articles divided by a country's population to gauge the efficiency of knowledge production and to control for large populations.

Latent cyber capability index

Given the theoretical importance of skill and knowledge to country's ability to operate in cyberspace (Slayton 2017), the dataset includes a composite index variable based on Olympiad performance and computer science publications to approximate each state's overall latent cyber capability in these areas. A composite index combines several variables into a singular variable to give an average assessment of a theoretical concept. Here it is used to give an idea of the current ranking of countries in terms of their latent skill and knowledge for cyber operations. The two component variables are Olympiad skill measure just described and a measure of net computer science articles published.

My approach builds on recently published scholarship by Beckley (2018). He argues that capability assessments should account for per capita resources as well as gross resources, so as to not overestimate the capabilities of the most populous nations and to account for some of the inefficiency associated with large populations. Adopting similar methods, my computer science knowledge component is calculated by multiplying total computer science journal articles with per capita journal articles to create a proxy for net computer science knowledge. This method allows me to gauge both the country's total knowledge production output and how each individual in a society contributes to this knowledge production on average.

I convert my Olympiad skill and net computer science knowledge variables into z-scores to standardise them (put them into comparable dimensions) thus allowing them to be averaged. Z-scores are calculated by subtracting the mean of a variable in the entire population of countries from each individual country's value and dividing by the standard deviation. Z-scores indicate by how much they vary from the mean value of each variable in the entire population of states. I then average these two z-scores. A z-score of 0 indicates that a country has the mean capability, negative values indicate below mean capability and positive values indicate above mean capability. I then convert them into t-scores which places the scores in a different scale with no negative values. I do not want negative numbers because I want to avoid division of negative numbers in a later chapter when I assess the relationship between relative capabilities and conflict.

Software Industry

The industry variable gauges the ability of a society to design the technologies that can be applied to cyber defence and offence. Scholars of military power have argued that a country cannot become a

top-tier power without a domestic manufacturing base because without the industrial capacity of its own, a country will be dependent on inferior imported military hardware while the privileged countries at the forefront of technological innovation and production can develop the most advanced tools for warfare (Buzan and Herring 1998, 30). While the international arms trade can help somewhat in redressing the imbalance in military capabilities, the industrial leaders have an incentive to keep hold of the most sophisticated technology to maintain their qualitative military advantage in world politics.

The same might be true in the cyber domain since states that possess the strongest software industry can produce the most sophisticated cyber weapons or security tools, and the most capable states are unlikely to make these commercially available in the global cyber arms trade. Commercially available cyber technology is likely inferior to a state's most advanced tools.

Industry is also an important indicator of the country's ability to maintain and develop its technical knowledge base. Without an established industry for a country's graduates to work in, they may search for work abroad rather than contribute to their own country's capability in a process known as "brain drain" (Gibson and McKenzie 2011, 107-111). It is little wonder then that the development of a domestic IT industry is a prominent goal in many of the national cyber security strategies. The 2016 Australian National Cyber Security Strategy for example aims to "promote Australian cyber security products and services for development and export, with a particular focus on the Indo-Pacific region" (Australian Government 2016, 45). The presence of established industry therefore helps indicate whether the country has the means to hold onto the technically skilled population it educates.

The software industry is especially relevant to cyber capabilities as it is involved in the designing, developing, manufacturing, and supplying of computer and Internet related technology and services to supply governments with cyber tools it can apply in cyber defence and offensive operations.

An indigenous cyber industry is also a useful asset for avoiding dependence on foreign IT goods which may have vulnerabilities and exploits written into them (Military Balance 2014, 21; Pollpeter 2015, 156). It is possible for a foreign company to deliberately leave backdoor access on a product which is unknown to the state using it. This is especially concerning if the vulnerable software or hardware is used in industrial control systems of critical infrastructure. States that produce IT products therefore have an advantage over states that are dependent on foreign goods and services. These concerns have prompted some western states for example to ban products from Chinese IT company Huawei and Russian anti-virus software company Kaspersky Labs (Bowler 2020; Caruana 2020).

The industrial component is measured using two indicators. The first is a measure of the size of a country's software industry by the number of software companies headquartered there. The data comes from Capital IQ platform (S&P Global n.d.) which provides information on "99.9% of the

worlds market capital”. Software was selected as the industry classification because it covers a broad range of offensive and defensive cyber technology that can be used in cyber operations. Using information on the year the company was founded and where it is headquartered this variable was adapted into a country-year format. While this indicator is helpful in capturing the size of the industry in a very relevant area of technology, it does not measure how much software is developed by the country.

To indicate the output of a country’s cyber-related industry, the second indicator is the value of exports (in current US dollars) in the Information and Communications Technology (ICT) sector. This variable comes from the World Development Indicators by the World Bank who describe the indicator as follows: “Information and communication technology service exports include computer and communications services (telecommunications and postal and courier services) and information services (computer data and news-related service transactions)” (The World Bank n.d.). Since the ICT service industry sector is evidently broader than the software industry, the number of software companies are not likely to correspond entirely with ICT service exports.

Cybersecurity infrastructure

Cyber infrastructure is the third component of latent cyber capabilities. In the cyber domain, infrastructure refers to the structures such as network connections, servers, computers that enable Internet operations. Infrastructure has been identified as an important dimension of cyber capability in previous research (Military Balance 2014, 22; Billo and Chang 2004, 22; Booz Allen Hamilton 2011).

All cyber operations depend on Internet infrastructure, but it is not just the presence of infrastructure but its quality that is crucial to the state’s overall cyber defences. Cybersecurity infrastructure is measured by one indicator, a country’s number of secure Internet servers. Servers are a type of computer hardware that enables communication between a client computer and Internet content and are one of the basic building blocks of the Internet. A secure server is one which utilises encryption technology to store information in a scrambled format instead of plain text to make the communications very difficult to be monitored (The World Bank n.d.). This therefore gauges the prevalence of cyber infrastructure in the country as well as how secure it is.

Secure ICT is a fundamental asset for defence against cyber operations, many of which aim to intercept information as it is transmitted through Internet connections. The more secure servers in a country the more protection individuals, companies, organisations, and governments have their communications being targeted by malicious actors. High numbers of secure servers may also correlate with a high usage of other cyber security technologies and therefore could serve as a proxy

variable for a more general defensive capacity. The variable is the number of secure servers existing in the country per million people. This data comes from Netcraft and available from the World Development Indicators (The World Bank n.d.).

Industry and infrastructure are not included in the latent capability index, which focuses purely on skills and knowledge. Skills and knowledge should be a necessary resource for engaging in cyber operations because it is needed for creating the technology and for conducting operations, both offensive and defensive. There are some states, however, that do not have a strong industrial base or secure internet infrastructure that can nevertheless engage in cyber conflict. While these factors are not included in the index, they are used in various sections of the forthcoming analysis as stand-alone variables.

Indicators of active cyber capability

Active cyber capabilities are assessed with three indicators – the presence of a military computer network operations (CNO) unit, a national computer security incident response team (CSIRT), and a national cyber security strategy (NCSS). These are dichotomous variables meaning they take a value of 1 if the entity is present or 0 if absent. The data was collected and coded into variables through a mixture of primary and secondary Internet-based research. Primary sources included national cyber security strategies and other official documents and defence ministry websites. Secondary sources included various think tank reports, data bases, and media reports. The information is then turned into numerical data and stored on an Excel spreadsheet. These variables are collected for 194 countries from 2000 to 2017. An appendix is included at the end of this thesis with a complete listing of all national CSIRTs, military units, and strategies collected for this research.

Military Computer Network Operations (CNO) unit

A logical approach for assessing a state's ability to conduct computer network operations is by quantifying the government organisations responsible for them. The first indicator of a country's active cyber capability is the presence of a military Computer Network Operations (CNO) unit. A CNO unit is defined as *a governmental organisation that engages in Computer Network Operations on behalf of a country's military*. This indicator shows whether the state has integrated cyber security into their military planning and operations.

These units had to meet the criteria of being government entities, tasked with engaging in defensive or offensive military operations involving computer networks. An obvious example of one of these unit is the U.S. Cyber Command – created in 2010 – which “unifies the direction of cyberspace operations, strengthens DoD cyberspace capabilities, and integrates and bolsters DoD's cyber

expertise” (Department of Defense n.d.). Organisations involved purely in policy or research and development are excluded. Also excluded are military-sector CSIRTs which – although technically being military units engaged in cyber operations – are purely defensive, and incident response capability is covered by the national CSIRT variable.

Organisations considered ‘cyber commands’ are encapsulated within this indicator rather than treated as a separate entity. There is no clear definition of a cyber command, but they appear to be the highest military coordinating authority on military cyber security. Sometimes they are a separate branch of the military as in the case of Germany’s Information and Space Command (Bundeswehr n.d.), yet there is so much variance across countries in terms of the location of the department within the military’s organisational structure that it is difficult to code clearly. The decision was therefore taken to group them with any military cyber unit because of no clear delineating criteria for a cyber command.

The NCC dataset does not distinguish between offensive and defensive CNO units because there is not enough information on this aspect. It is likely that most of these units have an offensive role since military forces must be prepared to engage in every type of military activity. As the US Cyber Command mission states, the function of the cyber unit is to “conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries” (Department of Defense n.d.). Moreover, there is an overlap in skills and methods between offensive and defensive computer network operations. It is therefore likely that many CNO units have a dual role and so it would be impossible to code the variable into offence and defence anyway.

This variable measures the presence of cyber units that are involved in military operations. These are generally situated organisationally within a state’s armed forces, defence ministries, or military intelligence agencies. Given issues of secrecy, there may be no open source information available about some units. Understandably, this might especially be the case for units located within a country’s intelligence agencies such as GCHQ in the UK or the National Security Association in the United States. This is unfortunate, as these agencies are an important component of national cyber capability. For example, as Gioe, Goodman and Stevens (2020, 218) point out:

“Today, on account of their relative experience with the technical requirements of both cyber offence and defence, the United States and the United Kingdom rely on their SIGINT agencies to carry out much, but not all, of their offensive cyber operations.”

Given the secrecy of these types of organisations however it might not be possible to identify the presence of military CNO units consistently and reliably by trying to search through open-source information on each country’s intelligence agencies. So, while the data collection partly involves searching through each country’s armed forces and defence ministry websites, the decision was taken

not to do this for intelligence agencies since they are unlikely to consistently reveal relevant units. As a result, there is a possibility of missing units engaged in military operations that are situated not in any military organisation but in an intelligence organisation. Yet this is not to say that a military CNO that falls organisationally under an intelligence agency cannot be identified from other sources. For instance, the Information Security Centre (Military Unit 64829), as documented by Jeffrey Carr (2012, 229), is located within Russia's Federal Security Service (FSB).

While this is a potential source of missing data for this specific variable, there is probably a high correlation between military and intelligence capability in cyberspace. Scholars suggest there are "few technical distinctions" between offensive and intelligence gathering operations in cyberspace (Whyte and Mazanec 2019, 77). The organisational synergy between US Cyber Command (a military organisation) and the NSA, for instance, is also well documented (Pomerleau 2019; Gioe, Goodman and Stevens 2020, 219). As the appendix of this thesis shows, the countries one would generally consider to be the most advanced intelligence powers – the Five-Eye countries and other major powers like Russia, China, Brazil, Germany, Japan, and France - are mostly (with the exception of New Zealand) recorded as possessing a military cyber unit (or multiple units), frequently going back several years. Therefore, there is reason to be confident that the risk of significantly underestimating the cyber capabilities of these countries is minimal if the military CNO unit data is already capturing much of the information on intelligence capability. In the future, the dataset will be continuously updated as new evidence comes to light and the data collection strategy can be expanded to include resources more directly relating to intelligence organisations.

A state's possession of CNO units helps gauge its ability to conduct military operations in cyberspace as it presupposes the presence of trained personnel to operate within them and the basic infrastructure and organisation to achieve operational capacity. It is clearly not a suitable measure of overall capability however because it does not wholly gauge the capabilities that might reside in non-military organisations, the proxy groups that the state may act through, or the societal resources existing outside direct government control. Nevertheless, it at least captures the intent and effort by the state to boost its military influence in the cyber domain. It is therefore reasonable to use this indicator as a dependent variable for helping to investigate why states pursue active cyber capabilities.

National Computer Security Incident Response Team (CSIRT)

The second indicator is the presence of a national Computer Security Incident Response Team (nCSIRT)¹⁵. These are a key government organisation and asset in the defence against cyber

¹⁵ Alternative names for these teams include CERTs (Computer Emergency Response Teams) and CIRTs (Computer Incident Response Teams).

incidents. They consist of a unit of IT specialists whose functions include responding to and managing cyber incidents, analysing threats, detecting vulnerabilities, and disseminating information on behalf of an organisation or government (West-Brown 2003). CSIRTs have no offensive role and can be considered a cyber defensive capability.

The earliest CSIRTs were mostly established in the private sector and by the technical community, but as cyber threats have grown, they have become a fundamental component of a state's national cyber security policy. The first CSIRT was established at Carnegie Mellon University in response to the 1988 Morris Worm cyber incident and they have since proliferated widely to many states (Software Engineering Institute n.d.). These teams can be based throughout various public and private sectors of society such as private companies, academia, or the military and are often the first point of call when a cyber breach occurs. The focus here is on national CSIRTs which are usually established by government to have country-wide responsibility, rather than sector-specific CSIRTs.

The European Union Agency for Network and Information Security considers national CSIRTs as "teams that serve the government of a country by helping to protect the critical information infrastructure" (ENISA 2012). According to Carnegie Mellon, the most basic characteristic of a national CSIRT is that it is "specifically recognised by the government as having responsibility in the country or economy." (Software Engineering Institute n.d.). Teams that are considered 'national' can in fact vary widely in terms of their area of responsibility, the government ministry or department in which they are located, and whether they are government or non-governmental bodies (Morgus, Skierka, et al. 2015). A more precise definition is therefore needed to code the CSIRT data into the cyber capability data set.

In this study, a national CSIRT is defined as "*any computer security incident response team that is tasked to respond to cyber incidents affecting government networks or networks and users nationwide.*" This broad definition allows me to include both privately established CSIRTs which serve government, like Japan's JPCERT/CC, as well as government established CSIRTs which protect national but not specifically government networks, like South Korea's KrCERT/CC. Privately run CSIRTs which are not tasked with protecting government are excluded. The key criterion is that the team has some link with government – either by being a government entity, or by having a role to protect government. Sector-specific CSIRTs operating solely in the private sector, academic sector, or military sector, for example, are excluded. Due to these criteria, a country may have more than one national CSIRT as would be the case if a state established one CSIRT for defending government and another for defending the wider nation. Both are considered national CSIRTs here. For simplicity, the variable is binary and records whether the country has no CSIRTs (coded as 0) or at least one of these types of CSIRTs (coded as 1) but does not count the total number.

National cyber security strategy

The third and final indicator of active capability is the presence of a national cyber security strategy. IR theorists have long recognised the importance of non-material as well as material factors in contributing to national power (Morgenthau 1948, 96-108; Biddle 2004). The presence of a strategy of action suggests a greater level of preparedness and organisation by the government to pursue its aims in cyberspace. I therefore include the presence of a national cyber security strategy in the NCC dataset as an indicator of non-material active capability.

There are multiple types of policy document that could be relevant to cyber security, but this research focuses on a specific narrowly defined type of document. A national cyber security strategy (NCSS) here is defined as “*an official, government published document setting out the national approach to cyber security*”. NCSSs are documents that articulate the government’s broad cyber security objectives and the steps it will take to achieve them. There are pre-existing repositories for these documents, like that of the ITU (International Telecommunications Union n.d.), but they are incomplete. Therefore, a new data collection effort was warranted to gather this information systematically and comprehensively.

The key criteria for coding a document as a national cyber security strategy is that it addresses the issue of cyber or information security directly. Documents excluded on this basis include ICT development strategies because they do not necessarily concern security issues. Moreover, the strategy has to refer to the nation as a whole, as opposed to a particular sector. This means that strategies focusing on the military’s cyber approach, for instance, are excluded. In most cases, the title of the document contains the words, “cyber”, “security” and “strategy” which makes coding straightforward. Documents are still counted as NCSSs if the words in their titles are closely synonymous with the word cyber. For instance, France uses the word “digital” and Russia uses the word “information”. While the Russia case reflects a non-western perspective of cyber security, the concepts of information and cyber security are sufficiently similar to be treated as one for the purposes of this study.

To code the year the strategy was published, the year contained within the document is used or secondary information is used if this information is not available. States can publish new or updated national cyber strategies over time and these are accounted for in the data set. A summary of all the latent and active capability variables coded into the data set are provided in table 1.

Table 1.
NCC dataset variables and measurement

<i>Type</i>	<i>Indicator</i>	<i>Measure</i>
Latent capability	Programming skill	3-year moving average of IOI and IMO gold medals
	Computer science knowledge	Computer science journal articles published
	Software industry	Number of incorporated software companies/ ICT service exports (current US dollars)
	Secure infrastructure	Secure Internet servers (per million people)
	Latent cyber capability index	Programming skill and computer science knowledge converted to t-scores and averaged
Active capability/ strategy	Military CNO unit	Presence of an agency dedicated to computer network operations for military purposes
	National CSIRT	Presence of CSIRT with national or governmental responsibility
	National Cyber Security Strategy	Presence of published national strategy for cyber security

Chapter V

Research Design for Investigating the Causes and Consequences of Cyber Capability

Introduction

This chapter explains and justifies the methods I adopt in the following chapters to address my research questions. To restate the research objectives, I seek to describe how cyber capabilities have proliferated internationally, explain the determinants of this process, and assess the effect of capabilities on cyber conflict.

The first of these analytical chapters (chapter 6) asks: *how have capabilities proliferated* and involves a description of the NCC dataset variables to highlight first the relative position of countries in the international system in terms of their latent cyber capability and describe the rate and extent at which states have adopted active cyber capabilities and strategies.

In chapter 7 I ask: *what are the driving factors behind cyber capability proliferation?* Here I use indicators of active capability as my dependent variables and run statistical tests to determine their relationship to latent capability measures and threat-based indicators obtained from secondary sources. The analysis begins by identifying bivariate relationships before moving to a more robust multivariate regression model.

In the following three chapters I ask *what are the effects of capability on cyber conflict?* Using my capability data to create the explanatory variables, I test their statistical relationship to cyber conflict, drawing on a published dataset. Each chapter addresses this question from a different perspective. Chapter 8 examines how defensive capabilities relate to cyber incidents from the defender's perspective, chapter 9 examines how the balance of preponderance of capabilities between two rivals affects their propensity for conflict, and chapter 10 investigates the association between the initiator's capabilities and conflict.

Finally, chapter 11 adopts a qualitative case study approach to trace the process of capability development and conflict initiation in the country of Iran. This illustrates the possible causal mechanisms leading from latent cyber capability to active cyber capability and then to engagement in cyber conflict.

I structure this chapter by first discussing the underlying assumptions about establishing causality before going through each of these research questions and explaining my methods. This includes a

discussion of the specific dependent, independent, and control variables, the temporal and spatial scope of the data, and the methods of statistical or case study analysis adopted to address them. Variables taken from the NCC dataset have already been explained in the last chapter, so there is no need for repetition here. However, I will describe in more depth any non-NCC dataset variables that are taken from other sources. Some methods that are overly specific are explained during the later analytical chapters instead of in this discussion.

Establishing causality

Since a large part of my methodology is about establishing patterns of causality between variables, I need to clarify my underlying assumptions regarding causation. I take a “Neo-Humean” approach to causality which has several prescriptions about how causality should be established (Brady 2008, 219). First, there should be a correlation between the theorised cause and effect. For a causal relationship to exist, a change in the value of the explanatory variable should have a concomitant change in the outcome variable. Throughout my analyses, I determine correlation through a series of bivariate tests which are a method of inferential statistics. These tests include cross-tabulations, different in proportions tests, and correlational analysis, which are all standard in social science research design (Salkind 2010).

Secondly, one might want to specify whether a cause is considered sufficient or necessary to have its effects. I do not suggest that any of my proposed explanatory factors are necessary or sufficient conditions of their hypothesised effects. There are cases, for instance, where a state has established active cyber capabilities, yet did not have high latent capability. Moreover, there may be cases where a country had a military CNO unit but did not employ its capabilities against a rival state, as would be the case if this type of capability were a sufficient condition for the initiation of conflict. Instead I infer causation in probabilistic terms and argue that there will be an increased likelihood of the hypothesised cause leading to the event.

To determine if a correlation is meaningful, I conduct tests of statistical association throughout my analysis. Statistical significance testing is a means of showing whether the relationship between two variables is a real difference, rather than one that has arisen by chance (Michaelson and Hardin 2010, 1361). These tests provide a p value which conveys how likely it is of obtaining the observed results if there was no real correlation. As is common practice, p values lower than 0.05 are considered sufficient to reject the hypothesis that there is not a real relationship between the variables and to accept instead that the result is statistically significant (Capraro and Yetkiner 2010).

Thirdly, alternative causes should be considered. To account for rival explanations or confounding variables I run multivariate regressions which model a multicausal relationship and allows me to

control for the effects of other variables aside from the key independent variables identified by the theory. This adds robustness to the original relationships uncovered by bivariate tests. If the initial results survive a more robust test, there is more evidence that a causal relationship exists (Ray 2003, 5).

Another important condition for causation is temporal precedence. Establishing that the proposed cause preceded the effect is important for providing more evidence of a causal relationship. If not, reverse causality could be explaining an observed correlation. In the multivariate analysis I can account for this by lagging certain variables to achieve the correct temporal ordering, as is common practise in quantitative IR research (Barbieri 2002, 49).

Finally, theory is crucial for establishing causal relationships hence why in chapter 3 I developed a set of theoretical expectations based on a review of the relevant literature. There is more reason to believe a correlation is causal if it conforms to the expectation of the a theory because there is a logical reason behind it. Nevertheless, I refrain from concluding with full certainty that any of my observed correlations are causal. Instead I aim to provide evidence in support of causality.

Methods of statistical analysis

With the exception of chapter 6, which is a descriptive analysis, I use similar statistical methods across chapters seven to ten. To assess the determinants of capability or the relationship between capability and conflict, I begin by employing a series of bivariate tests. I first use cross tabulation with a chi-square test of statistical significance. This approach compares the observed number of observations within cells of a cross-tabulation table (according to their value under each categorical variable) by the number of observations that would be expected if there was no relationship between the variables. A p-value accompanies the chi-square statistic which conveys whether the association is statistically significant. I also frequently employ a difference in proportions test to determine if the conditional probability of an outcome is significantly different from the baseline probability, following a similar method to Bremer (1992, 326).

After bivariate tests I proceed to a multivariate analysis which allows me to include multiple independent and control variables together. Multivariate methods are useful for establishing more robust findings as they allow the independent effect of each explanatory variable to be measured while controlling for the effect of all other variables on the model. For the multivariate analysis I adopt a method of maximum likelihood estimation called logistic regression. Logistic regression is “a statistical technique used in research designs that call for analysing the relationship of an outcome or dependent variable to one or more predictors or independent variables” (Menard 2010, 730). This method is standard in political science when the dependent variables take either one of two possible

values, as my indicators of active cyber capability and cyber incidents do (Bennet and Stam 2003, 56). Since I am running the analysis using panel data (each country is observed over the same time period), I employ robust standard errors clustered by country to account for the problem of heteroscedasticity (Cameron and Trivedi 2005). Stata 15 statistical software is used for all statistical analysis.

Logistic regression coefficients (the values that express the size and direction of the relationship between explanatory and outcome variables) are expressed in terms of log odds. To communicate these effects in a more intuitive way, I often express these in terms of the change in probability in the outcome variable that results from a given increase in each explanatory variable.

Part 1: Describing the proliferation and distribution of capabilities

In chapter 6 I describe the NCC dataset to provide a picture of how cyber capabilities have proliferated, of the current distribution of capabilities in the international system, and an overview of the most capable countries. This is a key part of developing my theory because it establishes how a state derives its opportunity for engaging in cyber activity. By proliferation, I am referring to the increase or acquisition, either across time or geographical space, of latent and active cyber capabilities to states around the world. By distribution, I am referring to the amount of resources held by each country relative to others.

I highlight the most capable countries in each indicator by ranking the top ten countries using descriptive tables by their latent cyber capability (programming skill, computer science knowledge, software industry, secure infrastructure etc.). Then I use line graphs to show how the resources of the top three most capable countries have changed from the year 2000 until 2017. The countries are limited to three because otherwise the visualisation would appear overly cluttered.

I then present the complete latent capability ranking, based on a composite index of programming and computer science knowledge. As cyber capability is fundamentally based on skill and knowledge, these variables were chosen as the most appropriate method for approximating a country's potential to project and resist influence in cyberspace.

Next, I describe the proliferation of active cyber capabilities as measured by the number of military CNO units, national CSIRTs, and national cyber strategies in the international system. To describe across-space distribution, I show world maps to highlight the countries that have adopted each of these assets. To describe over-time proliferation, I use bar charts to track the increase in overall numbers of these assets from 2000 to 2017.

Part 2: Identifying the determinants of cyber capability

Chapter 7 investigates the determinants of national cyber capacity-building globally. By determinants, I am referring to the factors that will have an effect on the adoption of capabilities. I want to identify if the explanatory variables that I derived from the opportunity and willingness theoretical framework can account for the increase in active cyber capabilities across the international system. The following discussion sets out the research design for this part of the analysis.

Unit of analysis

This analysis draws on a cross-sectional time-series data set¹⁶ meaning that the data varies both across space (countries) and time (years). Specifically, the dataset contains 3,492 observations of 194 sovereign nation states recorded over the period 2000 through 2017. The unit of analysis is the country-year which means that each observation provides information about one country in a given year. I adopt this approach because I am interested in identifying the country-specific characteristics that increase the likelihood of proliferation. The 194 countries are all the UN member states plus Taiwan and so represent practically the entire population of states in the international system.¹⁷ Because I use information on almost every country, selection bias is eliminated and the conclusions drawn from the analysis refer to all countries in the international system, rather than a subsample of countries.

The temporal domain is limited to the 2000-2017 period. The Internet has its foundations in the US military's ARPANET developed in the 1960s, but has only become popularly accessible in the early 1990s with the invention of the World Wide Web. However, most activity has occurred later than this in the 2000s. As the following chapter will show, the proliferation of capabilities also only began in earnest after 2000. Therefore, the 2000-2017 period was chosen partly to capture most of the relevant cyberspace activity. Another reason for this decision is that this time span matches closely with an important data set on cyber conflict (Valeriano and Maness 2014) that is used later to explore the relationship between capabilities and cyber incidents. While it is somewhat arbitrary it captures very up to date developments at the time of writing contributing to the research's policy relevance.

Dependent and explanatory variables

¹⁶ This is also known as a panel dataset.

¹⁷ Taiwan is effectively a sovereign nation state but is not a recognised UN member due to pressure from China over its claim to Taiwan.

A dependent variable, or outcome variable, is used to quantitatively capture the phenomenon the researcher is trying to explain and can be defined as “the result of the action of one or more independent variables” (Salkind 2010, 347). The two dependent variables for this part of the analysis capture whether a government has adopted active cyber capabilities in the civilian and military sectors. The dependent variables are the presence of a *national CSIRT* and a *military CNO unit*. As already discussed, these are dichotomous variables that take a value of either 1 if the country had these assets in a given year and 0 if otherwise.

An independent, or explanatory variable, is one that is manipulated by the researcher to ascertain whether changes to it have an observed effect on the dependent variable (Fan 2010, 592). The independent variables represent the state’s opportunity and willingness to adopt active cyber capabilities in line with the theoretical framework established in chapter 3. A state’s opportunity is modelled by its latent resources. The variable *Programming skill* is based on a country’s performance in the IMO and IOI. The variable *computer science knowledge* measures the publication output of a country in the field of computer science.

Software industry is measured by the number of software companies incorporated in the country. Issues may arise with this variable if the companies associated with a country are established there for administrative or tax purposes, rather than reflecting an underlying quality of the country where the company is incorporated. As a robustness check, ICT service exports (current US dollars) is used as an alternative measure of industrial capacity. This data is taken from the World Development Indicators by the World Bank (World Bank, n.d.).

Financial capacity is gauged by Gross Domestic Product (GDP) per capita (constant US dollars) which is obtained from the World Development Indicators by the World Bank (World Bank, n.d.). GDP per capita is a common measure for economic development and has been used as a proxy for technological sophistication in several studies (Singh and Way 2004; Fuhrmann and Horowitz 2017; Tang 2010, 240). Accounting for GDP per capita also helps to compare its effectiveness in explaining proliferation vis a vis technical skill and industry. As a measure of financial resources, it also explores the assumption that the cyber domain has low financial barriers to entry. Together, these four independent variables are used to test the opportunity-based side of the theory of cyber capability proliferation.

The willingness-based independent variables gauge a country’s international threat environment and are obtained from external data sources. The variable, *interstate rivalry*, is a count of the number of interstate rivalries a country is engaged in. In this analysis, a rivalry is considered to be present if the peace scale developed by Goertz, Diehl, and Balas (2016, 27) has a value of 0 (serious rivalry) or 0.25 (lesser rivalry). The authors determine the peace scale based on the presence of war planning, military conflict, unresolved issues, a breakdown of communication, lack of diplomatic recognition

and agreements. The peace scale data has not been updated past 2015 but here it is forward filled two years to complete the series up to 2017. While a rivalry may have ended within these two years, this step can capture the effect of rivalry in the very recent past in these cases.

CNO unit rivals, indicates the number of rivals a country has that possess a military CNO unit, using the same rivalry coding based on the peace scale data set. This tests the security dilemma notion that cyber capability adoption is influenced by the threat posed by the military capabilities of a rival.

The variable, *cyber threat*, is the three-year moving average of cyber incidents a country has suffered using information from the Cyber Operations Tracker database by the Council on Foreign Relations (CFR, n.d.).¹⁸ The Cyber Operations Tracker records publicly known state-sponsored computer network operations (DDoS, espionage, defacement, data destruction, sabotage, and doxing)¹⁹ since 2005 and identifies which country was targeted. Before creating the variable instances of domestic repression are excluded because they do not represent a threat against the state but against non-state actors within the same country. As the Council on Foreign Relations admits, missing data may be an issue due to a bias towards English language sources and a reliance on open source information. As a result, the relationship between threats and cyber build-ups may be underestimated among non-English-speaking and less open societies and the findings must therefore be interpreted with caution.

The three-year moving average is the mean number of incidents affecting the state over the previous three years and serves two purposes. First, it smooths out short-term fluctuations in the number of cyber-attacks to create a measure that is more stable over time. Secondly, it allows the analysis to account for previous experience of threat under the assumption that changes in national policy are unlikely to be observed in the same year of an incident, but to the general level of threat experienced over recent years. The three-year period is arbitrary, but it seems an appropriate amount of time for states to develop reactionary capabilities.

Finally, the variable, *US rival*, tests the hypothesis that states develop cyber capability as a means of challenging the unipolar country in the international system. For this, a dichotomous measure is created with a value of 1 if the country is rivalled to the United States and 0 if otherwise. The United States is the obvious candidate as a target of balancing because it is the most powerful country throughout the entire period under study, which fits with structural realist theory. The condition of rivalry is built into the variable because by definition any state building up capability to challenge another's dominance would be considered a rival to that state.

¹⁸ This data source is preferable to the DCID (Valeriano and Maness) for the purposes of this analysis because it contains data on not only rival countries and is not dyadic in nature.

¹⁹ For a definition of these terms see the methodology of the Cyber Operations Tracker at <https://www.cfr.org/cyber-operations/#OurMethodology>

Control variables

Finally, control variables are a type of explanatory variable that are not of primary theoretical interest but may have a confounding influence on the relationship between the key independent variables and the dependent variables (Salkind 2010, 252). The multivariate regression includes a further three variables that do not fit under the explanatory framework of opportunity and willingness but are added to control for their potentially confounding influence. A confounding variable is an “antecedent third factor that brings about a statistical association or correlation between two other variables” by being “correlated with both of those two other variables” (Ray 2003, 7). Failing to control for confounding variables can lead to spurious findings and a wrong interpretation of a correlation between independent and dependent variables.

The first control variable is domestic *Regime type*, which describes how democratic or autocratic a country is. This may be correlated with the development of capabilities if democratic leaders are more responsive to public fears of cyber threats than their authoritarian counterparts (Maoz and Russett 1993). Moreover, democratic states are perhaps more prone to the effects of the ‘cyber-industrial complex’ (Diebert 2011), whereby vested economic and political interests push for increased investment in cyber capacity, partly through cyber threat inflation and “cyber doom scenarios” (e.g. cyber ‘Pearl Harbour’) (Lawson 2012; Cavelty 2008, 2). This phenomenon may be more likely in a democracy due to societal openness giving interest groups an ability to have influence in political processes (Risse-Kappen 1991). A confounding relationship might arise because democracy should also be associated with latent resources since democracies are generally more economically developed (Robinson 2006).

On the other hand, capability development could be linked to authoritarian regime type since repressive states are known to employ Internet tools against their own citizens to prevent dissent and collective action (King, Pan and Roberts 2013). Thus, the addition of this variable will also test whether it is democratic or autocratic states that are more likely to adopt capabilities. This is especially relevant in relation to the establishment of military units, which are known to engage in operations not only against foreign actors but against domestic society. For instance, Vietnam established a “cyber warfare unit” in 2018 to tackle “wrong views” over the Internet (Reed 2017). Regime type is measured using Polity IV project’s autocracy-democracy scores which places countries on a scale from -10 (most authoritarian) to 10 (most democratic) (Jagers and Gurr 1995).

The second control variable is *Major power status*. Some states may develop capabilities primarily because they are prestige seekers and perceive that it befits a country of their status, not because they face greater threats (Gilady 2018). To capture the effects of a state being a prestige- or status-seeker, the regression models include a dichotomous variable of whether the country is a major power (1) or not (0) using the Correlates of War classification (Correlates of War Project 2017). In the period

under study, the major powers are the United States, China, Russia, the United Kingdom, France, Germany, and Japan. Since major powers possess more resources and tend to be more engaged in international conflict, this factor is controlled for because it could have a confounding influence in the analysis.

The final control variable, *Internet years*, is operationalised as the number of years that have elapsed since the World Wide Web was invented in 1990. This controls for temporal dependence (that capabilities will be related to time). Cyber capabilities are more likely to be acquired as time goes on due to the inevitable spread and imitation of technology in the international system, as reflected in the technological imperative hypothesis (Buzan and Herring 1998, 50). Time may have a confounding influence on the relationship between resources and capabilities or threat and capabilities given that countries grow their skill, knowledge, wealth, and industry over time and since cyber incidents are also rising over time. Table 2 summarises the three types of explanatory variable used.

Table 2.
Explanatory variables for investigating the determinants of active capability

<i>Type</i>	<i>Variable name</i>	<i>Summary</i>
Opportunity	Programming skill	Recent medals won at the IOI and IMO
	Computer science knowledge	Computer science journals published
	Software industry	Software companies incorporated
	Economic development	GDP per capita
Willingness	Rivalry	Number of rivals
	CNO unit rivals	Number of rivals with military CNO unit
	Cyber threat	Recent cyber incidents against country
Controls	Regime type	Democracy - autocracy classification
	Major power	Major power status
	Internet years	Time elapsed since WWW invented

Part 3: Investigating the impact of capabilities on cyber conflict

Chapters 8, 9, and 10 investigate the effect of cyber capabilities on cyber conflict. This research question can be tackled from several perspectives, hence why it is addressed across three separate chapters. Chapter 8 examines whether a country's defensive capabilities reduces the occurrence and impact of cyber incidents from a rival state, chapter 9 investigates how the dyadic balance of capabilities affects the likelihood of conflict between pairs of states, and chapter 10 shows how capabilities of a state promotes the initiation of conflict by a state against a rival. These research

questions are tackled with quantitative methods similar to the previous chapter. Here, however, the capability data is used as explanatory variables and a measure of cyber conflict as the dependent variable. The following discussion sets out the research design for this part of the analysis, by first explaining the temporal and spatial scope of the data, the variables employed, and the methods of statistical analysis for each of the three chapters.

Units of analysis

Each of the three questions is tackled at varying levels of analysis. Chapter 8 asks if defensive capabilities can reduce the incidence of cyber incidents against a state. For this, I use a country-year dataset. The data on cyber conflict come from a source that is limited to a subset of states that are rivals (Valeriano and Maness 2014), so the temporal and spatial scope is limited to 95 countries recorded from 2000 to 2016 resulting in a dataset of 1,632 country-year observations.

Chapter 9 asks how the relative capabilities between a pair of states affects the likelihood of conflict occurring. For this, I use a non-directed dyad-year dataset, where there is only one observation per pair of states and no distinction is made between the initiator or defender of an incident. According to the DCID there are 130 rival dyads (pairs of states) observed from 2000 to 2016. This results in a data set of 2210 observations.

Chapter 10 asks how a state's capabilities affects the likelihood that it will initiate cyber operations against a rival state. For this, I use a directed dyad-year dataset, where there are two observations for each dyad-year in order to provide the perspective of each state as a potential initiator and a potential defender in a dispute. For instance, there is one observation for the United States – Russia in 2010 and a second observation for Russia – United States in 2010. This allows me incorporate country level information on the initiator or defender and dyad-level information into the analysis. This results in a dataset of 4420 observations.

Although most of the analysis uses the three aforementioned units of analysis, at times I also examine patterns in capabilities and conflict at the system level and how capability is related to the outcome of cyber conflict at the incident level.

Dependent variable

To measure cyber conflict, the dependent variables are derived from the Dyadic Cyber Incident Dataset (DCID) (v1.5) by Valeriano and Maness (2014). In the DCID there are a total of 266 incidents recorded between rival states from 2000 to 2016. A cyber incident is an individual computer network operation targeting a state initiated by another state or on behalf of a state (Valeriano and

Maness 2014, 349). They define their rivalry sample based on the work of Klein, Goertz and Diehl (2006) where rivals are a subset of dyads that are more prone to engaging in military disputes. These data were collected by the authors through publicly available sources obtained through a structured Internet search which were corroborated with cyber security firm threat reports, think-tank reports, and newspaper articles. I use this data source because it is more trusted than other sources (having past the peer review process) and because of its dyadic format. They discuss the potential limitations of the data in their article (Valeriano and Maness 2014) which include the issue of missing data and bias towards English-speaking countries.

The DCID distinguishes incidents by method – DDoS, website defacement, intrusion, and infiltration. I include all types of operation at this stage because I want to first establish in this project if cyber capabilities promote any kind of cyber conflict initiation. Out of the 130 rival pairs, 29 have ever engaged in cyber conflict. To give an overview of the dataset, I describe the number of incidents each of these 29 rival dyads has engaged in over the 2000-2016 period in table 3.

Table 3.
Frequency of cyber incidents between rival dyads (2000-2016)

<i>Rival country 1</i>	<i>Rival country 2</i>	<i>Number of cyber incidents</i>
US	China	48
US	Russia	26
N. Korea	S. Korea	22
US	Iran	20
India	Pakistan	20
Iran	Israel	18
Russia	Ukraine	17
US	N. Korea	8
S. Korea	Japan	8
China	Japan	8
China	Taiwan	8
Iran	Saudi Arabia	7
China	India	7
Russia	Georgia	7
China	Philippines	5
China	Vietnam	5
Russia	Lithuania	4
Russia	Turkey	4
Russia	Estonia	4
France	Russia	3
UK	Russia	3
Germany	Russia	3
Poland	Russia	3
Iran	Turkey	2

Canada	Russia	2
US	Syria	1
N. Korea	Japan	1
Syria	Israel	1
Lebanon	Israel	1

These incident data are transformed in various ways throughout this analysis depending on the question being asked. These will be clarified during the relevant analyses when the purpose behind these methods will be more apparent.

Independent variables

My independent variables are based on either latent or active cyber capability data, but take various forms depending on the level of analysis being used. To assess the defender’s capability from the latent capability perspective I use the number of secure servers in a country. This approximates the extent of encryption across an entire country’s computer networks which could help reduce vulnerabilities to cyber operations. From the active capability perspective, I use the presence of a national cyber security strategy and a national CSIRT. These are also proxy-variables because they may not directly cause a prevention in cyber incidents, but they should correlate to increased effort at implementing greater cyber security practices in general. A national strategy reflects an increased effort by the government to implement policies to improve the cyber security of a country’s institutions. A national CSIRT can relate more directly to the detection of cyber incidents but it also gauges a more general level of effort by the state to build security.

To assess the relative capabilities of two states in chapter 9, I use the military CNO unit variable as the active component and the latent cyber capability index as the latent component. I use these variables as they could be applied to offence and I am interested in states could be deterred by the potential of their rival to retaliate offensively. A preponderance or balance of latent cyber capability is measured by dividing the latent index of the stronger state by the weaker state. A balance of active capability is measured by the mutual possession of military CNO units. A preponderance is if only one state has a military CNO unit.

In chapter 10 I am interested in the initiator’s capability specifically. I therefore use data on a state’s latent capability index – either taken on its own or divided by the defender’s capability to get a measure of relative capability. Moreover, I use the presence of a military CNO unit to gauge the initiator’s active capability. These methods will be explained in more detail during the relevant analyses.

Control variables

In the multivariate analyses on the effect of conflict on capabilities I include several control variables. In chapter 8 (defensive capabilities and conflict) I control for the Internet penetration of a country, defined as the proportion of a population using the Internet (World Bank, n.d.). A country more connected to the Internet should have more need to develop cyber security capacity and should also be more likely to experience cyber incidents. Therefore, it could have a confounding impact between defensive initiatives and the frequency of cyber incidents.

Chapters 9 and 10 focus on conflict at the dyadic level. Here I draw on Bremer's (1992) "pathbreaking" Dangerous Dyads study which was one of the first analyses to explain the onset of conflict between states through multivariate methods (Ray 2005, 278). This article, and its successors (Geller and Singer 1998; Barbieri 2002; Bennet and Stam 2004; Senese and Vasquez 2008), are useful for choosing the control variables for this part of the analysis because they have identified some consistent determinants of conflict which may need to be controlled for in a multivariate analysis of cyber conflict.

I control for *rivalry intensity* which is measured by the level of conventional conflict that a pair of states have engaged in. Pairs of states that have experienced more conventional conflict between them may be more likely to engage in cyber conflict because their interstate relations have deteriorated to such an extent that they are more willing to try new technological means of harming their rival (Valeriano and Maness 2015, 51-54) Furthermore, if cyber operations are seen as a means of managing and de-escalating disputes (Valeriano and Jensen 2019), this may offer another reason why cyber incident would be more frequent amongst dyads that have more history of violent conflict.

At the same time, greater conflict-proneness may be linked to the build-up of capabilities as it creates insecurity (Glaser 2000, 253-256) and could give states greater urgency to invest in a wider range of technological capabilities, including that of cyber. In this sense, conflict-proneness could have a confounding impact between capabilities and conflict. They may also want to invest in cyber capabilities as a way of managing their rivalry.

Since the dataset is limited to only include states engaged in rivalry, the level of animosity between states is already being controlled for to some extent. Amongst rivals, however, there is likely to be some variation in the conflict-proneness of each dyad. In a similar study, Pytlack and Mitchell (2015) measure the rivalry intensity by a composite indicator incorporating territorial disputes, trade disputes, the number of militarised interstate disputes (MIDs), and duration of the rivalry, but find no relationship between this factor and the onset of cyber conflict using an earlier version of the DCIC with a cross-sectional research design.

I take a simpler approach and measure the total number of MIDs experienced by each dyad over period 2000 through 2010 using data from Correlates of War.²⁰ An MID is the threat or use of force from one state to another resulting in no more than 1000 battle deaths (Correlates of War, n.d.) which therefore gauges levels of interstate conflict short of war. When analysing the effect of the initiator's capabilities in chapter 10, I control for the total MIDs conducted by the initiator against the defender from 2000 through 2010. Although the data does not extend past 2010, this method should nevertheless capture the average level of pre-existing hostility in interstate relations, which may spill-over to the cyber domain.

Including an indicator of rivalry intensity also examines the theory of opportunity and willingness if applied to the cyber domain. This would suggest that the initiation of cyber conflict should be driven by the state's active cyber capability and its willingness to carry out a computer network operation. The rivalry intensity variable gauges this willingness component.

When examining the initiation of cyber conflict in chapters 9 and 10, I also control for the *regime type* of the disputing states. In chapter 9 I control for the joint democracy of a dyad as the analysis does not distinguish between the initiator and the defender. In chapter 10 I control for the democracy of the initiator. Proponents of the "democratic peace thesis", on which there is a vast literature, has long held that democratic countries will very rarely engage in armed conflict with one another and most empirical studies have supported this (Maoz and Russett 1993; Bremer 1992; Ray 1993; 1995; Gleditsch 1992; 1995). Several explanations for this phenomenon have been proposed over the years. For example, Maoz and Russett (1993,625-626) offer a structural argument - that democratic states face greater domestic constraints on the executive's use of force which include the presence of an independent judiciary, legislative oversight, free press, and opposition parties, and a normative argument - that the norms of cooperation, trust, and managed competition that citizens of democracies have internalised become reflected in the state's foreign policies. Alternatively, scholars have focused on the political costs of going to war among democracies (Bueno de Mesquita and Lalman 1992) and the greater credibility of a democratic state's signalling and resolve during disputes (Fearon 1994a; 1995), but the entirety of democratic peace thesis explanations are too numerous to review here.

Democracy may also be linked to conflict in the cyber domain. The question has not been tested empirically in relation to the onset of cyber conflict, nor has much theory been developed on the issue. If cyber operations are to be considered another form of conflict, the same logic may apply to the cyber domain as democratically elected governments may want to avoid audience costs associated with cyber aggression or democratic norms may prevent engagement in conflict with other democratic states (Naim 2015). However, since many cyber operations are secretive, democratic

²⁰ MID data has not been updated beyond 2010.

governments may not face these kinds of institutional constraints relevant to traditional Democratic Peace Theory (Buchanan 2016, 118). On a further note, if some cyber operations are a means of avoiding escalation, managing a dispute, and reducing the risk of human fatalities (Smeets 2018, 103), democratic states may in fact be more willing to engage in cyber conflict instead of more deadly and escalatory means.

Regime type may also correlate with cyber capabilities. Countries that are democratic are more stable which may aid the development of cyber capability. Also, democratic states may be more responsive to public demands for increased cyber security and build-up greater capabilities accordingly. Indeed, Buchanan (2016, 118) observes that democracies such as the United States and its five-eyes partners have some of the most advanced cyber capabilities in the world. Democracy may therefore have a confounding influence in the regression model, explaining any observed relationship between capabilities and conflict.

To measure joint democracy, I first obtain the polity scores for each state which range from -10 (most autocratic) to 10 (most democratic). Using the same methodology as Bremer (1992), I consider a state to be democratic if its polity score is greater than or equal to 5 and then code a dyad as being jointly democratic if both states meet this threshold, not jointly democratic if otherwise. In chapter 10, where I am interested in the initiator's characteristics, I control for the democracy of the initiator. This is measured by the polity score of the potential initiator.

I also control for *major power* to gauge status-based arguments. Countries that are major powers are status-seekers and tend to take on a more active role in international politics. Their willingness to take on a prominent international presence may bring them into conflict with other states and might explain the empirical finding that major powers are more likely to be involved in war (Bremer 1980; Bremer 1992, 328). The same type of states may also be more engaged in cyber conflict, as they seek to expand influence in the cyber as well as physical domains.

Major powers should also be more likely to build-up cyber capabilities for similar purposes of prestige and the notion that a major player in international politics must invest in a full portfolio of capabilities across different types of technology in order to preserve its status as a powerful state (Jo and Gartzke 2007, 171). Theories of status-seeking aside, power status may be linked to a greater involvement in cyber conflict and greater tendency to build-up cyber capabilities simply because by definition major powers possess greater resources and capabilities than other states to do so.

In chapter 9, using the Correlates of War definition of major powers (which for this period comprise of the United States, United Kingdom, Russia, France, Germany, Japan, and China), I create a dichotomous variable taking the value of 1 if both members of the dyad are a major power and 0 if otherwise. In chapter 10, I control for the major power status of the potential initiator.

Finally, in time series-cross sectional data, it is important to control for temporal dependence. Logit models assume that events are independent from one another. This is unlikely here because cyber conflict between two states in one year should be influenced by their conflict in previous years. Beck, Katz and Tucker (1998) recommend that when modelling conflict, the researcher should add variables to count the number of years the dyad has remained at peace alongside their squared and cubed versions. It is based on the logic that the longer a dyad remains at peace the less likely they will engage in conflict. In the regressions in chapters nine and ten, I include a peace years variable counting the number of years each dyad has been at peace (and its squared and cubed variants).

Part 4: Illustrative case study of Iran

In the final analytical chapter of this dissertation I adopt a qualitative case study approach to compliment the quantitative analysis and provide a richer causal explanation (George and Bennet 2005). Quantitative analysis can identify the causal effects of variables on cyber activity, but it cannot highlight the causal mechanisms involved in the process. Causal effects describe how variable B changes in response to changes in variable A, while the causal mechanism refers to the process or pathway by which variable A causes outcome B. George and Bennet (2005, 137) define causal mechanisms as “unobservable physical, social, or psychological processes through which agents with causal capacities operate, but only in specific contexts or conditions, to transfer energy, information, or matter to other entities.” The advantage that qualitative methods have over quantitative methods is that they can identify the causal mechanisms linking causal factors with an outcome. My central purpose in this analysis is therefore to explain *how* opportunity and willingness factors are translated into cyber capability and then how capabilities translate into cyber conflict.

My case study is of the country of Iran and can be classified as an “illustrative case study” (Levy 2008, 6). The goal is not to perform a test of the hypotheses set out in chapter 3 since the statistical analyses already performs that function. Rather, an illustrative case study aims to:

“Give the reader a ‘feel’ for a theoretical argument by providing a concrete example of its application, or to demonstrate the empirical relevance of a theoretical proposition by identifying at least one relevant case.” (Levy 2008, 6-7).

My purpose is to use Iran to give a reader a feel for my theoretical argument that latent skill and knowledge combined with interstate rivalry and threat environment promotes cyber activity. Iran is a specific example of a set of probabilistic patterns which my analysis has uncovered in a much larger set of cases in that it possesses relatively high levels of latent capability, has faced an intense threat environment, has developed active cyber capability, and has engaged in cyber conflict. As a recent think tank report argues: “it is clear Iran has invested in indigenous cyber capabilities for both

defensive and offensive purposes and is willing to use them in the event of conflict” (Anderson and Sadjadpour 2018, 5). It therefore provides a helpful illustrative example of the processes explored in this thesis. Some readers might object that Iran could be an outlying data point in cyberspace and therefore cannot be used to draw general conclusions about cyber capabilities and conflict. This is true and is also not the aim of the case study. While generalisable findings are drawn from the statistical models (because they use data on a large sample of countries), the purpose of the case study is only to give readers more context, detail, and description to the findings suggested by the data analysis and to show how the theory can be applied to help explain an individual country’s cyber policy development.

While selecting on the dependent variable is discouraged in quantitative analysis because it creates selection bias, it is an acceptable method in case study research because it can help establish the causal pathways leading from the explanatory variables to the outcome (George and Bennet 2005, 23). Selecting a country that has not engaged in cyber activity will obviously not help in illuminating how the process works because the outcomes of interest never occurred.

The within-case method I use is the process tracing method. Process tracing “attempts to identify the intervening causal process – the causal chain and mechanisms – between an independent variable and the outcome of the dependent variable” (George and Bennet 2005, 206). I identify the steps and uncover the causal mechanism by which the rivalry process is translated into capabilities and then how capabilities and rivalry are translated into conflict. This also allows the theory to be further developed by uncovering new variables of interest or causal mechanisms that were not previously identified. Under the umbrella of rivalry there can be specific events that serve as more proximate causes that statistical analysis could not uncover. I can also identify types of capabilities that were developed that the data set does not incorporate.

Summary

This chapter has provided an overview of the methods employed, but detail of more specific steps will be clarified during the relevant analyses as they are more easily understood when discussed in context. With the analytical methods set out, the upcoming chapters should provide a robust account for how, why, and to what effect capabilities have proliferated.

Chapter VI

A Descriptive Analysis of Cyber Capability in the International System

Introduction

In this chapter I describe the NCC dataset to give the reader a feel for the data and to demonstrate the spatial and temporal patterns of proliferation in national capabilities. I provide a descriptive analysis of the NCC dataset variables to highlight the distribution of capabilities across the international system and the scale of proliferation using various visualisation and summation methods. This analysis is key to developing the Opportunity-Willingness theory because it demonstrates the latent capabilities available to states which gives them the opportunity to establish active capabilities. Furthermore, it demonstrates the acquisition of active capabilities which gives states the opportunity to engage in computer network operations.

This analysis will also shed light on how cyber capability compares with other measures of cyber power and conventional power. Scholarly opinion has ranged from arguments that traditionally weaker countries like North Korea or Iran are at an advantage in cyberspace (Singer and Friedman 2014, 151) to counterarguments that cyber capabilities only reinforce the power of the major powers like the United States (Lindsay 2013, 385). So far, these arguments have not been supported by extensive quantitative research. This analysis can now help to bring empirical evidence to the debate and highlight the foundations of national cyber power.

My assessment begins with a description of the latent cyber capability indicators. Then I provide the full ranking of countries based on programming skill and computer science knowledge, which I consider to be the crucial resource of cyber capability and compare this with pre-existing indices of cyber capacity and material capabilities. Next, I describe the indicators of active cyber capability and strategy, before concluding the chapter.

Latent cyber capabilities: where do countries stand?

Latent capabilities are defined as the societal based resources or assets that the state can draw on for strategic advantage in cyberspace and are assessed across four areas: 1. programming skill, 2. computer science knowledge, 3. software industry, and 4. secure Internet infrastructure. Unlike the active capability indicators, the latent capability indicators are continuous which means countries can be ranked by how much of a resource they possess. To describe this data, the top ten countries in

each indicator are compared cross-sectionally and the top three are compared across time. Data are described in absolute terms, relative terms, and by their change in capability.

Computer programming skill

Which countries possess the most technical skill that the state could translate into cyber operations? My indicator of skill is a country's performance in the International Olympiad in Informatics, supplemented with data from the International Mathematics Olympiad. These data sources provide information on participation rates which allows this factor to be controlled for. For instance, a country might have low numbers of medals not because of poor skill but because of a lack of participation. By using the ratio of gold medals won at these competitions to the number of times the country has participated, a standardised assessment of relative skill can be ascertained.²¹ Table 4 shows the top ten countries ranked by technical skill according to their combined performance in these two high school Olympiads.

Table 4.
National performances at the IOI and IMO by country (2016)

<i>Country</i>	<i>Olympiad skill (gold medals/participations)</i>	<i>IMO participations</i>	<i>IMO gold medals (cumulative total)</i>	<i>IOI participations</i>	<i>IOI gold medals (cumulative total)</i>
China	4.18	31	159.5	29	90
Russia	3.85	25	118	25	74.5
US	3.43	42	177.25	25	65.75
S Korea	2.98	29	104.25	25	59
N Korea	2.90	13	37.75	0	-
Taiwan	2.65	25	83.25	23	45.5
Iran	2.64	31	95	23	51
Japan	2.54	27	84.25	14	29.5
Romania	2.53	57	168.5	27	57
Vietnam	2.28	40	122.75	28	42

East Asian countries are particularly prominent under this metric. China has demonstrated the most skill with an average ratio of 4.18 gold medals per participation compared with the United States' 3.43. Russia also performs better than the United States with a skill value of 3.85. The results suggest the United States may not possess the most programming and mathematics skill, whereas

²¹ Specifically, the technical skill variable is calculated by averaging the ratio of IMO gold medals to participations with the ratio of total IOI gold medals to participations. When counting gold medals, bronze and silver medals are also incorporated into the measure by giving bronze medals a value of 0.25 gold medals and silver medals a value of 0.5 of gold medals.

traditionally weaker countries may be able to invest in this area as a way to compete with stronger states. Interestingly, the top ten list includes North Korea and Iran who are considered to be very active offensively in cyberspace despite their relative weakness conventionally and their skill might provide a partial explanation for this. While North Korea has never participated in the IOI, its performance in the Mathematics Olympiad has been relatively strong.

Figure 2 shows how Olympiad-based skill has changed over time for the top three countries. Instead of the medals to participation ratio, however, the line graph uses an alternative measure which is the 3-year moving average of gold medals won. This is better for showing short term trends in performance over time. It shows that the three countries are neck and neck in terms of performance, obtaining on average between 3 to 5 gold medals every year. While it is close, China has performed slightly better across time.

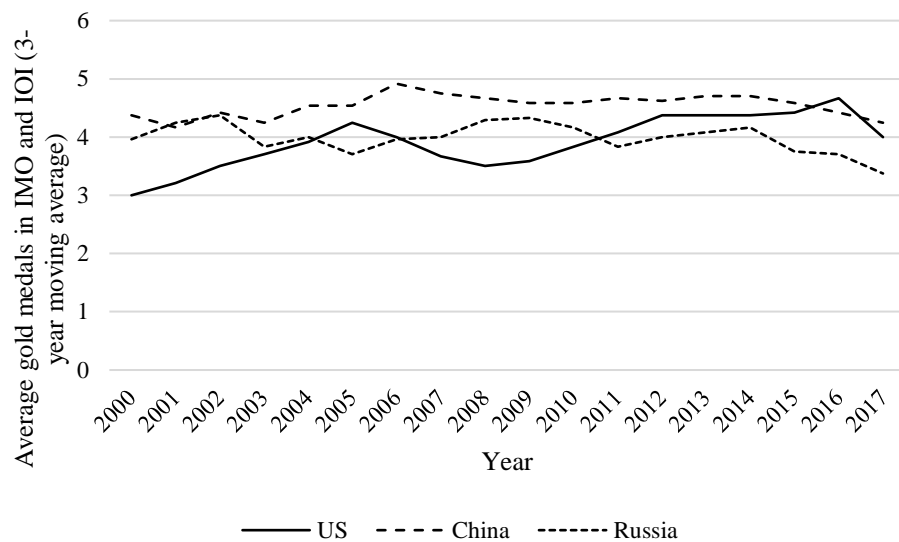


Figure 2. IOI and IMO programming skill among top three (2000-2017)

Computer science knowledge

While the previous two indicators gauge applied technical skill, cyber-related knowledge from a more theoretical, academic level is assessed through a country’s publication output in computer science. This data reflects an ability to produce research that can be applied to cybersecurity including innovations in software and hardware which can be applied in cyberspace operations. Figure 5 ranks the top ten countries in terms of the total number of computer science articles published by that country in 2016.

Table 5
Computer science publication output by country (2016)

<i>Country</i>	<i>Articles</i>	<i>Articles (per million people)</i>	<i>Citations per article</i>
China	75,396	54.69	1.49
United States	60,068	185.74	1.92
India	27,938	21.10	0.89
Germany	19,654	238.67	1.61
United Kingdom	18,140	276.54	2.07
Japan	15,678	123.45	0.95
France	14,699	219.85	1.50
Italy	12,851	211.97	1.89
Canada	11,045	304.57	1.94
South Korea	10,373	202.42	1.31

Knowledge production in computer science is clearly skewed towards the major economic powers in international politics. While the United States comes second to China in absolute terms, China produces far less articles when accounting for population with only 54.69 articles per million people compared with the United States' 185.74. Canada produces the most articles relative to its population in this list, while the United Kingdom achieves the highest citations per article reflecting its quality not just quantity of computer science research output.

The across-time dimension of the data is depicted in figure 3 which highlights the rapid rise in China's research output relative to its nearest competitors – the United States and India. China begins with a relatively low output in the year 2000 but overtakes the United States around 2008 to become a leader as it begins to challenge the United States' technological superiority in world politics (Brooks and Wohlforth 2016, 28).

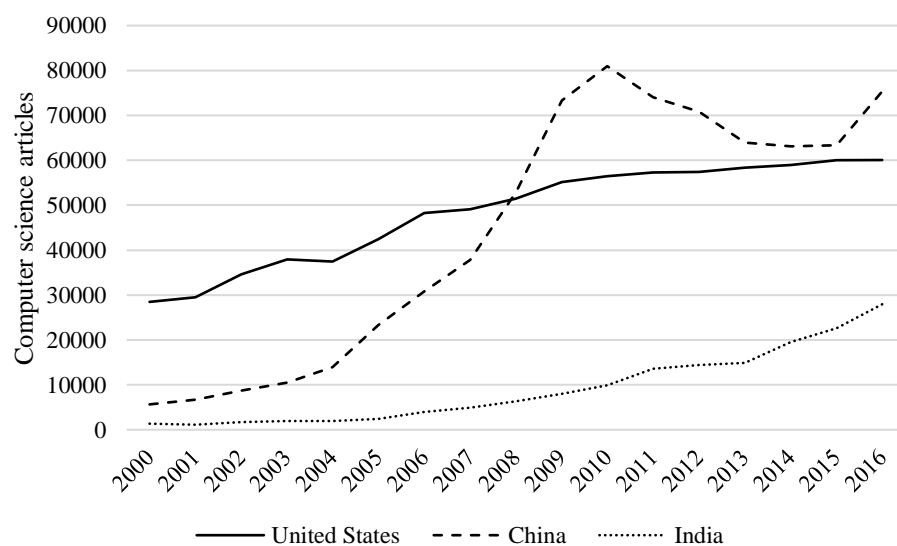


Figure 3. Computer science publications among top three (2000-2016)

Industrial capacity

The third indicator of latent cyber capabilities is industrial capacity. The data here can help highlight which countries have the largest IT industry which may indicate their ability to produce domestically the technology required for engaging in cyber operations. The size of industry is first measured by the number of software companies incorporated in a country. The top ten countries under this metric are ranked in Table 6.

Table 6.
Software companies by country (2016)

<i>Country</i>	<i>Software companies</i>	<i>Percentage share among top 10 (%)</i>	<i>Software companies (per million people)</i>
US	23,473	61.74	72.58
UK	4,243	11.16	64.68
France	2,255	5.93	33.73
Germany	1,710	4.50	20.77
China	1,459	3.84	1.06
India	1,412	3.71	1.07
Canada	1,207	3.17	33.28
Australia	1,082	2.85	44.69
Sweden	613	1.61	61.78
Netherlands	568	1.49	33.35

The data shows how the United States far surpasses other states with over 23,000 software companies and a 61.74% share of the companies incorporated in the country amongst the top ten countries. Countries with large economies are prominent here, which is understandable given that industrial output clearly feeds into GDP. The economically underdeveloped countries here, China and India, have notably smaller software industries when taking population into account with only 1.06 and 1.07 companies per million people, respectively. Overall, this list reflects the dominance of western countries in the software industry.

The change over time in software companies amongst the top three in this list are plotted in figure 4 which further shows the continued dominance of the United States in this area which is unlikely to be challenged in the foreseeable future.

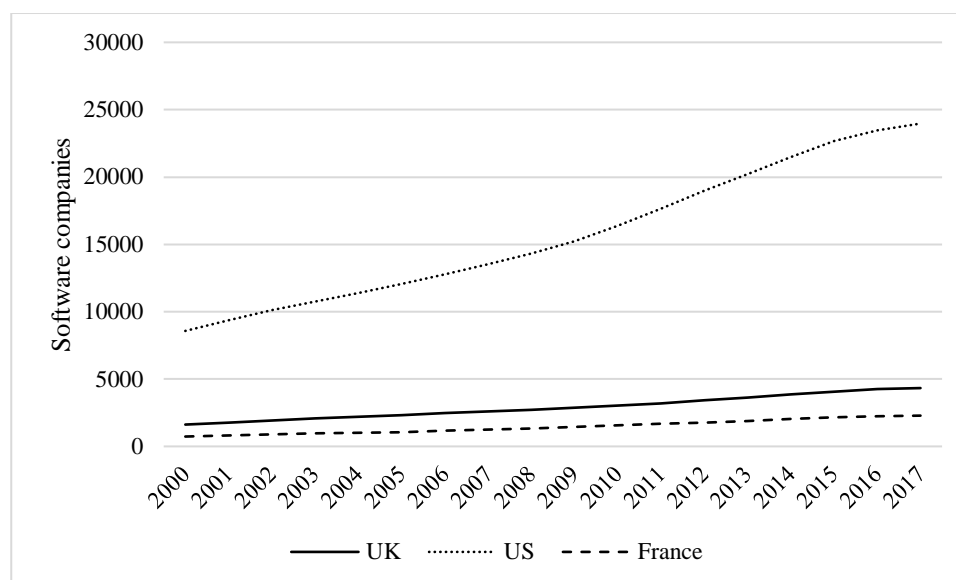


Figure 4. Number of software companies among top three (2000-2017)

This indicator does not quantify the industrial output of the companies, only the presence of firms. To measure output, table 7 is the ranking of countries by Information Communication Technology (ICT) service exports. The values do not necessarily correspond to the number of software companies, as this indicator is gauging a broader industrial classification.

Table 7.
ICT service exports by country (2016)²²

Country	ICT service exports (billion US dollars) ²³	ICT service exports (% of total service exports)	ICT service exports (% of GDP)
India	76.54	47.30	3.37
United States	38.55	5.08	0.21
Germany	33.99	11.90	0.98
United Kingdom	26.35	7.57	1.01
China	25.43	12.20	0.23
France	17.34	6.67	0.70
Israel	17.02	43.20	5.36
Netherlands	15.56	9.87	2.00
Switzerland	14.09	11.85	2.11
Sweden	14.02	19.27	2.73

Nevertheless, the top ten in both industry indicators share eight of the same countries. India evidently has a very large ICT service sector worth 76.54 billion US dollars in 2016 which made up 47.3% of

²² Taiwan data missing.

²³ Measured in current US dollars.

its total service exports and 3.37% of its GDP. The United States comes second in this indicator with a much smaller value of exports of 38.55 billion. Among the smaller countries in this top ten, Israel for the first time appears on the top ten with 17.02 billion worth of ICT service exports which make up 43.2% of total service exports and 5.36 of its GDP. Israel’s presence is notable given its small size, but it is well known for its strong activity in the IT sector and has been known to develop software and malware for cyber operations (Egozi 2019).

Figure 5 demonstrates the huge rise in India’s ICT service exports going from under 10 billion in 2000 to overtaking the US around 2004 and reaching a value of almost 80 billion by 2017.

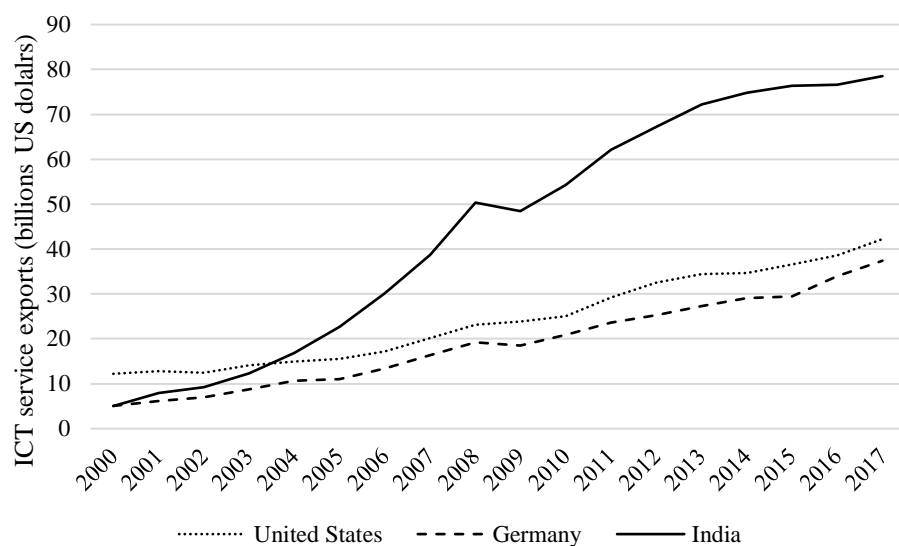


Figure 5. ICT service exports among top 3 (2000-2017)

Internet infrastructure

The final aspect of latent capabilities is Internet infrastructure. The first indicator is Internet penetration used as a proxy for Internet dependence. Internet penetration is the proportion of the population using the Internet defined as “individuals who have used the Internet (from any location) in the last 3 months. The Internet can be used via a computer, mobile phone, personal digital assistant, games machine, digital TV etc” (World Bank n.d.).

Internet penetration is a double-edged sword because while high levels bring economic and social benefits, a lack of Internet penetration means the country is more isolated and thus more protected from cyber intrusions compared with a country that has greater dependence on the Internet. As this research focuses on the factors that give states advantage in computer network operations, the lack of infrastructure in this case is more relevant. Table 8 ranks the top ten countries and the bottom ten countries by their Internet usage as a percentage of population as of 2016.

Table 8.
Internet penetration, top and bottom 10 countries (2016)

Top 10 countries		Bottom 10 countries	
<i>Country</i>	<i>Internet penetration (%)</i>	<i>Country</i>	<i>Internet penetration (%)</i>
Iceland	98.24	North Korea	0.00
Luxembourg	98.14	Eritrea	1.18
Liechtenstein	98.09	Somalia	1.88
Bahrain	98.00	Guinea-Bissau	3.76
Andorra	97.93	Central African Rep.	4.00
Norway	97.30	Niger	4.32
Denmark	96.97	Madagascar	4.71
Monaco	95.21	Chad	5.00
UK	94.78	Burundi	5.17
Qatar	94.29	Congo, Dem. Rep.	6.21

The most connected countries on the left-hand column tend to be small but economically developed, and frequently European. While these countries are the most connected in the world, it is likely that many of their critical systems are reliant on Internet networks which makes them comparatively more vulnerable to cyber-based threats. On the other hand, the least connected countries are shown in the right-hand column and these tend to be very economically underdeveloped societies. North Korea tops the list of lowest Internet penetration as its citizens have little to no access to the World Wide Web. This makes North Korea a difficult target for cyber operations, although the United States is reportedly preparing to overcome these challenges (Ryall and Demetriou 2018).

Although a lack of Internet dependence may provide advantages, the security of the existing infrastructure is also crucially important for cyber defensive capability. And while underdeveloped countries are lacking in Internet dependence, their infrastructure is likely to be insecure and vulnerable. The third indicator for infrastructure is the number of secure servers in a country. These are servers that are secured by encryption technology making the unauthorised access of data and communications more difficult for hackers. Figure 9 ranks the top ten countries by number of secure servers.

Table 9.
Secure Internet servers, top ten countries (2016)

<i>Country</i>	<i>Secure Internet servers</i>	<i>% of secure servers among top 10</i>	<i>Secure Internet servers (per million people)</i>
United States	3,694,357	50.85	11,423.28
Germany	957,300	13.18	11,624.96
United Kingdom	570,586	7.85	8,698.55
France	446,252	6.14	6,674.45
Netherlands	410,955	5.66	24,130.79

Canada	369,091	5.08	10,177.72
Japan	267,900	3.69	2,109.54
Australia	237,318	3.27	9,802.15
Russia	168,007	2.31	1,163.95
Switzerland	143,994	1.98	17,196.73

The results suggest that economically developed countries are some of the most secure, reflecting the need for secure commercial transactions in these countries. Over half of the secure Internet servers are located in the United States, although the Netherlands is the strongest on this list if measured in per capita terms with 24 thousand secure servers per million people. Figure 6 shows how the top three ranked states have increased the security of their websites since 2010.²⁴

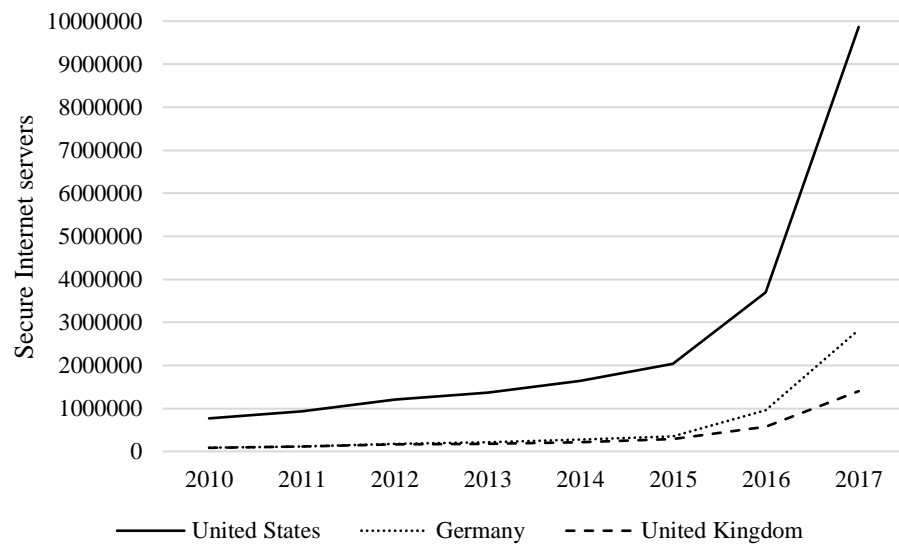


Figure 6. Secure Internet servers, top 10 countries (2010-2017)

Latent cyber capability index

Table 10 presents the country ranking according to the latent cyber capability index constructed from Olympiad performance and computer science knowledge. From this information, we see how countries compare with one another as of the year 2018. Only 126 of the total 194 countries are assessed here because of missing data from the remaining countries that have never performed at either Olympiads. Most of the excluded countries are the least populous countries on earth which are not expected to have substantial cyber capability anyway. No quantitative measure is perfect, and this assessment should only be seen as an approximation of each country's potential to carry out

²⁴ This data only exists since 2010

cyber operations based on observed skill and knowledge production, rather than a definitive evaluation.

The index is based on skill and knowledge as these should be necessary conditions for capability development among all countries, unlike the other indicators like software industry. A certain level of skill and knowledge in computers should be the common factor amongst countries that can project influence in cyberspace. As explained in chapter 5, the index is based on Olympiad performance, total computer science articles, and the computer science articles per million.

The composite index is measured by converting each indicator to a t-score which is a standardisation technique allowing the composite indicators to be directly compared. The final index value is the average of the component t-scores. A t-score of 50 signifies that the country has a capability equal to the mean of all countries in this year. Each increase or decrease of 10 in the t-score reflects an increase or decrease in one standard deviation from the mean.

The results suggest that the United States is the most capable country in cyberspace. It has a t-score of 102.98 which means its capability is more than 5 standard deviations greater than the average country's capability. This supports other academic judgments (Lindsay 2013). China comes second with a capability score of 84.63, demonstrating the gulf that still remains between the two countries. While China is arguably more active in cyber espionage, the United States appears to have greater levels of technological resources. This suggests that frequency by which a country engages in cyber operations is not necessarily the best indicator of its capability.

Singapore's ranking of 5 is a notable achievement for such a small country, showing that countries with small populations can perform well in the cyber domain. It outperforms much larger countries such as Brazil or India under the proxy indicators of per capita computer science articles and programming ability. Singapore would not have achieved such a high rank if computer science articles per capita had not been accounted for, to correct for population size.

With a ranking of 11, Russia is not on the same level as China or the United States. Russia performs only slightly worse than China in the Olympiads and has a similar number of computer science journals per capita. The difference is in the total number of journal articles. China has published more given its much larger population. In some circumstances, therefore, a country with a larger population will outrank a country with a smaller population. Nevertheless, this makes sense given a more populous country like China has a larger talent pool from which to draw expertise than Russia.

Table 10.
Latent cyber capability index country ranking (2018)

<i>Rank</i>	<i>Country</i>	<i>Olympiad skill</i>	<i>Computer science articles</i>	<i>Computer science articles (per million people)</i>	<i>Latent capability index (t-score)</i>
1	United States	3.96	70490	215.46	102.98
2	China	4.33	103120	74.04	84.63
3	UK	2.33	21322	320.68	73.19
4	South Korea	4.00	12212	236.51	70.45
5	Singapore	3.00	4688	831.40	68.47
6	Germany	1.42	22522	271.59	67.00
7	Canada	2.54	12254	330.66	66.75
8	Australia	2.25	10496	419.97	66.34
9	Japan	3.04	16991	134.29	64.37
10	Taiwan	3.04	7289	307.55	64.26
11	Russia	3.71	10727	74.25	63.52
12	North Korea	4.00	9	0.35	62.76
13	Italy	2.00	14114	233.55	62.21
14	France	1.63	15858	236.73	61.68
15	Poland	2.58	6169	162.43	58.82
16	Iran	2.75	6729	82.26	58.41
17	Vietnam	2.83	1847	19.33	57.42
18	Sweden	1.50	4503	442.20	56.41
19	Thailand	2.50	2514	36.21	56.01
20	Ukraine	2.29	2968	66.51	55.32
21	Romania	2.13	2239	114.97	54.71
22	Hungary	2.13	1335	136.66	54.51
23	Bulgaria	2.17	765	108.91	54.44
24	Israel	1.71	2639	297.06	54.17
25	Czech Republic	1.63	2820	265.39	53.68
26	Switzerland	0.67	4480	526.04	53.50
27	Netherlands	0.88	5824	338.00	53.44
28	Indonesia	1.92	5682	21.23	53.37
29	Spain	0.42	11154	238.72	53.15
30	India	1.13	42899	31.72	52.98
31	Kazakhstan	1.88	479	26.21	52.89
32	Serbia	1.79	904	129.47	52.78
33	Belarus	1.83	166	17.50	52.67
34	Peru	1.75	493	15.41	52.29
35	Malaysia	0.67	7398	234.64	51.85
36	Finland	0.46	3389	614.17	51.79
37	Greece	1.00	3455	322.06	51.74
38	Brazil	1.46	7996	38.17	51.73
39	Croatia	1.54	710	173.62	51.63
40	Turkey	1.33	5244	63.70	51.22
41	Philippines	1.46	735	6.89	50.93
42	Georgia	1.46	118	31.63	50.93
43	Portugal	0.42	4201	408.59	50.63
44	Austria	0.46	3791	428.51	50.58
45	Belgium	0.58	3351	293.38	49.45
46	Bangladesh	1.13	1465	9.08	49.40
47	Denmark	0.25	2912	502.29	49.18
48	Mexico	1.00	3043	24.11	48.97
49	Slovakia	0.88	1216	223.24	48.92

50	Armenia	0.96	80	27.10	48.59
51	Argentina	0.92	793	17.82	48.43
52	Norway	0.25	2465	463.84	48.33
53	New Zealand	0.50	1706	349.20	48.03
54	Saudi Arabia	0.54	3785	112.31	47.77
55	Mongolia	0.75	34	10.72	47.62
56	Estonia	0.58	444	336.14	47.23
57	Lithuania	0.58	365	130.85	46.96
58	Ireland	0.17	1914	394.35	46.90
59	Moldova	0.58	58	16.36	46.84
60	Latvia	0.54	334	173.37	46.80
61	Cyprus	0.46	487	409.50	46.79
62	Bosnia and Herzegovina	0.54	235	70.70	46.69
63	Syria	0.54	29	1.72	46.64
64	Tajikistan	0.54	7	0.77	46.64
65	South Africa	0.38	2072	35.86	46.06
66	Tunisia	0.08	2536	219.28	45.99
67	Costa Rica	0.33	133	26.60	45.68
68	Luxembourg	0.04	550	905.01	45.64
69	Slovenia	0.17	662	320.21	45.46
70	Macedonia	0.25	227	108.98	45.35
71	Nicaragua	0.25	22	3.40	45.28
72	Sri Lanka	0.21	535	24.69	45.13
73	Azerbaijan	0.21	86	8.65	45.09
74	Colombia	0.17	1821	36.68	45.07
75	Chile	0.13	1278	68.24	44.93
76	Paraguay	0.17	32	4.60	44.90
77	Kyrgyzstan	0.17	17	2.69	44.90
78	Turkmenistan	0.17	1	0.17	44.90
79	Jordan	0.08	1122	112.70	44.84
80	Morocco	0.08	1997	55.43	44.80
81	Ecuador	0.08	1364	79.84	44.80
82	Montenegro	0.13	103	165.50	44.75
83	Cuba	0.13	209	18.43	44.71
84	UAE	0.00	1460	151.59	44.71
85	Algeria	0.08	1769	41.89	44.70
86	Egypt	0.08	2698	27.41	44.70
87	Venezuela	0.13	135	4.68	44.70
88	Uzbekistan	0.13	27	0.82	44.70
89	Iceland	0.08	155	438.38	44.69
90	Pakistan	0.08	3587	16.90	44.67
91	Uruguay	0.08	157	45.52	44.53
92	Albania	0.08	81	28.26	44.51
93	El Salvador	0.08	41	6.39	44.51
94	Iraq	0.00	1831	47.64	44.35
95	Malta	0.00	146	301.95	44.24
96	Liechtenstein	0.00	36	949.62	44.21
97	Kuwait	0.00	321	77.59	44.19
98	Bahrain	0.00	117	74.55	44.14
99	Brunei	0.00	50	116.56	44.13
100	Nigeria	0.00	884	4.51	44.13
101	Botswana	0.00	49	21.74	44.12
102	Ghana	0.00	165	5.54	44.12
103	Libya	0.00	74	11.08	44.12

104	Panama	0.00	36	8.62	44.12
105	Kenya	0.00	120	2.33	44.12
106	Trinidad and Tobago	0.00	19	13.67	44.12
107	Jamaica	0.00	26	8.86	44.12
108	Myanmar	0.00	106	1.97	44.12
109	Uganda	0.00	77	1.80	44.12
110	Nepal	0.00	55	1.96	44.12
111	Tanzania	0.00	63	1.12	44.12
112	Zimbabwe	0.00	32	2.22	44.12
113	Guatemala	0.00	26	1.51	44.12
114	Cambodia	0.00	24	1.48	44.12
115	Burkina Faso	0.00	23	1.16	44.12
116	Honduras	0.00	15	1.56	44.12
117	Ivory Coast	0.00	25	1.00	44.12
118	Bolivia	0.00	15	1.32	44.12
119	Gabon	0.00	6	2.83	44.12
120	Mauritania	0.00	8	1.82	44.12
121	Madagascar	0.00	15	0.57	44.12
122	Dominican Republic	0.00	10	0.94	44.12
123	Benin	0.00	11	0.96	44.12
124	Mozambique	0.00	13	0.44	44.12
125	Laos	0.00	3	0.42	44.12
126	Gambia	0.00	2	0.88	44.12

Most of the major economic and military powers in international relations feature highly in the cyber capability ranking. Countries including China, UK, Japan, France, Italy, Russia, and Germany all reach the top 20 in latent capability. This suggests that in general latent cyber capability favours traditionally more powerful states. These countries' large economic resources may allow them to invest more in education and develop skills and knowledge in areas relevant for cybersecurity. Moreover, major powers likely have an added incentive to compete internationally in this field because they are by definition prestige seekers, which could help to explain the predominance of major powers in the top of the cyber capability ranking.

That being said, the notion that Internet technology allows some traditionally weaker states to punch above their weight also gains some evidence here. North Korea and Iran are frequently called out as antagonists in national security threat assessments in the West (Coats 2019) and are known to have engaged in many cyber incidents (Valeriano and Maness 2014). This index shows that these countries have relatively strong levels of latent cyber capability despite their economic difficulties, being ranked 12th and 16th respectively. North Korea particularly performs exceptionally well in the mathematics Olympiad highlighting the high level of skill the government is able to cultivate. One promising aspect of this index is that it can quantitatively capture the capability of such a secretive country like North Korea. To the best of my knowledge, no other assessment has been able to do this.

There is, moreover, a notable concentration of capability among east Asian countries. This could reflect the traditionally strong performance of these countries in mathematics and science which has translated effectively to capability in the cyber domain. The latent cyber capability index could therefore be capturing the impact of cultural differences between countries in terms of the emphasis some societies place upon academic performance in scientific disciplines (Leung 1998; Sui Ngan Ng and Rao 2010; Leung 2017).

The distribution of the observations according to latent capability in the year 2018 is highlighted in figure 7. There is a large skew in the data with very few countries appearing at the high end of the cyber capability scale. Most countries in fact have very little evident skill and knowledge. This could be one reason why cyber conflict has been shown to be relatively rare amongst rival states (Valeriano and Maness 2014): many countries may simply lack the capability to conduct successful computer network operations against their rivals. The figure also demonstrates how far ahead the United States is in this domain, despite widespread assumptions that cyber capabilities allow weaker states to overturn traditional balances of power in the international system.

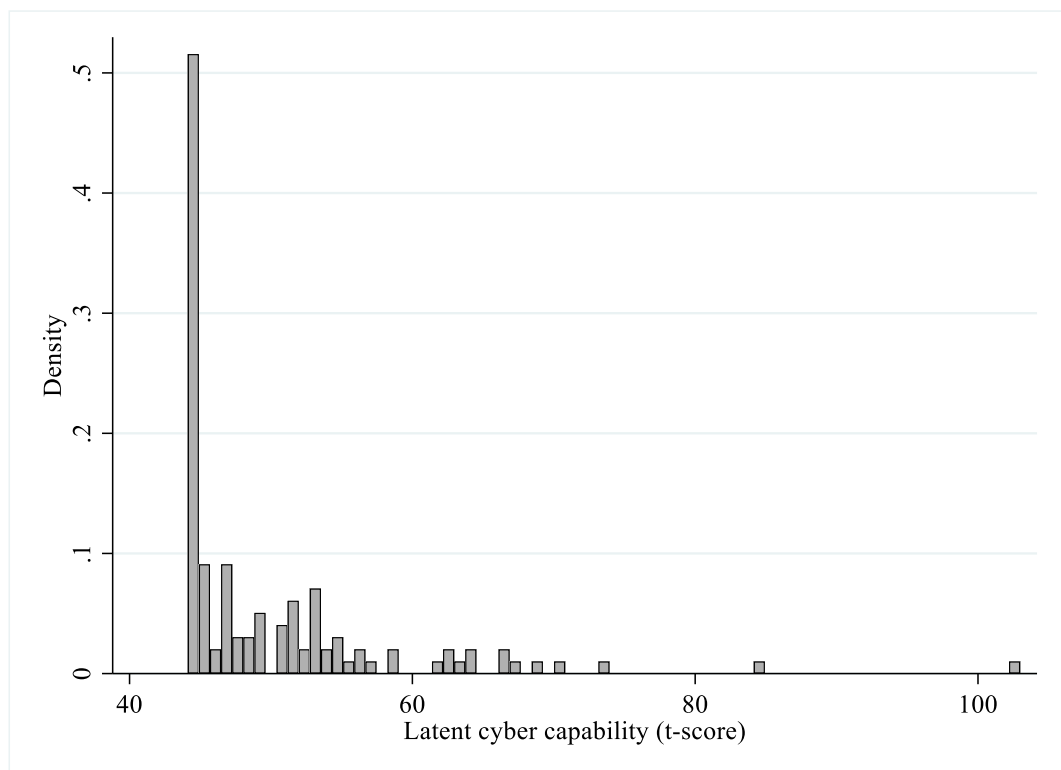


Figure 7. Histogram of latent cyber capability (2018)

With the complete cyber capability ranking of countries established, I can compare it with other established indices of cyber capacity and material capabilities. Table 11 gives the correlations

between these indicators and my latent cyber capability index. A correlation coefficient ranges from -1 to 1 where the closer the value is to 1, the more similar the two measures are.

The first comparison is with the ITU’s Global Cybersecurity Index from 2017 which assesses a country’s commitment to reducing cyber threats by its legal, organisational, technical, capacity-building, and cooperative efforts. The correlation between this and the latent capability index is 0.577 which is a moderately positively relationship but with substantial divergence. Its top 5 countries for instance are Singapore, the United States, Malaysia, Oman, and Estonia which shares only two of the same countries in the top 5 as the latent capability index.

The second index is the National Cyber Security Index which also measures the preparedness of a country to cope with cyber threats based on legislative, organisational, and policy initiatives taken by the state. The correlation between this and latent cyber capability is 0.421, suggesting that my measure has even less in common with this cyber capacity index. Indeed, its top 5 countries are Greece, Czech Republic, Estonia, Spain, and Lithuania, none of which appear near the top ranking of latent cyber capability.

The divergence can be explained by the fact the latent cyber capability index focuses on the concept of scientific and technical knowledge and skill whereas the other cyber capacity indices consider a wide range of enacted policies and established organisations. Moreover, at this stage I am assessing the potential of a state to engage in computer network operations rather than what current policies or organisations have been created. This aspect of cyber capability will be covered in the next section of this chapter. Assessments of cyber capability therefore are very dependent on methodology and what concepts are deemed to be of key importance.

Of all the comparisons made here, latent cyber capability is most strongly associated with the Composite Index of Material Capabilities with a correlation of 0.654. This is a measure of material power based on demographic, industrial, and military resources. This suggests that on the whole a country’s material capability should be a good predictor of a country’s cyber capability. Yet since the correlation is only moderate it suggests that there are many countries that either underperform or overperform in cyberspace given their material resources.

Table 11.
Correlation of latent cyber capability with cyber and material capability indices

<i>Comparison measure</i>	<i>Correlation with latent cyber capability</i>
ITU Global Cybersecurity Index (2017)	0.577
National Cyber Security Index	0.421
Composite Index of Material Capabilities (2012)	0.654

To get an impression of which states under or overperform in cyber capabilities compared to their material capabilities, I subtract each country's ranked position in its CINC score by its ranked position in its latent cyber capability. A positive number means the country is ranked higher in cyber capability than in material capability and a negative number means the country is ranked lower in cyber capability than it is in material capability. I show the results for the twenty most capable countries in cyberspace in figure 8.

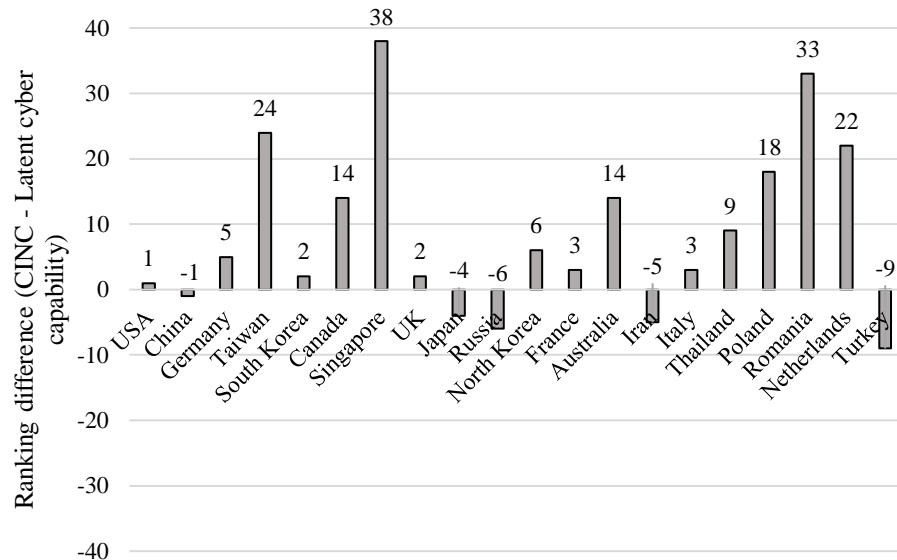


Figure 8. Difference between material and cyber capability among selected states.

The United States and China's position in the cyber domain is predicted well by their material capabilities as measured by total and urban population size, steel and iron production and energy consumption, and military personnel and spending, since their ranking only differs by one between measure. While China is ranked first in material capability and second in cyber, the United States is ranked first in latent cyber capability and second in material.

Among the other countries that underperform based on their material capabilities are Japan, Russia, Iran, and Turkey. Despite their level of material strength, these countries do not have as strong levels of programming and computer science skill and knowledge. Several countries, on the other hand, strongly outperform in terms of what would be expected by traditional power assessments. For instance, Singapore is ranked 38 places higher in cyber capabilities than in material capabilities. These findings demonstrate the importance of accounting for the immaterial resources of skills and knowledge as well as controlling for population size when assessing capability. The CINC measure ignores this component of national capability, despite its potential importance in explaining the ability to project and resist influence in the cyber domain.

This data has provided a novel method for gauging latent cyber capability which evidently differs from pre-existing attempts. Ultimately, a capability ranking will be shaped by subjective methodological choices. Given the theoretical importance of skills to cyber capability I have decided to base latent cyber capability on skills and knowledge. The next section describes how capabilities at the governmental level (active capabilities) have proliferation over time and space, as states have translated their latent potential into military CNO units, national CSIRTs, and national cyber security strategies.

Active cyber capabilities and strategies: temporal and spatial proliferation

Active cyber capabilities are the government-based resources or assets that the state can use more directly for strategic advantage and are assessed by three dichotomous indicators: 1. The presence of a national Computer Security Incident Response Team (CSIRT), 2. a military Computer Network Operations (CNO) unit, and 3. a national cyber security strategy (NCSS). The proliferation of these assets shows the growing activity of states in cyberspace as they have translated their latent resources into operational organisations and policies to pursue their strategic interests. This section describes the spread of active cyber capabilities and strategies by indicating how they have increased in number over time and how they are distributed geographically. As an added indicator of organisational capability (Horowitz 2010, 27), I show how countries rank in terms of the number of years they have held each type of capability.

National Computer Security Incident Response Team (CSIRT)

The first indicator is the presence of a national CSIRT²⁵ which provides the state with increased defence, resilience, and organised response against cyber incidents affecting national assets. Figure 10 records the proliferation since 2000 of these entities.

²⁵ CSIRTs are alternatively called CERTs or CIRTs. I use the term CSIRT for consistency.

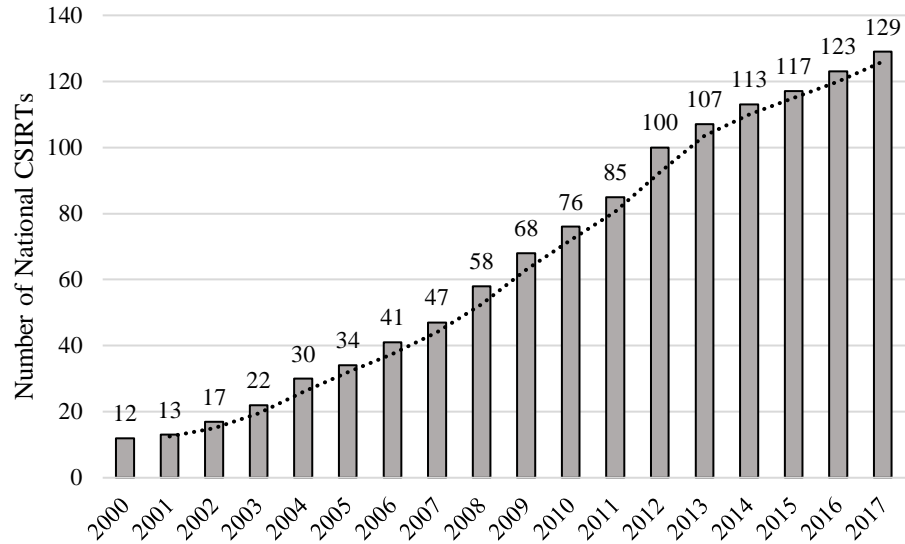
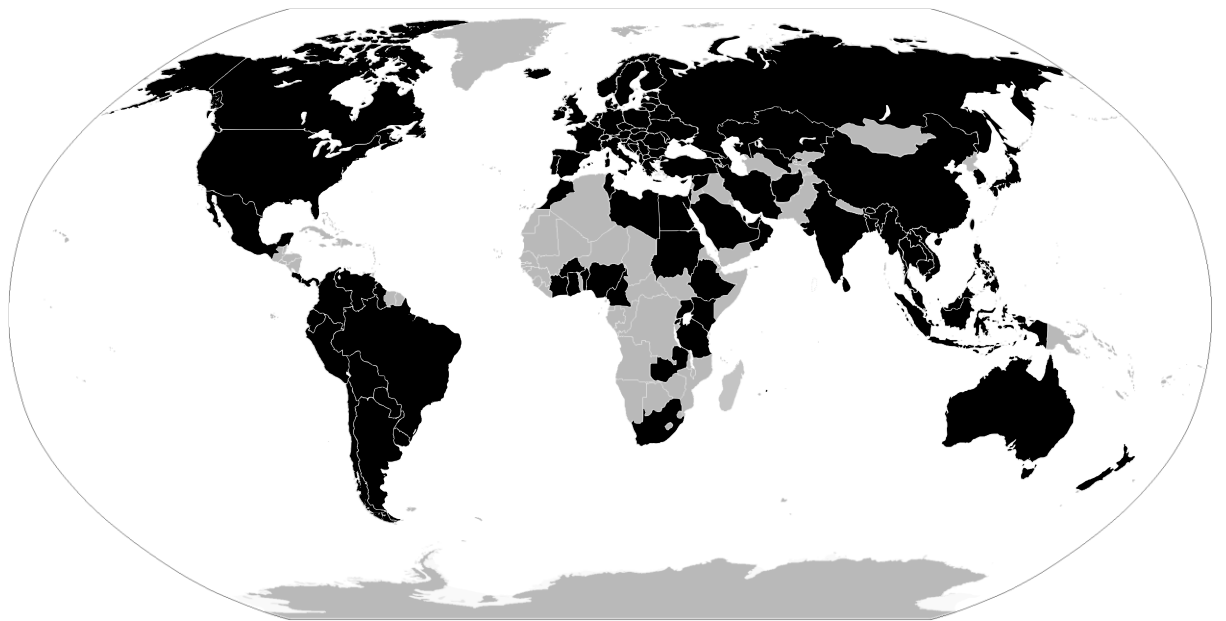


Figure 9. Temporal proliferation of national CSIRTs (2000-2017)²⁶

The acquisition of national CSIRTs has been rapid. In the year 2000 there were only 12 national CSIRTs, but their number has since grown. The largest increase coming in 2012 when 15 new CSIRTs were established. Afterwards the rate of increase levelled off and as of 2017 there were a total of 129 of these teams – more than a ten-fold increase since 2000. States have evidently seen the creation of national CSIRTs as an urgent policy in the digital age. Figure 11 illustrates how CSIRTs are distributed across the globe.



²⁶ Two period moving average trendline added has been included in the bar chart.

Figure 10. Spatial proliferation of national CSIRTs (2017)

Countries can also be compared by the length of time they have had a national CSIRT. This provides an indication of capability from the perspective of organisational and policy maturity. Countries with longer established capabilities have had more time to develop the best operating practices than a country whose capabilities are in the initial stages of development. Table 12 ranks the top ten countries by the number of years they have had a national CSIRT. The top three countries are Slovenia, Japan, and Poland which have had a national CSIRT for 20 years as of 2016. What is notable about this list is the predominance of East Asian countries – six of the top ten countries are East Asian.

Table 12.
Organisational age of national CSIRTs (2017)

<i>Country</i>	<i>Abbreviated name of team</i>	<i>Years active</i>
Slovenia	SI CERT	24
Japan	JPCERT/CC	22
Poland	CERT Polska	22
Brazil	CERT.Br	21
Malaysia	MyCERT	21
Singapore	SingCERT	21
Russia	RU-CERT	20
Taiwan	TWCERT/CC	20
Argentina	ArCERT	19
France	CERT-Fr	19

Military Computer Network Operations (CNO) Units

The second indicator of active cyber capability is the presence of a military CNO unit which provides a country's military with a capability to operate through cyberspace both defensively and often offensively. Figure 12 demonstrates the across-time increase in CNO units.

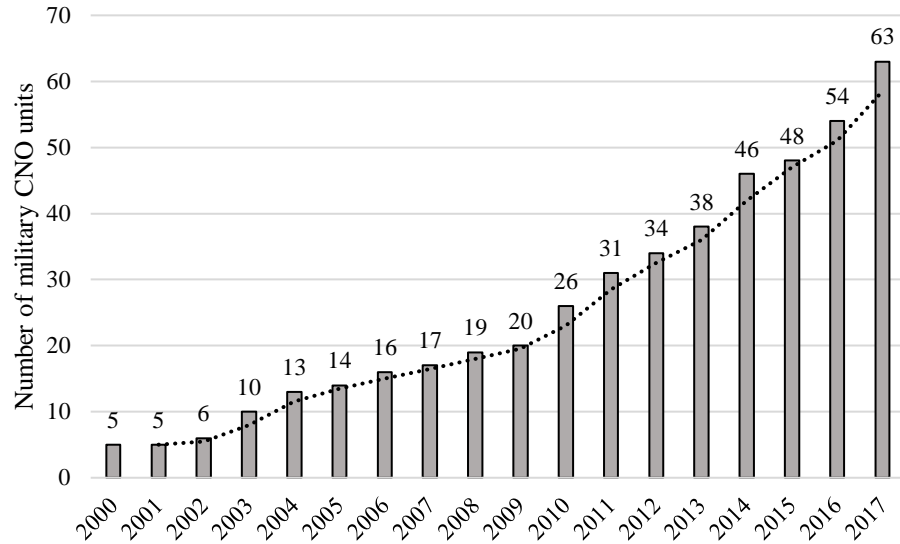


Figure 11. Temporal proliferation of military CNO units (2000-2017)

Like national CIRTs, military units have also been adopted at a rapid rate. In 2000 there were just 5 yet this has grown to 63 by 2017 – 12.6 times as high as in 2000. The rate of increase was steady until 2010 when the rate of adoption shifted upwards, perhaps a response to the Stuxnet incident. Nevertheless, these numbers are significantly smaller than the total number of CSIRTs in the international system which may suggest there are higher costs to establishing military units or that many states have lacked the motivation to integrate cyber security into their military organisations. Yet, given the continued increase seen here, proliferation is likely to continue into the future as cyber becomes an increasingly prominent aspect of national security and military posture.

Figure 13 highlights (in black) the countries that possess military CNO units as of 2017 to show the global distribution of these capabilities. From this overview it is clear that the adoption of military capabilities is much less common in underdeveloped areas in Africa, Central America, Eastern Europe, or central Asia, whereas the major economic powers have all established this kind of capacity.

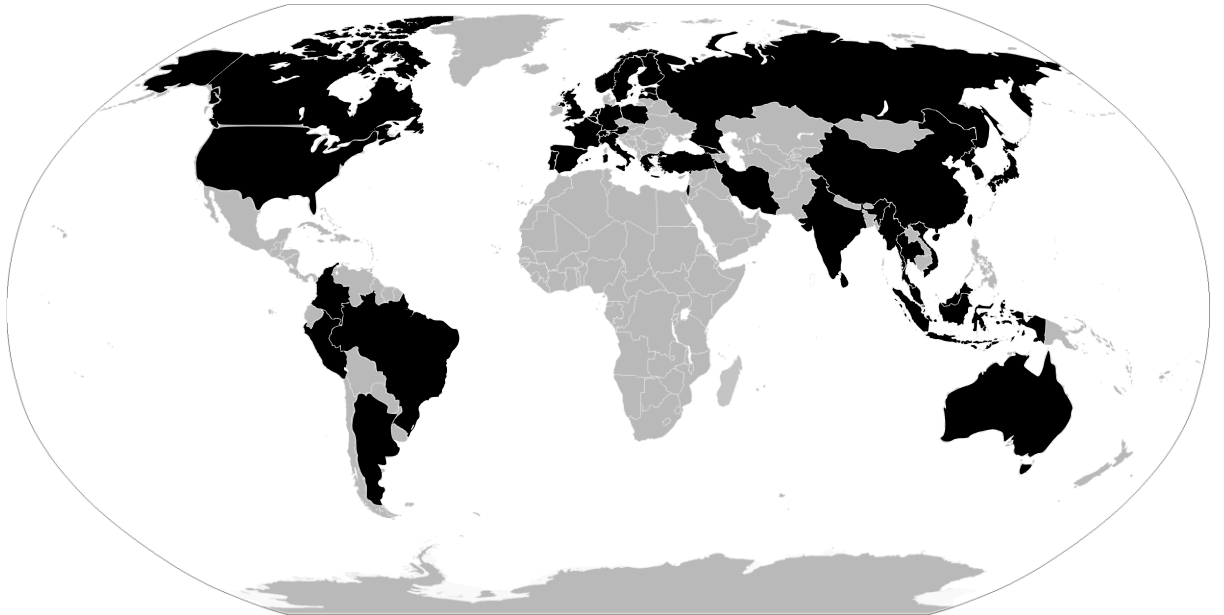


Figure 12. Spatial proliferation of military CNO units (2017)

Table 13 provides an indication of which states have had the longest established military cyber organisations. This list contains many of most commonly cited states in the cyber warfare discourse. China, North Korea, and the United States come out on top as they have had the longest established CNO units dating back to the 1990s.

Table 13.
Organisational age of military CNO units (2017)

<i>Country</i>	<i>Name of team</i>	<i>Years active</i>
China	“100-member elite corps”	21
North Korea	Bureau 121	20
United States	Joint Task Force: Computer Network Defence	20
Russia	Information Security Centre	16
Australia	Defence Network Operations Centre	15
India	Defence Information Warfare Agency	15
Israel	Computer Services Directorate	15
Canada	Canadian Forces Network Operations Centre	14
Myanmar	Defence Services Computer Directorate	14
France	Centre of Analysis in Defensive Computer Control	12

National Cyber Security Strategy

The last indicator is the presence of a national cyber security strategy (NCSS), which is perhaps better described as a policy rather than an active capability as it is not directly engaged in CNO. Nonetheless, I include it as it shows the growth of efforts to secure cyberspace and should reflect a greater level of preparedness by of governments to deal with cyber threats and plan responses.

Figure 14 shows the total number of national cyber security strategy documents published in each year from 2000 to 2017. Unlike national CSIRTs and CNO units, which have grown in a more linear fashion, there has been a more rapid increase in the publication of these documents since 2000. Since the first strategy was published (Russia’s Information Security Doctrine) in the year 2000, the number has risen to 131 strategies of 2017. The rate of increase suddenly jumps after 2010, again possibly in response to Stuxnet which raised concerns worldwide about vulnerability of critical infrastructure to cyber-attacks by malicious foreign actors and could have motivated cyber security policy.

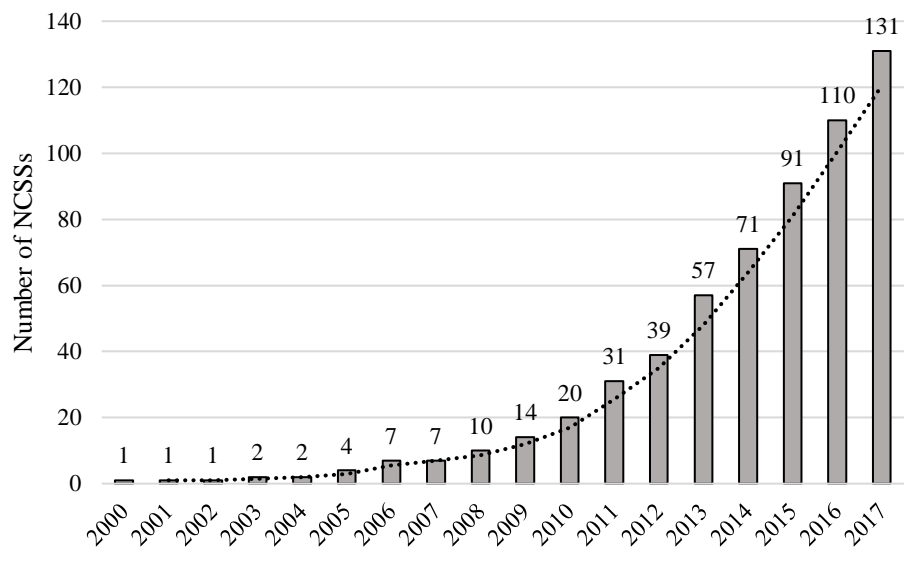


Figure 13. Temporal proliferation of National Cyber Security Strategies (2000-2017)

Figure 15 demonstrates the countries that possess a national cyber security strategy in 2017. It suggests that strategies have spread quite widely across the globe but are particularly focused in large economies and less so in underdeveloped areas of the world.

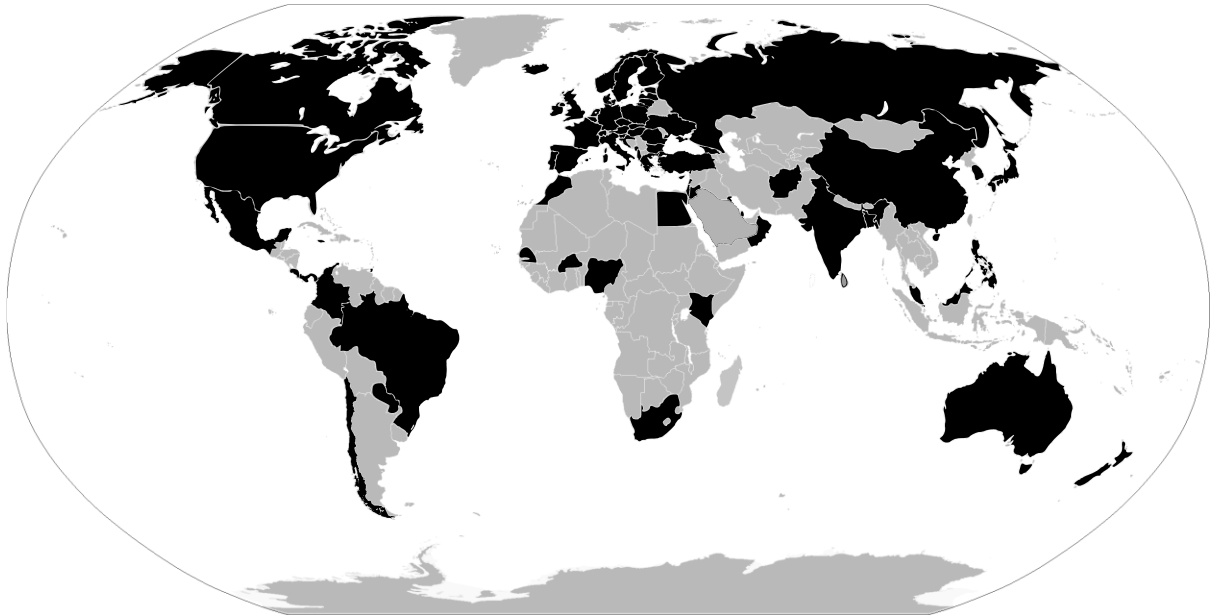


Figure 14. Spatial proliferation of National Cyber Security Strategies (2017)

Finally, Table 14 ranks countries by the length of time they have had a national cyber strategy. Russia was the first to publish a cyber security strategy suggesting cyber (or more accurately, information) security has been an important aspect of its strategic planning for a long time. The United States is second on this indicator with its first national cyber strategy published in 2003. East Asian countries also feature prominently here as well as traditionally advanced countries in areas of intelligence such as the United Kingdom, the USA, and Australia.

Table 14.
Organisational age of national cyber security strategies (2017)

<i>Country</i>	<i>Name of document</i>	<i>Years active</i>
Russia	Information Security Doctrine of the Russian Federation	17
United States	National Strategy to Secure Cyberspace	14
Singapore	Info-comm Security Masterplan	12
Philippines	National Cyber Security Plan	12
Malaysia	National Cyber Security Policy	11
Sweden	Strategy to Improve Internet Security in Sweden	11
Japan	National Strategy on Information Security	11
Estonia	Cyber Security Strategy	9
Australia	Australia's Cyber Security Strategy	8
United Kingdom	Cyber Security Strategy of the United Kingdom	8

These figures provide an extensive picture of the rate and extent of cyber capability proliferation in the international system. Clearly, the scale of cyber capability adoption has been significant. The key

questions that arise are therefore: what drives the process of active cyber capability adoption, and what are its consequences for conflict in the cyber domain?

Discussion

This chapter has described the distribution and proliferation of cyber capabilities globally. It has shown the types of latent resources available to each state, measured across areas of skill, knowledge, industry, and infrastructure, and shown which states have acquired military operations units, national CSIRTs and strategies, and indicated how these have increased over time.

Overall, cyber capability appears to be a weapon of the traditionally more powerful state rather than the weak state. Most states that are at the top of the latent cyber capability ranking are the major world powers. The spread of active capabilities appears to be similarly concentrated among economically powerful or developed states. However, some smaller or economically underdeveloped states have shown surprisingly strong capability in both components.

As vulnerability and awareness of digital threats have grown, most countries have clearly invested in developing cyber capabilities and strategies. In every area of active cyber capabilities, we have seen a rapid proliferation of capacities. The key takeaway is the undeniable fact that cyber capabilities and policies are being adopted at a rapid scale, a process which only began in earnest over the past two decades.

In line with Opportunity-Willingness theory, the capabilities explored here should give states increased ability to operate in cyberspace. In the next chapter, I explain the adoption of active cyber capabilities based on the opportunity derived from latent cyber capability and the willingness based on external threat environment, in accordance with the theoretical framework established in chapter 3.

Chapter VII: The Determinants of Cyber Capability

Introduction

The previous chapter described the patterns of cyber capability proliferation. This chapter moves on from a descriptive assessment to a statistical analysis of why states have acquired cyber capabilities, structured according to the theoretical framework of Opportunity-Willingness established in chapter 3. Simply put, a state is more likely to adopt a capability if it has the opportunity and the willingness to do so. Opportunity-based arguments are assessed through the state's latent resources that provide it with the internal capacity to adopt capabilities. Willingness-based arguments on the other hand are assessed through the state's external threat and rivalry environment.

To identify the determinants of cyber capability adoption, I assess the statistical relationships between these opportunity and willingness-based factors on one hand and the creation of active cyber capabilities by the state on the other. In this analysis, active cyber capabilities are indicated by the presence or absence of a national CSIRT and a military CNO unit. They are most closely related to the engagement in defensive or offensive cyber operations than a national cyber security strategy.

This chapter first revisits the hypotheses set out in chapter 3 for the drivers of cyber capability proliferation. The analysis then proceeds by summarising the key variables, and then investigates the bivariate associations between the explanatory and outcome variables. Afterwards, all the variables are combined into a larger multivariate regression model which allows the independent effect of each factor to be assessed while controlling for others. Finally, the empirical findings and their implications are discussed.

Hypotheses for capability adoption

The adoption of active cyber capabilities should be shaped by a country's level of resources and its external threat environment, as these factors give a state the opportunity and willingness to engage in cyber activity. The first hypothesis is from the opportunity perspective. Regardless of its political interests, a state without the opportunity to adopt cyber capabilities will be unable to do so. For a state to have the opportunity to establish active cyber units, it must meet the resource requirements. States with more of a certain type of resource will therefore be more likely to adopt cyber capabilities than states without these resources.

The key type of resource that should help determine the adoption of cyber capabilities is the knowledge and skill available to the state in areas relating to computing and Internet technology.

Expertise of the technical processes involved in developing malware and carrying out computer network operations should be essential for a country to develop its own domestic cyber capabilities, reflected in the creation of national CISRTs and military units. These are not the only sources of capability, but they serve as proxies for a growing capacity to defend against cyber-attacks or engage in offensive operations.

While the S&T variables should have the most predictive capacity, other types of resources may also be important. Higher economic development for instance should correlate with cyber capability. Although the basic infrastructure to carry out computer network operations is cheap, governments require some degree of financial resources to set up national cyber units, to fund the development of technology, and to hire the skilled operators of these organisations. Economic development (as measured by GDP per capita) is also frequently used in IR literature as a proxy for a country's underlying technological sophistication (Singh and Way 2004; Horowitz and Fuhrmann 2017; Tang 2010, 240). Its inclusion into the analysis allows me to test its ability to explain cyber proliferation.

Industrial capacity should also be important. The private sector is a rich source of expertise and technology that governments can draw on to develop cyber capabilities. The software industry is particularly relevant given its involvement in the production of software and malware sold to political actors to engage in computer network operations (Herr and Ellis 2016).

Hypothesis 1: States with greater latent capability, especially programming skill and computer science knowledge, are more likely to adopt active cyber capabilities.

Turning to the hypothesis for willingness, countries facing a more threatening or competitive international environment should be more likely to develop capabilities. Given a country possesses the opportunity to operate through cyberspace, its willingness to develop cyber capabilities should have an impact on the likelihood that proliferation will occur. According to theory, willingness should be determined by the external threat environment, which I have conceptualised in the following ways.

The first willingness-based factor is interstate rivalry which describes a relationship between pairs of states that is marked by mutual animosity and conflict (Colaresi, Rasler and Thompson 2008). Rivalry is a way to gauge whether a country faces strategic competitors or enemies in the international system and therefore whether it has reason to defend against, deter, or compete with this rival by building up capabilities. Given the emerging opportunity for cyber conflict, states may seek not only conventional military capabilities but also cyber capabilities – either in the civilian or military sectors – as a means to counter the activity of their international rivals.

Drawing on balance of power theory, another reason why some states develop their offensive cyber capabilities is that they are seeking a low-cost means to challenge the United States – the unipolar power in international politics (Wohlforth 1999). This explanation should only be relevant for military cyber capabilities since national CSIRTs have no offensive capability and thus do not provide the means to pursue broader strategic objectives other than defence.

The third explanatory factor is the level of threat from cyber incidents that a state has experienced. If cyber capabilities are built in response to insecurity or to deter cyber threats, there should be a relationship between increased cyber-attacks and proliferation since they reveal a state’s vulnerability which should promote it to develop greater capability to deter and respond to future aggression.

The final way threat is conceptualised is by the capabilities of a rival state. According to the security dilemma hypothesis (Jervis 1978) and early arms race models (Richardson 1960), states build-up capabilities out of fear of their rivals’ capabilities. Applied to the cyber domain, countries with more rivals with military cyber capabilities should be more likely to adopt the capabilities themselves. States could create either military units or national CSIRTs, depending on their policy preference. If, on the other hand, more capabilities amongst rivals leads to a reduction in the likelihood of proliferation, this would lend support to the opposing theory of deterrence. A country’s perception of its rival’s superior offensive cyber capability may reduce its willingness to build similar capability.

Hypothesis 2: Countries with a more intense external threat environment are more likely to adopt active cyber capabilities.

Bivariate analysis: latent capability and active capability

The analysis now begins by first examining the summary statistics of the resource-based indicators that could provide the opportunity for capability adoption, and secondly by assessing the bivariate associations between these variables and the presence of military CNO units and national CSIRTs. Table 15 provides the summary of the four independent variables used in the analysis.

Table 15.
Summary statistics for opportunity-based variables

<i>Independent Variable</i>	<i>Obs.</i>	<i>Missing</i>	<i>Min.</i>	<i>Max.</i>	<i>Mean</i>	<i>Std. Dev.</i>
GDP per capita (US \$)	3,329	152	193.87	144,246.40	12,722.07	18,529.31
Programming skill	2,268	1,213	0	4.182	0.64	0.87

Computer science knowledge	3,481	0	0	79,507	1,445.43	5,995.25
Software Companies	3,481	0	0	23,971	154.31	1,213.35

As explained in the research design of chapter 5, economic development is measured by Gross Domestic Product (GDP) per capita in constant 2010 US dollars. Programming skill is the country's medals won to participation ratio in international maths and programming Olympiads. Computer science knowledge is measured by the total number of journal articles published in this field. Industrial capacity is indicated by the number of software companies incorporated in the country.

The minimum GDP per capita among countries in the dataset is \$193.87, the maximum is \$144,246.40, and the mean is \$12,722.07. The minimum Olympiad medals won is 0, the maximum is 4.18, and the mean is 0.64. The minimum number of journal articles is 0, the maximum is 79,507, and the mean is 1,445.43. The minimum number of software companies is 0, the maximum is 23,971, and the mean is 154.31. Olympiad skill has many missing values due to some countries' lack of participation. The variables, GDP per capita, journal articles, and software industry are particularly skewed – as reflected by their high standard deviations compared with their means – and are consequently transformed to their natural logarithmic in the multivariate analysis.

The first method of bivariate analysis used is cross-tabulation with chi-squared tests of statistical significance, yet this approach is suitable only when the independent and dependent variables are categorical. Accordingly, I recode the four independent variables into a dichotomous format where '1' indicates that the country has a value higher than the mean and '0' indicates that the country has a value lower than the mean. For instance, GDP per capita is recoded into high economic development if the country's GDP per capita is higher than \$12,722.07 and low economic development if it is lower than this figure. Note that this is very similar to the UN's threshold of \$12,615 to define high-income countries (United Nations 2014, 144).

Table 16 shows how resources relate to the possession of military CNO units by comparing the number of countries that are high or low-income within categories of military CNO unit possession. The chi-square (χ^2) statistical test determines the extent to which the observed frequency differs from the count that would be expected if there was no association between the variables. A significant result ($p < 0.05$) suggests we can reject the null hypothesis that the variables are unrelated. If this is the case, the observed association is highly unlikely to have arisen by chance and that therefore there is likely a meaningful relationship between the variables.

Table 16.
National resources and military CNO unit possession

	<i>No military CNO unit</i>		<i>Military CNO unit</i>	
	<i>Number</i>	<i>%</i>	<i>Number</i>	<i>%</i>
<i>Financial resources</i>				
Low GDP per capita	2,250	75.71	124	40.92
High GDP per capita	722	24.29	179	59.08
Total	2,972	100.00	303	100.00
$\chi^2 = 166.81$				
$p = 0.000$				
<i>Olympiad skill</i>				
Low medals	1,435	76.01	53	16.26
High medals	453	23.99	273	83.74
Total	1,888	100.00	326	100.00
$\chi^2 = 450.31$				
$p = 0.000$				
<i>Journal articles</i>				
Low output	2,811	90.65	86	26.38
High output	90.65	9.35	240	73.62
Total	3,101	100.00	326	100.00
$\chi^2 = 931.96$				
$p = 0.000$				
<i>Software industry</i>				
Small industry	2,886	93.07	141	43.25
Large industry	215	6.93	185	56.75
Total	3,101	100.00	326	100.00
$\chi^2 = 710.04$				
$p = 0.000$				

All the chi-square tests report a statistically significant result ($p < 0.05$) suggesting that there is a meaningful correlation between the four types of resources and military CNO unit possession. Above average levels of financial resources are positively associated with the presence of military units. Considering economic development, 59% of countries with a military CNO unit have a high GDP per capita, while only 24.29% of countries without a military CNO unit have a high GDP per capita. Although the possession of capability is associated more with richer countries, there is still a relatively large proportion (40.92%) of military unit possessing countries that have low GDP per capita, so high levels of economic development is by no means a necessary condition for proliferation.

Programming skill is also positively associated with proliferation. 83.74% of countries with a military CNO unit have performed above average in the Olympiads, while only 23.99% of countries without this capability have a high medal count. There appears to be a strong relationship between

Olympiad skill and capabilities, with only 16.26% of countries with a military unit being in the low skill category.

More publications in computer science increases the likelihood of proliferation. 73.62% of countries that have created a military CNO unit have published above average levels of journal articles and just 9.35% of countries that do not have a military unit have a high journal output. Technical knowledge and skill therefore appear to be particularly strong predictors of capability proliferation.

Finally, large software industries are also more likely amongst countries that have military cyber capabilities. Specifically, 56.75% of countries with a military CNO unit have an above average number of software companies, but only 6.93% of countries that do not have this capability have a large software industry. Capability adoption is still relatively common amongst countries with small software industries with 43.25% of military unit possessing countries having a small industry.

Turning to the civilian-based indicator of active cyber capability, Table 17 shows the cross tabulation and chi-square test between these resources and the possession of a national CSIRT.

Table 17
National resources and national CSIRT possession

	No National CSIRT		National CSIRT	
	<i>Number</i>	<i>%</i>	<i>Number</i>	<i>%</i>
<i>Financial resources</i>				
Low GDP per capita	1,897	81.84	531	52.52
High GDP per capita	421	18.16	480	47.48
Total	2,318	100.00	1,011	100.00
$\chi^2 = 306.48$ $p = 0.000$				
<i>Olympiad skill</i>				
Low medals	1,069	82.42	437	45.01
High medals	228	17.58	534	54.99
Total	1,297	100.00	971	100.00
$\chi^2 = 348.44$ $p = 0.000$				
<i>Journal articles</i>				
Low output	2,349	96.47	591	56.50
High output	86	3.53	455	43.50
Total	2,435	100.00	1,046	100.00
$\chi^2 = 890.43$ $p = 0.000$				
<i>Software industry</i>				

Small industry	2,350	96.51	731	69.89
Large industry	85	3.49	315	30.11
Total	2,435	100.00	1,046	100.00

$\chi^2 = 509.95$
 $p = 0.000$

As before, the relationship between each type of resource and national CSIRT adoption is statistically significant with p-values falling below 0.05. These observed frequencies are highly unlikely to have differed to this extent from their expected values by chance alone.

Turning to financial resources first, table 17 shows high-income countries are increasingly likely to have a national CSIRT than countries in the low-income category. The proportion of non-CSIRT countries with a high-income level is 18.16% but the proportion of CSIRT possessing countries with a high-income is 47.48%. Nevertheless, 52.52% of countries with a CSIRT have a lower than average level of economic development so a country need not be wealthy to establish one, although more wealth helps.

High levels of programming skill are more strongly associated with the presence of national CSIRTs. 54.99% of countries with a national CSIRT are in the high medal category compared to 45.01% in the low medal category. The next type of resource is computer science knowledge as indicated by journal article output. Like financial resources, Among the national CSIRT possessing countries, there are more countries with a low publishing output in computer science (56.50%) than with a high publishing output (43.50%). However, the vast majority of countries without a national CSIRT produce low number of computer science knowledge (96.47%). A similar pattern emerges in relation to industrial capacity. 69.89% of countries with a national CSIRT have a below average number of software companies. On the other hand, just 3.49% of countries without a national CSIRT have a large industry.

To conduct an alternative method of bivariate analysis, I compare the baseline probability of a country possessing active cyber capabilities to the probability under the conditional that a country has a certain level of financial, knowledge-based, and industrial resources. The results of this analysis for military CNO units are contained in table 18 and the results for national CSIRTs are contained in table 19.

For each low and high resource category, the first column shows the number of country-year observations where the capability is present, and the second column shows the total observations. By dividing the former with the latter, I calculate the conditional probability which is highlighted in the third column. I then run a difference of proportions test to compare the conditional probabilities to the baseline probability for the presence of cyber capabilities free of any conditions. The baseline

probability of a military CNO unit being present is $326/3427=0.095$, and the baseline probability of a national CSIRT being present is $1,046/3,481 = 0.300$. The Z-score in the fourth column indicates the size and direction of the difference between conditional and baseline probabilities. The last column shows the associated p-values, used to test the null hypothesis that there is no significant difference between conditional and baseline probabilities.

Table 18.
Conditional Probabilities of military CNO unit capability by resources

	<i>Observations with CNO unit</i>	<i>Total observations</i>	<i>Conditional probability</i>	<i>Z</i>	<i>p</i>
<i>Financial resources</i>					
Low GDP per capita	124	2,374	0.052	-7.124	<0.000
High GDP per capita	179	901	0.199	10.593	<0.000
<i>Olympiad skill</i>					
Low medals	53	1,488	0.036	-7.824	<0.000
High medals	273	726	0.376	25.798	<0.000
<i>Journal articles</i>					
Low output	86	2,897	0.030	-12.006	<0.000
High output	240	530	0.453	28.068	<0.000
<i>Software industry</i>					
Small industry	141	3,027	0.047	-9.104	<0.000
Large industry	185	400	0.463	25.043	<0.000

GDP per capita has a positive effect on capability adoption and the differences are statistically significant from the baseline probability of 0.095. The probability of a country with a low GDP per capita having a military CNO unit is reduced to 0.052 ($Z = -7.124$; $p<0.000$), and the probability of a country with a high GDP per capita having a military CNO unit is increased to 0.119 ($Z = 10.593$; $p<0.000$).

Programming skill also increases the likelihood of military CNO units being acquired and the differences are statistically significant. The probability of a country with a low Olympiad medal count having a military CNO unit is reduced to 0.036 ($Z = -7.824$; $p<0.000$), but this increases substantially to 0.376 when a country has a high medal count ($Z = 25.798$; $p<0.000$).

There is a positive and significant relationship between journal articles and the possession of a military cyber capabilities too. The probability of a country having a military CNO unit when it has a low output of computer science articles is 0.03 ($Z = -12.06$; $p<0.000$), but when it has a high output the probability rises to 0.453 ($Z = 28.068$; $p<0.000$).

Likewise, the number of software companies significantly increases the likelihood of countries adopting military cyber capabilities. Low industry countries have a probability of 0.047 of possessing a military CNO unit ($Z = -7.655$; $p < 0.000$), while high industry countries have a probability of 0.463 of having this capability ($Z = 21.245$; $p < 0.000$). As with all the types of resources assessed here, these conditional probabilities are significantly different from the unconditional probabilities.

Table 19.
Conditional probabilities of National CSIRT capability by resources

	<i>Observations with national CSIRT</i>	<i>Total observations</i>	<i>Conditional probability</i>	<i>Z</i>	<i>p</i>
<i>Financial resources</i>					
Low GDP per capita	531	2,428	0.219	-8.791	<0.000
High GDP per capita	480	901	0.533	15.206	<0.000
<i>Olympiad skill</i>					
Low medals	437	1,506	0.290	-0.873	0.383
High medals	534	762	0.701	24.102	<0.000
<i>Journal articles</i>					
Low output	591	2,940	0.201	-11.764	<0.000
High output	455	541	0.841	27.423	<0.000
<i>Software industry</i>					
Small industry	731	3,081	0.237	-7.655	<0.000
Large industry	315	400	0.788	21.245	<0.000

Table 19 highlights the conditional probabilities of national CSIRT adoption based on latent capabilities. The baseline, or unconditional, probability of a country having a national CSIRT is 0.3 which is considerably higher than the baseline probability for military CNO unit possession (0.095). The creation of CSIRTs may be a less resource intensive and more feasible policy to implement compared with military units.

That being said, financial resources are positively associated with the proliferation of national CSIRTs. For countries with below average GDP per capita, the probability of having a CSIRT falls to 0.219 which is significantly lower than the baseline ($Z = -8.791$; $p < 0.000$). For countries with above average GDP per capita, the probability of a national CSIRT increases significantly to 0.533 ($Z = 15.206$; $p < 0.000$).

Increases to a country's programming skill also has a significant effect on the CSIRT creation. When a country has an above average performance in the Olympiads, the probability of CSIRT adoption increases from the baseline of 0.3 to 0.701 ($Z = 24.102$; $p < 0.000$), meaning that a majority of

countries with this level of skill have created a CSIRT. However, countries with below average Olympiad performance do not have a statistically significant reduction in CSIRT adoption ($Z = -0.873$; $p = 0.383$).

Journal article publications has an even stronger relationship with national CSIRTs. There is a statistically significant drop in the probability of a country having a CSIRT when it has below average journal article publications to 0.201 ($Z = -11.764$; $p < 0.000$), and a statistically significant increase to 0.841 when it has above average publications ($Z = 27.423$; $p < 0.000$).

Finally, the size of the software industry is also positively and significantly linked to civilian active capability adoption. The probability of a CSIRT conditional on smaller than average industry is lower than the baseline at a value of 0.237 ($Z = -7.655$; $p < 0.000$), while the probability of a CSIRT conditional on larger than average industry is 0.788 ($Z = 21.245$; $p < 0.000$). Increases to a country's resources are therefore strongly associated with the acquisition of active capabilities in the civilian and military domains, with the largest effects coming from programming skill and computer science knowledge.

This analysis shows that the likelihood of active cyber capability adoption is significantly increased through greater economic, industrial, and science and technological resources. The next question to investigate is how a country's external threat and rivalry environment relates to capability acquisition.

Bivariate analysis: external threat environment and capability

Table 20 provides the summary statistics of the four independent variables used in the analysis to gauge a country's threat environment and therefore its willingness to adopt military CNO units and national CSIRTs.

Table 20.
Summary statistics for willingness-based variables

<i>Independent Variable</i>	<i>Obs.</i>	<i>Missing</i>	<i>Min.</i>	<i>Max.</i>	<i>Mean</i>	<i>Std. Dev.</i>
Rivals	3,481	0	0	12	0.711	0.578
US Rival	3,481	0	0	1	0.055	0.229
Rivals with CNO unit	3,481	0	0	4	0.195	0.578
Cyber incidents	1,937	1,544	0	7.667	0.683	0.376

These four variables are an attempt to capture the degree of insecurity perceived by a country from its international strategic environment or else its motivation to harm a rival's interests. The variable,

rivals records the number of rivals a country has in a given year. The minimum is 0 while the maximum is 12. *US rival* is a dichotomous indicator of whether the country is a rival to the United States which either takes a value of 0 (not a US rival) or 1 (US rival). The third variable, *rivals with CNO unit* measures how many of a country's rivals possess a military CNO unit. This variable has a minimum of 0 and a maximum of 4. The last variable, *cyber incidents* is the average number of cyber incidents experienced by a country over the previous three years. This has 1,544 missing observations because the information is only available from the year 2005. The minimum value is 0 and the maximum value is 7.667.

For cross-tabulation, the continuous variables here are recoded into dichotomous indicators. *Rivals* is recoded so that observations take the value of 1 if the country has at least one rivalry, and 0 if it has no rivalries. As *US rival* is already a dichotomous variable it remains unchanged. *Rivals with CNO unit* now takes a value of 1 if the country has at least one rival with a military CNO unit, and 0 if it has no such rivals. Finally, the variable, *cyber incidents* takes a value of 1 if the country has a 3-year moving average of incidents greater than zero and 0 if otherwise.

The cross tabulation in table 21 shows how the proportion of countries in high threat and low threat categories changes according to whether they possess a military CNO unit or not. Each threat variable is significantly and positively associated with military capability adoption with the p-values associated with the chi-square tests reporting values less than 0.05.

Table 21.
Threat environment and military CNO unit possession

	No Military CNO unit		Military CNO unit	
	<i>Number</i>	<i>%</i>	<i>Number</i>	<i>%</i>
<i>Rivalry</i>				
Rivals = 0	2,039	65.75	134	41.10
Rivals > 0	1,062	34.25	192	58.90
Total	3,101	100.00	326	100.00
$\chi^2 = 77.244$ $p = 0.000$				
<i>U.S. Rivalry</i>				
Not a U.S. rival	2,968	95.71	266	81.60
U.S. rival	133	4.29	60	18.40
Total	3,101	100.00	326	100.00
$\chi^2 = 110.601$ $p = 0.000$				
<i>CNO unit rivalry</i>				
CNO unit rivals = 0	2,796	90.16	186	57.06

CNO unit rivals > 0	305	9.84	140	42.94
Total	3,101	100.00	326	100.00

$\chi^2 = 286.197$
 $p = 0.000$

<i>Cyber incidents</i>				
Cyber threat = 0	1,561	95.42	170	62.73
Cyber threat > 0	75	4.58	101	37.27
Total	1,636	100.00	271	100.00

$\chi^2 = 296.477$
 $p = 0.000$

34.25% of countries without a military CNO unit have at least one rival, but this increases to 58.90% of countries with a military CNO unit. This suggests that the presence of rivalry increases the probability of having this capability.

The next set of results shows that most countries with a military CNO unit are not rivals of the United States (81.60%), so this by no means a necessary condition for capability adoption. On the other hand, countries that have no military CNO unit are much less likely (4.29%) to be rivals to the United States than countries with a military CNO unit (18.40%), suggesting that this factor also increases the likelihood of proliferation.

The presence of CNO capable rivals also appears to be positively associated with the adoption of military cyber capabilities. Among countries without a military CNO unit, the percentage with more than one rival with a military unit is 9.84%. Among countries with a military CNO unit, however, this percentage increases to 42.94%. There is nonetheless a majority (57.06%) of military unit capable countries that have no rivals with this capability.

Turning to the threat from cyber incidents. 4.58% of countries that do not have a military CNO unit have experienced cyber incidents, while 37.27% of countries with a military CNO have experienced cyber incidents, suggesting a positive association between cyber incidents and the adoption of military CNO units. A majority (62.73%) of countries with this capability have nevertheless experienced no cyber threat.

Table 22 shows the cross tabulations between the threat-based factors and the presence of national CSIRTs. Again, all the bivariate relationships are positive and significant with p-values below 0.05.

Table 22.
Threat environment and national CSIRT possession

	No National CSIRT		National CSIRT	
	<i>Number</i>	<i>%</i>	<i>Number</i>	<i>%</i>
<i>Rivalry</i>				
Rivals = 0	1,608	66.04	597	57.07
Rivals > 0	827	33.96	449	42.93
Total	2,435	100.00	1,046	100.00
$\chi^2 = 25.312$				
$p = 0.000$				
<i>U.S. Rivalry</i>				
Not a U.S. rival	2,315	95.07	973	93.02
U.S. rival	120	4.93	73	6.98
Total	2,435	100.00	1,046	100.00
$\chi^2 = 5.876$				
$p = 0.015$				
<i>CNO unit rivalry</i>				
CNO unit rivals = 0	2,232	91.66	785	75.05
CNO unit rivals > 0	203	8.34	261	24.95
Total	2,435	100.00	1,046	100.00
$\chi^2 = 174.850$				
$p = 0.000$				
<i>Cyber incidents</i>				
Cyber threat = 0	1,072	98.44	679	80.07
Cyber threat > 0	17	1.56	169	19.93
Total	1,089	100.00	848	100.00
$\chi^2 = 185.305$				
$p = 0.000$				

The proportion of countries that have rivals is higher among countries with national CSIRTs. 33.96% of countries without a national CSIRT have at least one rival, but this increases to 42.93% among countries with a national CSIRT. Rivalry therefore appears to increase the chances that a country adopts this capability. Only 6.98% of countries with a national CSIRT are rivalled to the United States, but this is slightly greater than the 4.93% of countries without a national CSIRT that are rivalled to the United States. This finding is statistically significant, but at a lower level of certainty ($p=0.015$).

The variable, CNO unit rivalry, is positively correlated also. 24.95% of countries that have created a national CSIRT have at least one rival with a military CNO unit, but only 8.34% of countries without a national CSIRT face a rival of this type. Finally, having a CNO unit is associated with larger cyber

threat. The proportion of states with no military unit yet higher cyber threat is 1.56%, but this increases to 19.93% among countries with a military CNO unit.

Now I examine the conditional probabilities of cyber capability and run difference of proportions tests to show whether the difference between the baseline probability of having cyber capabilities and the conditional probabilities is statistically significant. I begin with military CNO units for which the baseline probability of a country having one is 0.095.

Table 23.
Conditional Probabilities of military CNO unit capability by threat environment

	Observations with CNO unit	Total observations	Conditional probability	Z	p
<i>Rivalry</i>					
Rivals = 0	134	2173	0.062	-5.000	<0.000
Rivals > 0	192	1254	0.153	6.000	<0.000
<i>U.S. Rivalry</i>					
Not a U.S. rival	266	3234	0.082	-2.496	0.013
U.S. rival	60	193	0.311	10.216	<0.000
<i>CNO unit rivalry</i>					
CNO unit rivals = 0	186	2982	0.062	-6.096	<0.000
CNO unit rivals > 0	140	445	0.315	15.781	<0.000
<i>Cyber incidents</i>					
Cyber threat = 0	170	1731	0.098	-5.2852	<0.000
Cyber threat > 0	102	176	0.574	16.5752	<0.000

Having at least one rival significantly increases the probability of a country having a military CNO unit from 0.095 to 0.153 ($Z = 6$; $p < 0.000$), while having no rivals significantly decreases the probability from 0.095 to 0.062 ($Z = -5$; $p < 0.000$). Being a US rival or not also has a significant difference on the probability that a country adopts a military CNO unit. The probability falls to 0.082 when countries are not rivalled to the United States ($Z = -2.496$; $p = 0.013$) but increases to 0.311 among countries that are rivalled to the United States ($Z = 10.216$; $p < 0.000$).

Similarly, countries with CNO-capable rivals are more likely to have developed this capability themselves. The probability under this condition is increased to 0.315 which is significantly greater than the baseline probability ($Z = 15.781$; $p < 0.000$), while the probability in the absence of this condition is reduced to 0.062, which is also statistically significant ($Z = -6.096$; $p < 0.000$). Lastly, a lack of cyber threat significantly reduces from the probability of a CNO unit to 0.098 ($Z = -5.285$; $p = < 0.000$). When cyber threat is above zero the probability significantly increases to 0.574 ($Z =$

16.575; $p < 0.000^{27}$). The final set of bivariate tests assesses the conditional probabilities of national CSIRT possession based on external threat. The baseline probability for a CSIRT is 0.3.

Table 24.
Conditional Probabilities of national CSIRT capability by threat environment

	Observations with CNO unit	Total observations	Conditional probability	Z	P
<i>Rivalry</i>					
Rivals = 0	597	2205	0.271	-3.046	0.002
Rivals > 0	449	1276	0.352	4.004	0.000
<i>U.S. Rivalry</i>					
Not a U.S. rival	973	3288	0.296	-0.311	0.756
U.S. rival	73	193	0.378	1.449	0.147
<i>CNO unit rivalry</i>					
CNO unit rivals = 0	785	3017	0.260	-2.463	0.014
CNO unit rivals > 0	261	464	0.563	9.233	<0.000
<i>Cyber incidents</i>					
Cyber threat = 0	679	1751	0.388	-4.218	<0.000
Cyber threat > 0	169	186	0.909	12.942	<0.000

Table 24 shows the probabilities of a country possessing a national CSIRT conditional on the threat environment facing the country. The statistical test can show whether these conditional probabilities are significantly different from the baseline probability of CSIRT possession which is 0.3.

Most of the threat environment factors have a positive and significant impact on the probability of national CSIRTs. For instance, when a country has no rivals, the probability of it possessing a CSIRT drops to 0.271 ($Z = -3.046$; $p = 0.002$). When a country has at least one rival the probability increases to 0.352 ($Z = 4.004$; $p < 0.000$).

Rivalry status with the United States is not significantly associated with the possession of national CSIRTs since neither the presence of this rivalry ($Z = 1.449$; $p = 0.147$) nor its absence ($Z = -0.311$; $p = 0.756$) changes the probability significantly from the baseline probability of 0.3. Countries that have at least one rival with a military CNO unit see their probability of having a national CSIRT increase significantly to 0.563 ($Z = 9.233$; $p < 0.000$). When the country does not have this kind of rival the probability significantly drops to 0.260 ($Z = -2.463$; $p = 0.014$).

The factor with the biggest effect on proliferation is the presence of cyber incidents. Having a higher than zero level of cyber threat is associated with a 90.9% chance of having a national CSIRT and this

²⁷ Baseline probability is different because of missing data on cyber incident variable.

is a statistically significant increase in proportion ($Z = 12.942$; $p < 0.000$). When a country has no cyber threat their probability of having a national CSIRT significantly decreases to 0.388 from a baseline probability of 0.438²⁸ ($Z = -4.218$; $p < 0.000$).

To summarise the bivariate results, almost all the opportunity and willingness factors lead to a significant and positive increase in active cyber capability. The next step is to determine if these results hold up to a more robust multivariate analysis.

Multivariate analysis: opportunity and willingness theory tested

In this part of the analysis, the opportunity and willingness variables are included together alongside control variables in a multivariate model. The advantage of multivariate analysis is that it can indicate the independent effect of each explanatory factor while controlling for the influence of the other variables in the model, and therefore assess competing explanations for the proliferation of cyber capabilities. My goal is to provide a robust explanation for the adoption of active cyber capabilities.

To review the methods, I use a logistic regression analysis, performed on a cross-sectional time-series dataset of 194 nation states recorded over the period 2000 through 2017 to assess the factors impacting the likelihood of a country possessing operational cyber capabilities. Logistic regression is an appropriate method when the dependent variable takes one of two possible values. The dependent variables are the presence or absence of a national CSIRT and the presence or absence of a military CNO unit.

As well as incorporating the latent resources and threat environment indicators I control for three potentially confounding factors. These have been detailed in chapter 5 so there is no need to go into depth here. The first control variable is regime type, measured using Polity IV project's autocracy-democracy scores which places countries on a scale from -10 (most authoritarian) to 10 (most democratic) (Marshall, Gurr, and Jaggers 2016). Democracies may be more likely to have greater resources and build capacity. The second control variable is whether the country is a major power (1) or not (0) using the Correlates of War classification. In the period under study, the major powers are the United States, China, Russia, the United Kingdom, France, Germany, and Japan. Major powers possess greater resources, face a more intense threat environment, and may be more willing to build cyber capability. Finally, I control for *Internet years*, which is operationalised as the number of years that have elapsed since the World Wide Web was invented in 1990. This controls for temporal dependence and the notion that cyber capabilities are more likely to be acquired as time

²⁸ This baseline is different for this variable because I account for the missing data on the cyber incident variable and recalculate the baseline probability.

goes on due to the inevitable spread and imitation of technology in the international system, as reflected in the technological imperative hypothesis (Buzan and Herring 1998, 50).

I separate the results for my dependent variables, national CSIRTs and military CNO units into two separate tables. Within each table I include the results of four different regression models. I run four models for each dependent variable to separate independent variables that are likely to be collinear, and thus may bias the results. I separate Olympiad skill from computer science knowledge because Olympiad skill is likely to be a result of greater computer science knowledge (i.e. an intervening variable) and its inclusion will wipe out the statistical significance of the computer science knowledge variable. Moreover, I separate the number of software companies from ICT service exports as they are essentially measuring the same concept and I want to demonstrate that the results are robust with two alternative measures.

Results

Table 25 presents the results of the models predicting the presence of a military CNO unit. The results differ from the bivariate tests in that some factors are no longer statistically significant when tested under stricter conditions. For example, software industry under either measure has no statistically significant effect on proliferation. This supports my methodological choice of excluding this factor as a component of my latent cyber capability index. GDP per capita also is no longer statistically significant. Economic development is therefore not the key determinant of active cyber capability adoption.

On the other hand, the results have highlighted some reliable results. In terms of opportunity-based explanations, there is strong evidence that programming skill and computer science knowledge are robust predictors of military CNO units. These variables are positively associated with the possession of capabilities at a statistically significant level across every model, while controlling for other factors. Programming skill has a greater level of statistical significance ($\beta = 1.298$; $p \leq 0.01$ in model 1) than computer science knowledge ($\beta = 0.358$; $0.01 < p \leq 0.05$ in model 2). Olympiad performance is therefore a better predictor than journal articles of which countries will establish military operations units.

On the willingness side of the theory, many external threat-based factors are not robust predictors of capability adoption. Cyber incidents are statistically associated with military CNO units in models 2 and 4 but are no longer significant in models 1 and 3 when programming skill is controlled for. Moreover, there is no evidence that states rivalled to the United States are any more likely to develop military capabilities than other states when controlling for other factors. And there is no longer a statistically significant relationship between CNO rivals and capability adoption either. The cyber

domain therefore does not appear to follow the action-reaction pattern of military build-ups driven by the capabilities of rival states (Richardson 1960).

The number of interstate rivals, on the other hand, is the most robust determinant of the possession of military CNO units as it is significant to a high degree in all four models. Rivalry has an especially strong, positive, and significant impact on the presence of military CNO units, controlling for other factors ($\beta = 1.018$; $p \leq 0.001$). This finding could be explained by the fact this type of capability serves as a means of deterring or attacking rivals in cyberspace.

Table 25.
Logistic regression of military CNO unit possession

	(1)	(2)	(3)	(4)
<i>Programming skill</i>	1.298** (0.432)		1.538*** (0.392)	
<i>Computer science knowledge</i>		0.358* (0.142)		0.401* (0.181)
<i>Software companies</i>	0.334 (0.177)	0.272 (0.166)		
<i>ICT service exports</i>			0.238 (1.61)	0.191 (0.172)
<i>Rivals</i>	1.018*** (0.278)	0.840*** (0.241)	0.840** (0.281)	0.765** (0.250)
<i>CNO rivals</i>	-1.083 (0.596)	-0.734 (0.412)	-0.642 (0.606)	-0.637 (0.438)
<i>Cyber incidents</i>	1.120 (0.826)	1.468* (0.687)	1.588 (1.002)	1.761* (0.775)
<i>US rivalry</i>	-0.559 (0.874)	0.190 (0.904)	-1.959 (1.028)	-0.818 (1.129)
<i>GDP per capita</i>	0.109 (0.309)	0.048 (0.211)	0.329 (0.264)	0.155 (0.209)
<i>Democracy</i>	0.029 (0.060)	0.036 (0.059)	0.050 (0.054)	0.066 (0.067)
<i>Major power</i>	1.280 (1.101)	1.860 (1.023)	1.369 (1.241)	2.450 (1.265)
<i>Internet years</i>	0.355*** (0.065)	0.298*** (0.058)	0.387*** (0.056)	0.320*** (0.052)

<i>Constant</i>	-13.26** (4.055)	-12.70*** (3.130)	-20.30*** (3.356)	-17.81*** (0.052)
<i>N</i>	1143	1541	1040	1365
<i>Pseudo R²</i>	0.494	0.488	0.503	0.492

Notes: The regression coefficients convey the effect of a one-unit increase in each independent variable on the log odds of capabilities being present. Robust standard errors clustered by country in parentheses. Statistical significance at the 95%, 99%, and 99.9% levels denoted by *, **, and *** respectively. Major power is omitted from the CSIRT models because it completely predicts the presence of capabilities.

Table 26 displays the results for national CSIRTs adoption. This time the pseudo R² values range from 0.32 to 0.39 which are lower than the equivalent statistics for military CNO units. This suggests that the opportunity and willingness framework is better at explaining active cyber capabilities in the military rather than civilian sphere. This makes sense given that many of my theories were derived from studies on military capabilities.

Nevertheless, the regression results show that similar factors are responsible for the proliferation of national CSIRTs as they are for military CNO units. Again, there is very little evidence that a country's industrial capacity measured either by software companies or ICT service exports has an independent impact on the presence of national CSIRTs, given that neither of these variables are statistically significant except in model 1. These results suggest that industry is not a key determinant of cyber capability proliferation and that states with a smaller IT related industry should not necessarily be at a disadvantage.

Moreover, GDP per capita is only statistically significant in model 3. This finding, combined with similar results from table 25, casts doubt on the efficacy of this economic development as a proxy for technological capacity. The findings demonstrate that skills and knowledge are more precise measures of the state's opportunity to develop cyber capabilities. Technical knowledge may be a mediating variable in the causal sequence between economic development and cyber capability. While higher GDP per capita probably helps a country acquire the necessary skills and knowledge, it is not the proximate cause of capability adoption.

Programming skill and computer science knowledge provide the best explanation from the opportunity side of the argument. Computer science knowledge is a more significant predictor of national CSIRTs ($\beta = 0.527$; $p \leq 0.001$ in model 2) than Olympiad performance ($\beta = 1.243$; $0.01 < p < 0.05$ in model 1). This is the opposite finding from that of military CNO units. This could imply that practical programming skill as reflected in Olympiad performance is more relevant to military applications like hacking while the codified, academic knowledge as reflected by journal articles is more relevant to civilian cyber security development such as incident response operations.

As before there are mixed results for the willingness-based factors. Rivalry is also the most robust explanatory factor for national CSIRTs, but this time it is only statistically significant in three out of four models (0.851; $p \leq 0.05$) and at a reduced level of statistical significance. This makes sense given that national CSIRTs are a defensive asset and cannot be applied toward offensive operations to harm a rival's interests unlike military capabilities.

Table 26.
Logistic regression of national CSIRT possession

	(1)	(2)	(3)	(4)
<i>Programming skill</i>	1.243* (0.511)		1.333* (0.593)	
<i>Computer science knowledge</i>		0.527*** (0.124)		0.453*** (0.137)
<i>Software companies</i>	0.349* (0.143)	0.0931 (0.160)		
<i>ICT service exports</i>			0.203 (0.119)	0.094 (0.127)
<i>Rivals</i>	0.851* (0.350)	0.409 (0.215)	0.803* (0.382)	0.485* (0.232)
<i>CNO rivals</i>	-1.008* (0.506)	-0.800 (0.451)	-0.851 (0.523)	-0.825 (0.456)
<i>Cyber incidents</i>	2.342 (1.230)	2.774* (1.261)	2.097 (1.244)	2.351* (1.170)
<i>US rivalry</i>	-0.158 (1.035)	-0.115 (0.980)	-0.147 (1.034)	-0.004 (1.035)
<i>GDP per capita</i>	0.225 (0.189)	0.203 (0.171)	0.392* (0.194)	0.292 (0.191)
<i>Democracy</i>	-0.033 (0.034)	-0.026 (0.030)	-0.008 (0.046)	-0.005 (0.034)
<i>Major power</i>	(omitted)	(omitted)	(omitted)	(omitted)
<i>Internet years</i>	0.254*** (0.037)	0.213*** (0.030)	0.265*** (0.040)	0.230*** (0.033)
<i>Constant</i>	-8.392*** (1.701)	-9.015*** (1.532)	-13.74*** (2.092)	-11.61*** (2.530)
<i>N</i>	1173	1571	1070	1395

<i>Pseudo R</i> ²	0.327	0.394	0.329	0.386
------------------------------	-------	-------	-------	-------

Notes: The regression coefficients convey the effect of a one unit increase in each independent variable on the log odds of capabilities being present. Robust standard errors clustered by country in parentheses. Statistical significance at the 95%, 99%, and 99.9% levels denoted by *, **, and *** respectively. Major power is omitted from the CSIRT models because it completely predicts the presence of capabilities.

The control variables in both sets of results shows a similar pattern. There is no statistically significant correlation between how democratic a country is and its adoption of military CNO units or national CSIRTs. This undermines domestic political arguments for capability proliferation. Both types of countries are likely to pursue active cyber capabilities given they have the right resources and willingness. The major power status of a country also has no statistically significant impact on active capabilities. Internet years, on the other hand, is the most consistent independent variable in terms of statistical significance. The more years that have passed since the World Wide Web was invented, the greater the likelihood of state's possessing military CNO units and national CSIRTs, which shows that proliferation is very much a function of time. This factor could be gauging the diffusion of cyber technology over time throughout the international system which serves as an alternative explanation for proliferation besides domestic resources or external threat environment.

Substantive effects

The discussion so far has focused on the direction and statistical significance of the relationships between the explanatory variables and the dependent variables. A more substantive and intuitive understanding of their effects can be assessed through predicted probabilities. Table 27 highlights the impact of increasing the value of each independent variable by one standard deviation from its mean value (for continuous variables) or from 0 to 1 (for categorical variables) on the probability of a state possessing a military CNO unit, while holding other variables at their mean levels. Similarly, table 28 shows the effect of increasing the independent variables on the probability of a state possessing a national CSIRT.

Table 27.
Effect of changes in independent variables on the probability of military CNO unit²⁹

	Continuous variables			Categorical variables		
	<i>At mean</i>	<i>Standard deviation +1</i>	<i>Difference</i>	<i>At 0</i>	<i>At 1</i>	<i>Difference</i>
<i>Programming skill</i>	.115	.329	0.214			
<i>ICT service exports</i>	.087	.151	0.064			
<i>Rivals</i>	.116	.284	0.168			
<i>CNO rivals</i>	.126	.091	-0.035			
<i>Cyber incidents</i>	.112	.186	0.074			
<i>US rival</i>				.129	.021	- 0.108
<i>GDP per capita</i>	.104	.160	0.056			
<i>Democracy</i>	.109	.144	0.035			
<i>Major Power</i>				.110	.326	0.216
<i>Internet years</i>	.028	.176	0.148			

Of the statistically significant predictors from regression model 3, Table 27 shows that programming skill has the largest substantive effect on military CNO unit adoption. When Olympiad skill is increased by one standard deviation from its mean value, the probability of a state having this capability goes from 0.115 to 0.329, a difference of 0.214 in probability.

Rivalry has the second largest impact. States with a mean number of interstate rivals have a probability of 0.116 of possessing military CNO units which when increased by one standard deviation becomes a probability of 0.284, an increase of 0.168. Raising the number of Internet years by one standard deviation from its mean results in a change of 0.148 in the probability of military CNO units from an initial 0.028 to 0.176.

The model also predicts the probability among major powers to be 0.326 compared to 0.110 among non-major powers, but this result was not statistically significant in any model. The results suggest that the most substantive – as well as statistically significant – predictors of the proliferation of military cyber capabilities are technical skill, interstate rivalry, and the passing of time.

²⁹ Based on the results of Table 25, model 3

Table 28.
Effect of changes in independent variables on the probability of national CSIRT³⁰

	Continuous variables			Categorical variables		
	<i>At mean</i>	<i>Standard deviation +1</i>	<i>Difference</i>	<i>At 0</i>	<i>At 1</i>	<i>Difference</i>
<i>Computer science knowledge</i>	.422	.784	0.362			
<i>Software companies</i>	.556	.605	0.049			
<i>Rivals</i>	.567	.692	0.125			
<i>CNO rivals</i>	.574	.459	-0.115			
<i>Cyber incidents</i>	.556	.781	0.225			
<i>US rival</i>				.566	.538	-0.028
<i>GDP per capita</i>	.564	.637	0.073			
<i>Democracy</i>	.568	.527	-0.041			
<i>Major Power</i>				-	-	-
<i>Internet years</i>	.358	.627	0.269			

Turning to the national CSIRT predictions, table 28 shows that the number of computer science journal articles has the largest substantive effect on the probability of a national CSIRT. The probability of this capability being present is 0.422 for countries with a mean number of journal articles and 0.784 for countries with a one standard deviation increase in journal articles. Internet years has the second largest effect. Specifically, the probability of a national CSIRT being present increases by 0.269 from an initial 0.358 at the mean value to 0.627 after a one standard deviation increase.

The third largest impact results from an increase in cyber incidents. States facing a mean level of cyber threat have a probability of 0.556 of possessing a national CSIRT, while a one standard deviation increase results in a probability of 0.781, an increase of 0.225. Given that this variable is only statistically significant in two of the four national CSIRT regression models, it is not clear if there is a causal effect going on.

Finally, an increase in rivalry by one standard deviation from the mean is associated with an increase of 0.125 in the probability of a national CSIRT, but this variable is not statistically significant in the regression model in which these results are based. The results suggest that the statistically significant factors with the largest predictive capacity for national CSIRTs are technical knowledge and the passing of time.

Which countries are next?

³⁰ Based on the results of Table 26, model 2

Who are the next likely countries to adopt a military CNO unit and a national CSIRT? To answer this, I use the results of CNO unit model 3 and national CSIRT model 6 (which had the highest predictive power) to obtain the predicted probabilities of each country to possess these active capabilities. I then compare the predicted probabilities with whether or not the country had acquired the capability as of 2017. Table 29 lists the five countries predicted to be most likely to have acquired a CNO unit but have not yet done so. Table 30 lists the five countries predicted to be most likely to have acquired a national CSIRT but have not yet done so.

Table 29.
Likely next adopters of military CNO units

<i>Country</i>	<i>Probability</i>
Serbia	.853
Slovakia	.835
Czech Republic	.795
Croatia	.681
Ireland	.629

Table 30.
Likely next adopters of national CSIRTs

<i>Country</i>	<i>Probability of national CSIRT</i>
Algeria	.939
Jordan	.873
Kuwait	.872
Nigeria	.832
Pakistan	.825

According to the predictions, several Balkan countries as well as Ireland should soon establish computer network operations units within their military. Algeria is the most likely to create a national CSIRT next. Czech Republic is predicted to have a probability of 0.795 of possessing a military CNO unit. The validity of these predictions is supported by a news article from 2018 suggesting that the Czech Republic is planning to establish a “cyber force headquarters” in its military by 2019 with 400 to 500 soldiers (Xinhua News 2018, Ministry of Defence and Armed Forces n.d.). The Ministry of Defence of Croatia also announced in 2019 the creation of a cyber command (Office of the National Security Council n.d.).

Discussion

The findings helped us understand why states develop the capacity to engage in computer network operations. The analysis confirms hypothesis 1 from the theoretical chapter and restated at the beginning of this chapter. States more likely to develop active cyber capabilities if they have the opportunity to do so. More specifically, the most important type of resource that gives a country opportunity is technical programming skill and computer science knowledge. Other resource-based indicators like industry and economic development have less impact when controlling for other factors.

This emphasises the importance of accounting for the non-material assets of skill and knowledge when assessing how cyber technology is likely to proliferate in the international system. The cyber domain may have low financial and industrial barriers to entry, but as other scholars have pointed out (Slayton 2017, 82), skill is perhaps the key factor placing some states at an advantage over others in developing cyber capability.

In terms of policy relevance, these findings suggest that strategies aimed at improving education and skills cybersecurity should be promoted. Moreover, in trying to assess the level of potential threat, we should also pay attention to those countries whose citizens exhibit high computer programming skills since they have greater means of training professional hackers to carry out computer network operations.

That being said, the countries that go on to establish military CNO units tend to be those with pre-existing tensions with other countries. The results therefore also support hypothesis 2. States with increased willingness, as reflected by a state's external threat environment, are more likely to develop active cyber capabilities. Specifically, the number of international rivals is a key determinant of a state's possession of military-based cyber capabilities, yet this factor is not as robust a predictor for national CSIRTs. This finding suggests that the increasing role of the military in cyberspace, as seen through the creation of cyber commands, is in part driven by a state's competitive relations with other states. Rivalry was the only significant predictor of capability, compared with the other willingness factors like previous cyber-attacks, relationship to the United States, and a rival's cyber capabilities. These suggest that realist notions of the balance of power or security dilemma have limited relevance to explaining the proliferation of cyber capabilities.

Perhaps worryingly, states appear to be responding to rivalry through military means by developing units with the authority and capacity to act offensively, rather than focusing on defence and resilience against cyber incidents. Rivalry clearly has a key role to play in explaining state behaviour in cyberspace and policy makers should be aware of this when seeking how to limit the proliferation of

cyber capabilities. The finding that the adoption of capabilities is highly and positively correlated with time, however, suggests that the spread of cyber capabilities is likely to continue into the future.

Finally, the analysis also helps to bolster the predictive validity of the chosen measures of latent cyber capability. Olympiad performance and computer science publications are useful in predicting the adoption of active cyber capabilities and in that sense are successfully capturing the concept of latent cyber capability.

The next crucial question is whether the proliferation of active capabilities is likely to drive an escalation in cyber incidents and conflict, or whether cyber capabilities can deter aggressive cyber activity. Deterrence has clearly failed for the development of military capabilities, but will it have an impact on the propensity for cyber conflict? These questions are investigated in the upcoming chapters.

CHAPTER VIII

Cyber Capability and Conflict: The Effect of Defensive Capabilities

Introduction

Having established the determinants of active cyber capability in the previous chapter, the next puzzle is what effect capabilities have on cyber conflict. In this chapter, I assess the statistical relationships between capability that could be applied to cyber defence and the frequency and outcome of cyber incidents against the state. Deterrence by denial offers a causal mechanism between a state's defensive initiatives and the reduction of cyber incidents by lowering an attacker's expectation of success. As Nye (2016/2017) puts it, "by chewing up the attacker's resources and time, a potential target disrupts the cost-benefit model that creates an incentive for attack".

Indeed, this is a goal in many countries' national cyber strategies. The South Korean strategy for example aims to "strengthen security capabilities to deter cyber threats, detect and block them quickly, and respond to any incident promptly" (National Security Office of South Korea 2019, 12). Another example is the UK's Active Cyber Defence Programme which seeks to making the UK a "harder target for state sponsored actors and cyber criminals by increasing the resilience of UK networks resilience to attack" (HM Government 2016, 33). The establishment of these capabilities may in fact be a way for the state to signal to potential adversaries that they will not succeed in their attempts.

As argued in the theoretical framework chapter, efforts to achieve deterrence by denial through defensive cyber capabilities are likely to fail because of the inherent difficulty in preventing intrusions. This led to hypothesis 3: *Active cyber capabilities for defensive purposes will not cause a reduction in cyber incidents against the defender.*

This is because there are a multitude of possible attack vectors given the widespread nature of Internet infrastructure throughout a society meaning that a determined and sophisticated state actor is likely to find a way to harm its rival in cyberspace. Nevertheless, we need empirical analysis on this issue. My question here is do the efforts states make to manage cyber-attacks actually reduce the incidence and success of attacks? As the findings will show, increases in defensive capability do not lead to a reduction in cyber incidents or of their success. In fact, these initiatives are correlated with an increase in cyber incidents against the state. I end this chapter with a discussion of the deeper explanation and implications of these findings.

Research Design

Three variables from the NCC dataset are used here as proxies for governmental and societal efforts to build cyber defence. If these efforts are successful, we should expect an increase in these variables to lead to a reduction in the number of cyber incidents experienced by a state and for the impact of these incidents to also be reduced. From the latent capability component, I use the number of secure Internet servers per million people in each country. This reflects the level of security taken by firms and organisations country wide to secure their websites through encryption. It may also approximate the general security of infrastructure in a society.

From the active capability component, I use the presence of a national CSIRT and a national cyber security strategy, which are both governmental initiatives. National CSIRTs are teams dedicated to respond to computer network incidents at the national level and to serve as a central point of call for affected organisations. They are also tasked to promote better cyber security awareness and practices and to foster communication and coordination between sectors in society (Killcrece 2004). National cyber security strategies are documents setting out the national plan to reduce cyber threats against the country through various initiatives like establishing incident response capability, improving cyber security awareness and training, establishing public private partnerships, engage in international cooperation, or promoting domestic industry.

A country that has implemented these capacities and policies is evidently taking greater steps to increase cyber defence than a country that has not. Moreover, the purpose of these initiatives might also be to signal to potential aggressors an increased defensive capacity in an attempt to deter attack. It is reasonable to ask therefore if these efforts have had any impact in the level of cyber threat experienced.

To assess whether these actions have had an effect in reducing cyber conflict I first look at the bivariate relationships between each indicator and the frequency or likelihood of cyber incidents faced by the state, beginning at the system level and then moving to the country level. Cyber incident data is taken from the DCID dataset by Valeriano and Maness (2014). For robustness, I then employ a multivariate regression model to control for Internet penetration and introduce lagged explanatory variables in order to reduce the chance of capturing a reverse causal relationship. In other words, while my question asks if capabilities affect conflict, conflict might also affect capabilities as a response to threat. Lastly, I examine whether incidents are likely to be more or less successful when they target a country with stronger defensive capabilities.

Defensive capabilities and cyber incidents at the system level

I first investigate this question at the system level to gauge the relationship between total capabilities in the international system and the frequency of cyber incidents over time using the DCID dataset (Valeriano and Maness 2014). Figure 16 shows how the level of secure Internet infrastructure, as measured by total secure servers divided by world population relates to the number of cyber incidents occurring between rival states from 2010 to 2016.³¹ The graph shows that as secure infrastructure has increased from 2010 to 2016, the number of cyber incidents have fluctuated, reaching a first peak in 2011, falling in 2012, then reaching a second peak in 2014 before dropping again by 2016 to similar levels as in 2010.

Moving to the effect of active capability, figure 17 assesses the relationship between the total number of states with a national CSIRT and the frequency of incidents while figure 18 assesses the relationship between the total number of states with a national cyber security strategy and the frequency of incidents. They show the cyber conflict has increased despite a large increase in the national cyber security preparations of states.

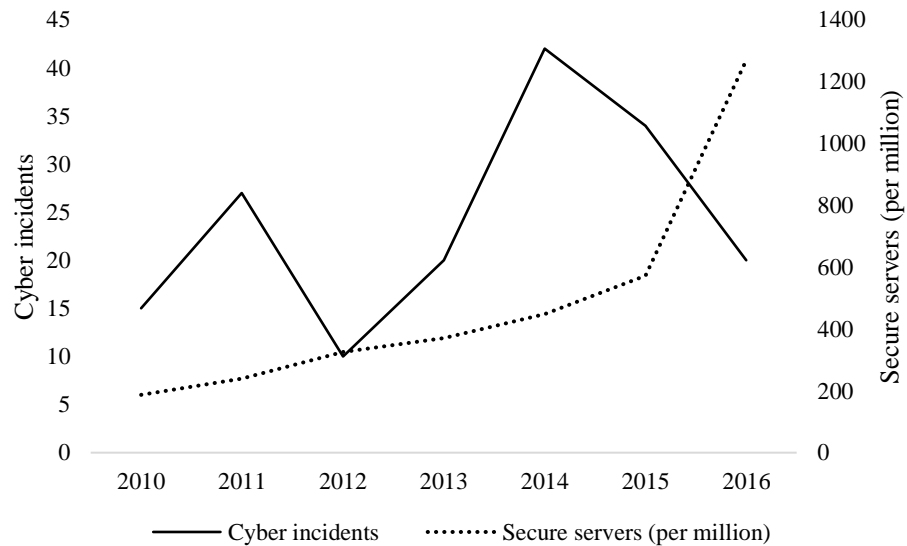


Figure 15. Secure Internet infrastructure and cyber incident frequency

³¹ The secure server data does not predate 2010.

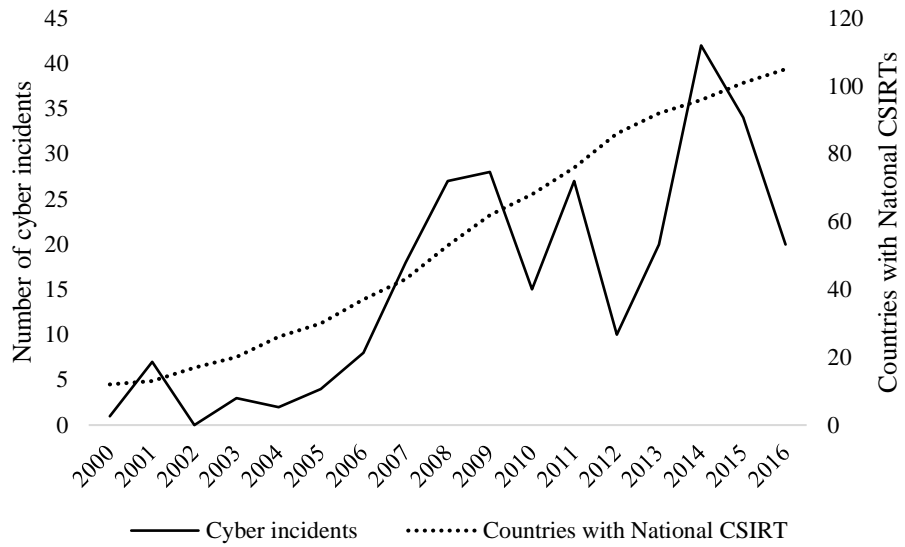


Figure 16. National CSIRTs and cyber incident frequency

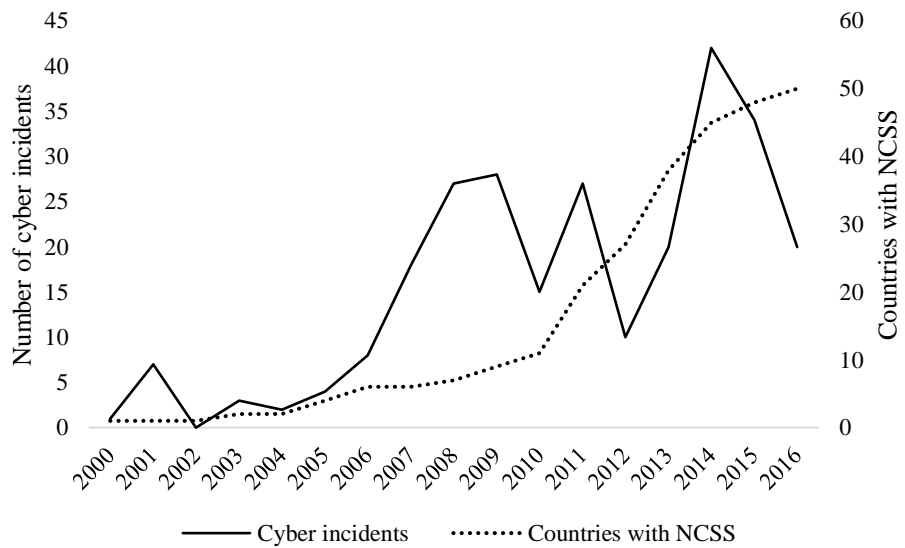


Figure 17. National Cyber Security Strategies and cyber incident frequency

To place a statistic on these patterns, table 31 gives the correlations between each capability variable and the number of cyber incidents in each year. Secure servers have almost no correlation with a coefficient of just 0.07. National CSIRTs and strategies have a high positive correlation (0.78 and 0.69 respectively). In years where there are more states with defensive capability, there tends to be higher levels of cyber incidents. The proliferation of CSIRTs and strategies, therefore, have not reduced levels of cyber threat. Rather these empirical observations may suggest that increased cyber threats have prompted investments in cyber capability.

Table 31.
Correlation between defensive cyber capability and cyber incidents

Variable	Correlation	Observations
Secure Internet servers (per million)	0.07	7
National CSIRTs	0.78	17
National Cyber Security Strategies	0.69	17

This type of analysis is very limited because it provides only a small number of observations with which to infer statistical associations and does not provide information on the characteristics of specific countries. In the next analysis, I investigate if a country’s capability reduces cyber incidents against it.

Defensive capabilities and cyber incidents at the country level

Turning to the country level of analysis, do states with more defensive cyber capability suffer fewer cyber incidents? I investigate this question first by comparing the total number of cyber incidents a country was a victim of between 2000 to 2016 with a country’s number of secure servers (per million) in the scatter plot in figure 19. Table 32 then shows the correlation between these variables in statistical terms.

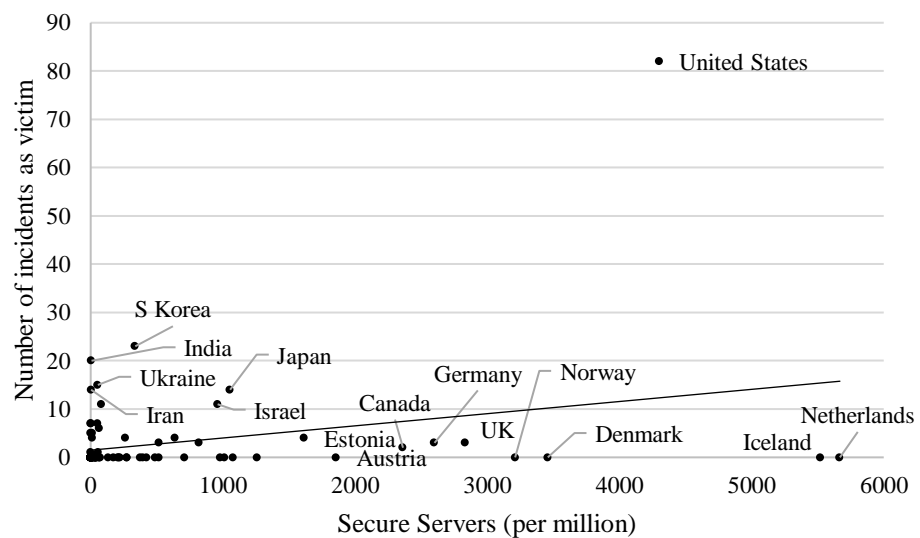


Figure 18. Secure servers and total incidents suffered (2000-2016)³²

³² The analysis was run again with the outlier (the United States) removed but this did not change the statistical significance of the secure server variable.

Table 32.
Correlation between secure servers (per million) and cyber incidents initiated (2010-2016)

Variable	Correlation (-1 to 1)	Observations
Secure servers per million	0.30	93

There is no clearly visible relationship between these two variables. Moreover, the correlation is just 0.30 which is weak yet positive. Countries with more secure infrastructure do not suffer fewer cyber incidents.

Another method is to examine whether countries with greater than average secure servers are less likely to experience a cyber incident in a given year. Table 33 shows the cross tabulation between the categorical indicators of secure servers and cyber incidents. The variable, secure servers is recorded as high if the country has above the median secure servers and low if it has below median secure servers. The cyber incident variable is whether or not the country was a victim of a cyber incident at least once in a given year.

Table 33.
Cross tabulation of secure servers (per million) and cyber incident initiation (2010-2016)

<i>Was the state the victim of cyber-attack?</i>	Low secure servers		High secure servers	
	<i>Number</i>	<i>%</i>	<i>Number</i>	<i>%</i>
No	315	93.20	297	86.34
Yes	23	6.80	47	13.66
Total	338	100.00	344	100.00

$\chi^2 = 8.706$
 $p = 0.003$

The results show there is a statistically significant relationship between secure servers and victimhood ($\chi^2 = 8.706$; $p=0.003$), but the relationship runs in the opposite direction from what might be expected if secure servers help defend against cyber incidents. Countries with greater secure servers are more, not less, likely to experience a cyber incident in a given year than countries with less secure servers. Specifically, 6.8% of countries with below average secure infrastructure were the victim of a cyber incident, while 13.66% of countries with above average secure infrastructure were the victim of a cyber incident. Secure servers are therefore associated with an increased likelihood of suffering a cyber incident from a rival country.

There are two plausible explanations for this finding. Countries with more secure servers are likely to be more Internet dependent and economically developed which means they are both more vulnerable to cyber threats and a more attractive target of cyber operations. Secondly, improvements

in cyber security infrastructure might be a response to increased cyber threats. These could explain the positive relationship between incidents and capabilities.

How does national CSIRT and NCSS possession relate to the number of cyber incidents? As figures 20 and 21 show, countries with national CSIRTs and NCSSs suffer more cyber incidents than countries without these capabilities and policies. Countries without a CSIRT suffered an average 0.41 incidents per year while countries with a CSIRT suffered an average 6.89 incidents per year against them. Similarly, countries without a national strategy experienced an average of 1.65 incidents per year while countries with a national strategy suffered an average of 23.2 incidents per year.

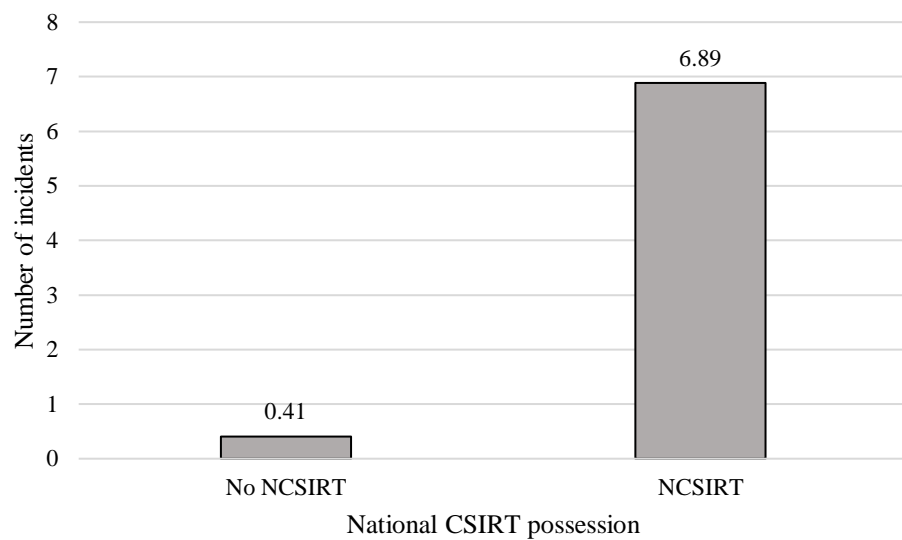


Figure 19. Average cyber incidents experienced according to National CSIRT possession

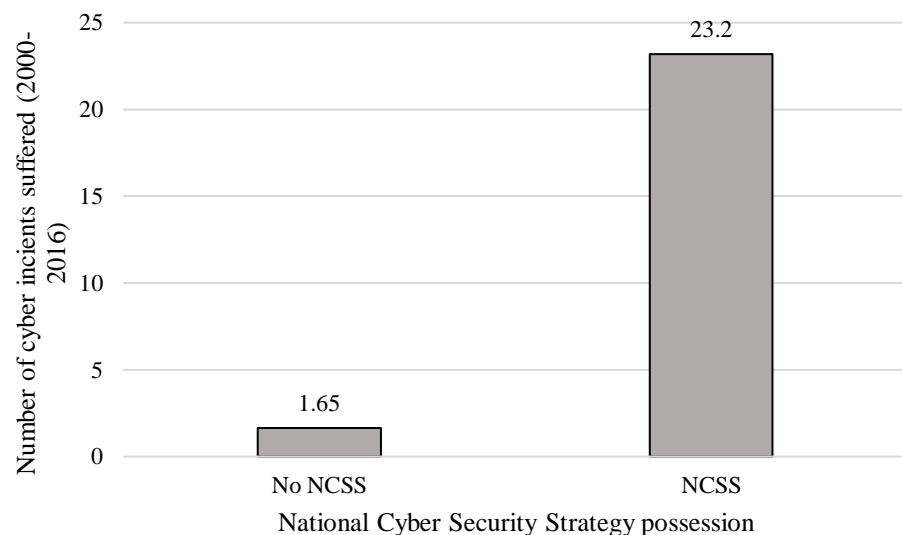


Figure 20. Average cyber incidents according to NCSS possession

By utilizing the time series dimension of the data, I can compare countries with or without these defensive capacities in terms of whether they experienced a cyber incident in a given year. In both cases, the presence of defensive capabilities or policies is associated not with a reduction in the likelihood of attack but with an increase. As indicated in the cross tabulations of table 34 and 35 defensive indicators are associated with an increase in cyber incidents.

Table 34.
Cross tabulation of national CSIRT and cyber incident initiation (2010-2016)

<i>Was the state the victim of cyber-attack?</i>	No CSIRT		CSIRT	
	Number	%	Number	%
No	1014	97.78	498	83.70
Yes	23	2.22	97	16.30
Total	1037	100.00	595	100.00

$\chi^2 = 110.096$
 $p = 0.000$

2.22% of states without a national CSIRT suffered a cyber incident in a given year which increased to 16.30% if a state did have a national CSIRT. Moreover, 4.74% of states without a national strategy experienced a cyber incident in a given year while 26.53% of countries with a strategy experienced one. Both relationships are statistically significant according to the chi-squared tests.

Table 35.
Cross tabulation of NCSS and cyber incident initiation (2010-2016)

<i>Was the state the victim of cyber-attack?</i>	No strategy		Strategy	
	Number	%	Number	%
No	1368	95.26	144	73.47
Yes	68	4.74	52	26.53
Total	1436	100.00	196	100.00

$\chi^2 = 120.260$
 $p = 0.000$

Like secure servers, these proxy indicators for defensive capability correlate to an increase in cyber incidents. These initiatives therefore have not been able to deter cyber incidents from rival states. One explanation for this finding could be the fact that countries with better developed cyber security infrastructure, capabilities, and policies are more likely to be economically developed, have a greater

degree of Internet dependence in general, and consequently more likely to face higher levels of cyber threat. To control for this baseline level of vulnerability and investigate the independent effect of cyber capabilities on conflict, I now employ multivariate regression techniques.

Multivariate analysis

The multivariate analysis allows for a more robust analysis by controlling for how dependent a state is on the Internet. Perhaps when controlling for this level of baseline vulnerability to cyber incidents, defensive capacities will be associated with a reduction in cyber incidents. I measure Internet penetration by the proportion of a country's population that use the Internet (World Bank, n.d)

Moreover, I can apply methods to reduce the problem of reverse causality between the independent and dependent variables. One explanation for the positive relationship between capabilities and incidents is that incidents are promoting the development of capabilities as a response to threat as the previous chapter explored. To account for this, I lag the incident variable so that each country's level of secure servers or possession of national CSIRTs or NCSSs is compared with a cyber incident occurring or not occurring in the subsequent year. A cyber incident cannot logically cause the creation of a national CSIRT in the previous year. By manipulating the causal sequence in this way, I can more accurately assess whether capabilities cause a change in cyber threat.

I use a logistic regression since the dependent variable is dichotomous and takes the value 1 (cyber incident occurred) or 0 (cyber incident did not occur). Because the secure server data is limited to the 2010-2016 period, I run a separate regression model where I exclude this factor in order to utilise the full time series available for the other variables. I run the models with robust standard errors clustered by country, and as previously explained I lag the cyber incident dependent variable by one year. This lagged variable tells us whether a cyber incident occurred one year ahead of the current observation.³³

Table 36 presents the results of the regression testing the effect of a country's defensive capabilities on the likelihood of a country being a victim of a cyber incident from a rival state. Model one excludes secure servers as an independent variable but includes national CSIRT, national cyber strategy, and Internet penetration. Model two includes all the explanatory variables.

³³ This removes the year 2016 from the analysis as there is no 2017 incident data to compare with 2016 observations.

Table 36.
Logistic regression of defensive capabilities and cyber incident occurrence³⁴ (2000-2016)

	(1)	(2)
Secure servers (per million) ³⁵		-0.056 (0.287)
National CSIRT	1.862*** (0.474)	1.683* (0.659)
NCSS	1.337*** (0.399)	1.635*** (0.484)
Internet penetration	-0.004 (0.010)	-0.001 (0.027)
Constant	-3.657*** (0.378)	-3.732*** (0.553)
Observations	1490	568
Pseudo R ²	0.163	0.158

Notes: Robust standard errors in parenthesis. Statistical significance at the 0.05, 0.01, and 0.001 levels denoted by *, **, and *** respectively

The findings demonstrate that the active capability indicators, CSIRT and NCSS remain positively associated with the occurrence of a cyber incident when controlling for other factors. In model 1, the coefficient associated with national CSIRT is statistically significant at the 99.9% confidence level ($\beta = 1.862$; $p < 0.001$) as is the coefficient associated with national cyber strategy ($\beta = 1.337$; $p < 0.001$). The creation of these capabilities and policies lead to an increased likelihood of the country suffering a cyber incident in the subsequent year.

In model 2 these factors remain significant, although the statistical significance of the national CSIRT variable is reduced ($\beta = 1.683$; $0.01 < p < 0.05$). Secure servers are predicted to reduce the occurrence of cyber incidents, but this finding is not statistically significant ($\beta = -0.056$; $p > 0.05$). Nevertheless, there is no evidence that defensive measures help to reduce the level of cyber aggression from rival states. Interestingly, Internet penetration is not significantly associated with cyber incidents when controlling for other factors, which is surprising given the widely held assumption that countries with greater dependence on the Internet are at greater risk of attack.

³⁴ Incident variable lagged 1 year

³⁵ To reduce skewness, this variable is log transformed.

Why would national CSIRTs and NCSSs lead to an increase in cyber incidents? It is hard to imagine there being a causal relationship between the implementation of these defensive efforts and an increase in cyber incidents. Despite accounting for reverse causality, it is likely that this issue still remains and that countries with NCSIRTs and NCSSs have created them in response to cyber threats that this data could not capture fully. The DCID incident dataset focuses on interstate, government sanctioned operations, and not the multitude of cyber-attacks that occur frequently on a daily basis. Moreover, countries likely create these capabilities because they have more assets and infrastructure to protect and face higher levels of cyber threat from actors targeting their well-developed industrial or banking sectors for instance.

Defensive capabilities and the success of cyber incidents

If capabilities do not reduce the frequency of cyber-attacks, can they reduce their success? The last part of this analysis assesses whether the incidents that have targeted a country vary in their outcome according to changes in defensive capability. To some extent, the occurrence of a cyber-attack already indicates that an attacker has had some effect against an opponent’s computer systems. However, I can assess this in more depth using another variable from the DCID that records:

“Whether or not the incident successfully achieved its objective; whether it breached the target’s network and fulfilled its intended purpose” (Valeriano, Jensen and Maness 2018, 217)

I use cross tabulations to show whether the proportion of successful incidents changes according to changes in the defender’s capabilities, the results of which are displayed together in table 37.

Table 37.
Defensive cyber capabilities and incident success

Secure Internet servers	Below median		Above median	
	<i>Number</i>	<i>%</i>	<i>Number</i>	<i>%</i>
Not successful	2	6.45	13	9.49
Successful	29	93.55	124	90.51
Total	31	100.00	137	100.00

$\chi^2 = 0.287$
 $p = 0.592$

<i>National CSIRT</i>	No CSIRT		CSIRT	
	<i>Number</i>	<i>%</i>	<i>Number</i>	<i>%</i>
Not successful	1	3.13	23	9.83
Successful	31	96.88	211	90.17

Total	32	100.00	234	100.00
-------	----	--------	-----	--------

$\chi^2 = 1.541$
 $p = 0.214$

<i>National Cyber Security Strategy</i>	No strategy		Strategy	
	<i>Number</i>	<i>%</i>	<i>Number</i>	<i>%</i>
Not successful	6	5.71	18	11.18
Successful	99	94.29	143	88.82
Total	105	100.00	161	100.00

$\chi^2 = 2.313$
 $p = 0.128$

For each indicator of defensive capability, the proportion of successful incidents decreases among countries with greater capability. For example, 93.3% of incidents were successfully among countries with below median secure servers but 90.51% successful among countries with above median secure servers. 96.88% of incidents were successful among countries with no national CSIRT but 90.17% successful among countries with a national CSIRT. Moreover, 94.29% of incidents were successful against countries without a national strategy but 88.82% successful against those that had a national strategy. Despite the correlation, however, none of the chi-square tests report a statistically significant relationship with all p -values well above the 0.05 level. Therefore, these results could have feasibly arisen by chance alone which suggests that defensive capabilities do not have an effect in reducing the success of rival countries in their cyber operations.

Discussion

In sum, increases in secure servers across a country, the government's implementation of a national cyber security strategy, or the creation of national CSIRTs do not reduce the frequency or success of cyber incidents against the state. Therefore, hypothesis 3 is confirmed. Active cyber capabilities for defensive purposes will not cause a reduction in cyber incidents against the defender.

Rather, the active capability indicators of defence are consistently associated with an increase in cyber threats. How should we make sense of these findings? Firstly, it is difficult to rule out a reverse causal relationship or a confounding relationship. Countries with these institutional developments have likely done so because they have more economic assets (banks, organisations, businesses) to be protective of in cyberspace. Also, countries may be reacting to cyber incidents not covered by the DCID but those from non-state actors or acts of cyber-crime that are not directed by governments. Despite efforts to account for the temporal sequencing and confounding variable of Internet penetration, it is likely that the causal relationship runs from enhanced cyber threat towards greater

efforts in capacity-building. The alternative explanation – that national CSIRTs and national strategies somehow cause an increase in cyber incidents – makes little sense.

Secondly, we should be aware that there are limitations to what these data can show. The success of cyber operations depends on the cyber security practices of the specific organisations that were targeted. Take the hack of the US Office of Personnel Management in 2015, for instance, where Chinese hackers were alleged to have stolen 21.5 million files of US government workers (Koerner 2016). The reason why the incident occurred was not only the offensive capabilities of the Chinese hackers, but the poor cyber security practices within the organisation, including a lack of two-factor authentication where users must undertake an extra step to access the system in addition to a username and password (Fruhlinger 2018). This analysis cannot provide data on these kinds of practices since they occur at an organisational level rather than a country level.

Another tool of defence not accounted for by the data is the ability of a government to reduce its dependence on the Internet or even completely isolate its national networks from the World Wide Web. For instance, Russia is reported to have successfully tested the separation of its own national intranet from the World Wide Web (Wakefield 2019), which is also a policy pursued by other authoritarian countries around the world like Iran as a means of reducing both external and internal cyber security threats (Sterling 2019; Singer and Brooking 2018, 89). While this may be an effective means of preventing or stopping the spread of computer network attacks, excessive Internet control clearly undermines human rights principles of freedom of expression online and so is not a preferable policy for democratic states committed to these ideals.

Furthermore, perhaps government-led cyber capability developments such as national strategies and CSIRTs will have an effect eventually on levels of cyber threat, despite having no observed effect in this analysis. After all, national strategies are a statement of intent regarding the implementation of cyber security policies rather than the current level of cyber security presently, and it might take time for these changes to take effect across society and across organisations. Similarly, it might take years for national CSIRTs to establish their collaborative networks and create a coordinated cyber security response across an entire country. Over a longer time-scale, maybe the effects of these developments will be observed.

Nevertheless, the findings demonstrate the difficulty in defending against computer network operations, despite government-led initiatives at building defensive capacity and despite levels of encrypted servers. Countries are able to carry out cyber operations against their rivals in spite of the capabilities of the defender, according to the proxies for defence used here. This supports the notion that resilience and recovery, rather than prevention, may offer a more sustainable cyber strategy as is being promoted by the EU (European Commission 2017).

The theoretical implication of these findings is that given the relative ease of attacking compared with defending, a state's opportunity and willingness to engage in cyber operations should increase. The next question to ask is if defensive capabilities do not reduce the incidence of cyber conflict, can the relative capabilities between a pair of states reduce cyber conflict through alternative deterrence mechanisms? To answer this, the next chapter assesses how different configurations in the balance of cyber capability among rival states, especially capabilities that could be employed for offensive purposes, influences the occurrence of cyber conflict.

CHAPTER IX

Capability and Conflict: The Effect of Capability Parity and Preponderance on Cyber Conflict

Introduction

The previous analysis showed that proxy indicators of defensive cyber capability did not lead to a reduction in the occurrence or success of cyber incidents. This chapter will further assess the relationship between capabilities and conflict but from the perspective of relative dyadic capabilities. In other words, how does the balance of capability between two states affect their level of engagement in cyber conflict? In doing so I test hypothesis 4: *Neither a preponderance nor balance of capabilities among two states will be associated with a reduction in cyber incidents between them.*

Anecdotally, there are cases where cyber-attacks occurred between a preponderant state against a weaker state in cyberspace. For instance, in 2007 Russia (ranked 8th in latent cyber capability) allegedly launched a series of DDoS attacks against Estonia (ranked at 58th) which disrupted the websites of banks, media, and government institutions for several weeks (Maurer 2018, 97). Estonia's relative weakness and inability to respond with its own cyber-attack could provide part of the explanation why a more powerful actor such as Russia felt it could carry out these actions. Russia might instead be deterred from initiating cyber conflict against a more powerful adversary.

It is possible that the United States and Russia, which are more equal in cyber capability, are currently seeking to deter one another in cyberspace. For instance, there have been reports that both governments have "implanted" computer viruses in each other's power grids that could be activated at will to cause widespread disruption (Perlroth and Sanger 2018; Sanger and Perlroth 2019). Mutual awareness of their offensive cyber capabilities could perhaps lead to a reduced risk of cyber conflict between them.

In this chapter, I investigate whether there are any general, observable trends in the international system between the relative cyber capabilities of countries and their engagement in cyber conflict. This will further build the case that intra-domain cyber deterrence is an unfeasible strategy. For realists, the balance of power is the main cause of war because states will either be discouraged or incentivised towards initiating war against their rival depending on how capable they are in comparison to their rival. As Singer and Geller (1993, 68-69) note, the relationship between relative power and war is one of the most recurring topics in international relations literature. This analysis

can show if there is a similar mechanism in cyberspace and therefore develop our understanding of the impact of cyber capabilities in international relations.

Before beginning my analysis, I revisit the theory and methods developed in earlier chapters. The analysis proceeds by assessing the bivariate relationship between relative latent cyber capability and conflict, and then between relative active capabilities and conflict. Next, I build a multivariate regression model which includes control variables for robustness. The findings confirm that the power preponderance or balance, and deterrence through punishment, perspectives are not a useful framework for understanding conflict.

Parity and preponderance

Two perspectives on the issue of relative capability and conflict were introduced in chapter 3. Balance of power theorists argue that a parity (balance) in capabilities will reduce the chance of conflict because each state will perceive victory to be less certain against an equally powerful rival and be deterred from initiating conflict (Wright 1964, Waltz 1979). Instead, conflict is more likely when one state is substantially stronger than the other because victory will be deemed to be more feasible for the stronger state against its weaker foe who will not be able to deter its stronger adversary.

Alternatively, power preponderance theorists argue that power balance increases the likelihood of war because both states perceive an opportunity for victory. In a condition of power preponderance (one state has substantially more capabilities), on the other hand, only the most powerful state has the capability to wage war but is more likely to be satisfied and have no need for war (Blainey 1973). Moreover, the likely outcome of war in such circumstances will be clearer to both states so there will be less need to go to war to find out and states are more likely to settle any disputes peacefully before it escalates to war. Most empirical evidence points towards conflict being more likely between equally capable states (Bremer 1992, 334; Geller 1993; Singer and Geller 1998, 72; Kugler and Lemke 1996; Bennett and Stam 2004, 125).

How does this relate to cyber conflict? When asking which pairs of states are most likely to engage in cyber conflict it may be worthwhile to consider how their relative capabilities will affect their incentives or disincentives for doing so. If one takes the balance of power perspective, two states that are that are equal in cyber capability such as China and the United States may be thought of as less likely to engage in cyber conflict because there is a fear of reprisal on both sides. On the other hand, two states where one is preponderant, such as Russia and Georgia, may be more likely to experience conflict because the more powerful state does not fear the reprisal of the weaker state. If one alternatively takes the power preponderance perspective, dyads where one state is preponderant

might be less likely to engage in cyber conflict because only one has the capability to conduct cyber operations. Dyads where there is a balance on the other hand might be more likely to engage in conflict because they both have the capability to conduct operations.

This debate implicitly draws on the idea of deterrence by punishment that I discussed in the theoretical framework. Deterrence by punishment suggests states can reduce cyber threats by building offensive cyber capabilities to signal the capacity to respond to a cyber incident by carrying out a retaliatory cyber operation. However, given the attribution and credibility problem, states are unlikely to be deterred by any rival in cyberspace regardless of their apparent level of capability. Aggressors know they can plausibly deny attacks thus avoiding retribution, and they have reason to doubt the efficacy of their opponent's ability to conduct a retaliatory cyber operation. Moreover, assessments of relative cyber capability are very difficult to make because of the nature of cyber weapons and the incentives towards secrecy.

The key variable instead is the opportunity to conduct attacks. Dyads where there is more overall capability should be more likely to engage in cyber conflict. The balance itself will not be important. I therefore expect to find that dyads where both countries have military CNO units (which could be thought of as a balance of active capability) will be more likely to engage in cyber conflict than dyads where only one or neither state has this capability because there is an increased opportunity. By the same token, the overall combined latent capability should be more important in explaining conflict than the balance.

Research Design

As I am interested in the capabilities that could be applied to offensive operations (i.e. those that could signal a deterrent threat), my independent variables here are different from the previous chapter. In this analysis I derive my explanatory variables from the data on military CNO units and latent cyber capability. Indicators like national CSIRTs or strategies are not useful as they cannot be employed in offensive operations.

My unit of analysis is the non-directed dyad year. This means that each observation in the dataset gives information on a pair of states in a given year regardless of which state initiated the cyber incident. At this level of analysis, the question is how the relative capabilities between two states impacts their propensity to engage in cyber conflict. When examining this question in relation to latent cyber capabilities, the question is how the relative balance (parity) or preponderance (inequality) of capability affects the occurrence of a cyber incident between the two countries.

When evaluating relative active cyber capabilities, which are measured by the presence or absence of a military CNO unit in this case, the question is how the occurrence of conflict is influenced by whether neither, one, or both countries in the dyad possess a military unit. This allows deterrence theory to be tested because the analysis accounts for the defender’s capabilities and thus its capacity to potentially dissuade cyber incidents from an aggressor.

The dependent variable in this analysis is the presence or absence of at least one cyber incident between a pair of rival states in a given year, using the DCID data (Valeriano and Maness 2014). The variable takes the value of 1 if at least one cyber incident was initiated in a given dyad-year, regardless of which state initiated it, and 0 if otherwise. Additional incidents between the same two countries in the same year are ignored. I am therefore explaining variation among rival dyads in whether they engage or do not engage in conflict in a given year. Table 38 shows the frequency of a cyber incident in a given year between rival dyads in the DCID.

Table 38.
Cyber incident occurrence among rival dyads (2000-2016)

Incident	Frequency	%
Yes	129	5.84
No	2,081	94.16
Total	2,210	100.00

The independent variables are measures of relative latent and active cyber capability. *Relative latent capability* is the ratio of the stronger state in the dyad’s capability by that of the weaker state, using the latent cyber capability index described in chapter 5.³⁶ This is the same method as many studies of conventional warfare (Bremer 1992; Oneal and Russett 1997; Barbieri 2002). The basic summary statistics for this variable for the 2,210 dyad year observations are shown in table 39.

Table 39.
Summary statistics for relative latent cyber capability

<i>Variable</i>	<i>Observations</i>	<i>Missing</i>	<i>Mean</i>	<i>Median</i>	<i>Std. Dev.</i>	<i>Min.</i>	<i>Max.</i>
Capability ratio	1,649	561	1.249	1.146	0.324	1	2.598

There are 561 missing values because of the missing latent capability data for several countries. The mean relative capability is 1.249 meaning that on average the stronger state has a capability score 1.249 times that of the weaker state. The minimum value is 1 in cases where both states have equal

³⁶ I divide the stronger state’s latent capability t score by the weaker state’s latent capability t-score.

capabilities, and the maximum is 2.598 reflecting the largest capability difference between a pair of states in the dataset. The median is 1.146 suggesting the data is skewed slightly towards large ratios.

Following a similar method to established research (Bremer 1992), for the bivariate analysis I recode this variable into three categories. I create the categories by first splitting the capability ratio variable into quartiles. Observations falling into the first quartile are coded as low capability difference (413 observations), those falling into the second and third quartile are coded as medium capability difference (824 observations), and those falling into the fourth quartile are coded as large capability difference (412 observations). This approach ensures that the variable is not based on arbitrary or subjective decisions but on the basis of a statistic.

The second independent variable is an ordinal variable for military CNO unit possession status. This take the value of 0 if neither country in the dyad has a military CNO unit, 1 if one country in the dyad has a unit, and 2 if both countries possess the unit. The proportion of dyad-year observations falling into each category are summarised in table 40. It shows that in 61% of rival dyads neither state has a military unit, and both states have a military unit in only 10.65% of dyads. There are 51 missing observations where the collection of military CNO unit data was not possible due to insufficient evidence.

Table 40.
Frequency table of military CNO unit status amongst rival dyads (2000-2016)

<i>Military CNO unit status</i>	<i>Observations</i>	<i>%</i>
Neither	1,328	61.51
One	601	27.84
Both	230	10.65
Total	2,159	100.00
Missing	51	

The discussion now turns to the bivariate tests between capability and conflict. Cross tabulations are used alongside conditional probability analysis to determine the size, direction, and statistical significance of the relationships.

Relative latent cyber capability and cyber conflict

In this section I investigate the bivariate relationship between the relative latent capability in a dyad and the occurrence of a cyber incident. Table 40 presents the results of the cross tabulation showing how the proportion of dyads that have small, medium, or large capability differences varies according

to whether the dyads have or have not experienced a cyber incident in a given year. The column percentages show the proportion of observations in each category of capability ratio that did or not did not experience an incident.

Table 41.
Relative latent cyber capabilities and incident onset among rival dyads (2000-2016)

<i>Cyber incident</i>	Low capability ratio		Medium capability ratio		High capability ratio	
	<i>Number</i>	<i>%</i>	<i>Number</i>	<i>%</i>	<i>Number</i>	<i>%</i>
Incident = 0	404	97.82	754	91.50	363	88.11
Incident = 1	9	2.18	70	8.50	49	11.89
Total	413	100.00	824	100.00	412	100.00

$\chi^2 = 28.418$
 $p = 0.000$

The chi square test statistic ($\chi^2 = 28.418$) reports a statistically significant p-value of 0.000 which means the difference between the expected and observed values within each category are unlikely to have arisen by chance. Dyads with low capability ratio (similar level of capability) are the least likely category to engage in cyber conflict. Only 2.18% of these dyads experienced a cyber incident. When capability ratio is at a medium level, 8.50% of dyads experienced cyber conflict. Dyads with a high capability ratio experienced cyber incidents 11.89% of the time. Although most incidents (70) have occurred amongst countries with a medium capability ratio, incidents are proportionally more likely amongst the rivals with the largest imbalance of cyber capability.

Another method of analysis is to calculate the conditional probabilities of a dyad engaging in a cyber incident based on the relative capabilities of the dyad. The baseline probability of a cyber incident is $128/1649 = 0.078^{37}$. A difference in proportions test shows the p-values, used to test the null hypothesis that there is no significant difference between conditional and baseline proportions. The added benefit of this method is showing which relative capability category variable is having a significant impact.

³⁷ The number of total observations has reduced here from the original 2210 because of missing data on the latent capability variable.

Table 42.
Conditional probabilities of cyber incident by relative latent capability

<i>Relative latent capabilities</i>	<i>Observations with cyber incident</i>	<i>Total observations</i>	<i>Conditional probability of incident</i>	<i>Z</i>	<i>p</i>
Small difference	9	413	0.021	-4.240	<0.000
Medium difference	70	824	0.085	0.786	0.432
Large difference	49	412	0.119	3.134	0.002

The results of table 42 show that dyads with a small latent capability difference have a conditional probability of 0.021 of experiencing a cyber incident which is significantly less than the baseline probability of 0.078 ($Z = -4.240$; $p < 0.000$). Dyads with a medium capability have an increased probability in experiencing a cyber incident but this result is not statistically significant ($Z = 0.786$; $p = 0.432$). Dyads with a large difference in capability have a probability of 0.119 of experiencing a cyber incident which is significantly greater than the baseline probability of an incident ($Z = 3.134$; $p = 0.002$).

These results support the notion that states with a parity (small difference) in capability will be the least likely to experience cyber conflict and dyads where there is a preponderance of capability are most likely. Perhaps conflict is most likely among dyads where one country is superior because the attacking state is undeterred and emboldened against a weaker rival. Moreover, perhaps conflict is least likely amongst countries with an equal balance of capabilities because these countries are deterring one another given their parity in capability.

However, this assumes two conditions that this analysis cannot uncover. First, that the stronger state was the state that initiated the cyber incidents – since it was presumably undeterred. The relationship between one state’s capabilities and the likelihood of initiation will be examined more fully in the next chapter, but by examining some individual cases we can get a preliminary idea of what is going on.

It is notable that all of the dyads which include the United States are classified as preponderant dyads where the United States has substantially greater cyber capability than its rival. These include some of the most conflict-prone dyad pairings: US - China (48 incidents), US - Russia (26 incidents), and US - Iran (20 incidents). Out of the 266 cyber incidents recorded between rival states by the DCID, 103 of these have included the United States as either a victim or initiator. Of these, the US was the victim in 82 (79.6%) cases and was the initiator in only 21 (20.4%) of cases. This shows that the United States is most often not the initiator of cyber conflict despite being the more capable state. This suggests that cyber conflict is not driven by the relative strength of the initiator compared with its rival. Moreover, this undermines the logic of power preponderance theory when applied to the

cyber domain which would predict that power preponderant dyads are more conflict-prone because the more powerful state is undeterred.

The second problem with the finding that dyads of power parity are least conflict-prone, is that it assumes that states under this category possess sufficient capabilities to be able to conduct computer network operations in the first place. Countries with a relative balance of capability may engage less in conflict not because they deter one another but because they have equally low levels of capability.

This is confirmed by figure 22. Pairs of states that have a small difference in capabilities (most equal capabilities) have on average a combined capability t-score of 101.48. Those in the medium difference category have an average combined capability score of 109.43 and those in the large difference category have an average score of 135.21. Therefore, rivals with a small difference in capabilities also tend to have a small overall level of capabilities. The finding that these countries are associated with a lower likelihood of cyber conflict could therefore be explained not by deterrence logic but by the fact that these countries have less capabilities and therefore less opportunity to carry out computer network attacks against their rivals.

Dyads where there is a preponderance of capabilities on the other hand tend to have more combined capability. Their increased likelihood towards conflict may be explained not by the lack of deterrence but because there is more capability and more opportunity to engage in conflict overall in these states.

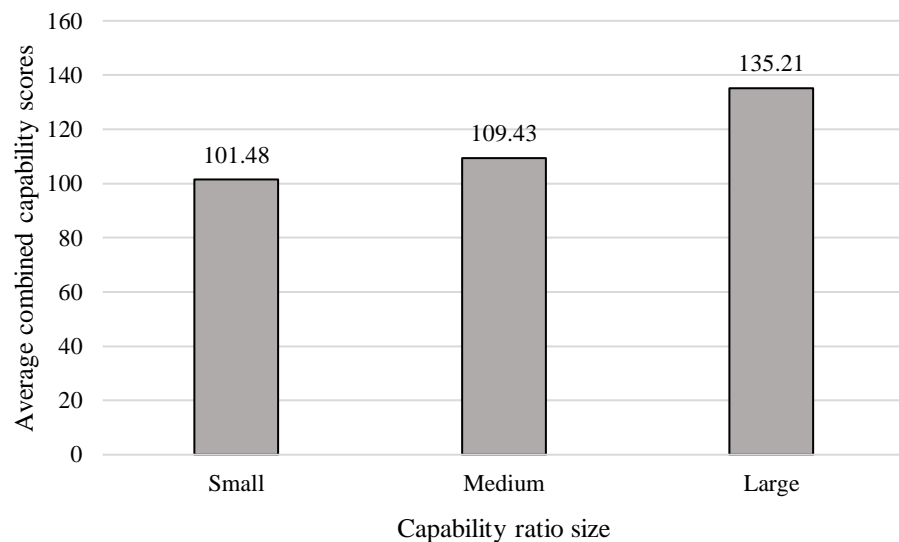


Figure 21. Average latent capability index by dyadic capability ratio size

This finding is confirmed statistically in the cross tabulation in table 43. It shows that there is a significant difference in combined capability between states with a parity and preponderance of

power. 22.28% of dyads with low capability ratio have above median combined capability, 43.92% of dyads with medium capability ratio have above median combined capability, and 90.05% of dyads with high capability ratio have above median combined capability. The chi-square reports a statistically significant difference between expected and observed counts in each cell ($\chi^2 = 403.432$; $p = 0.000$). The increase in conflict between power preponderant dyads therefore has more to do with the increased levels of capability among these countries than a calculation based on relative power.

Table 43.
Combined capability and relative capability among rival dyads (2000-2016)

<i>Combined latent capability</i>	Low capability ratio		Medium capability ratio		High capability ratio	
	<i>Number</i>	<i>%</i>	<i>Number</i>	<i>%</i>	<i>Number</i>	<i>%</i>
Below median	321	77.72	462	56.07	41	9.95
Above median	92	22.28	362	43.92	371	90.05
Total	413	100.00	824	100.000	412	100.00

$\chi^2 = 403.432$
 $p = 0.000$

These findings are unsurprising. Deterrence requires the presence of credible threat, but latent cyber capability is non-material in nature and therefore does not signal an observable threat to potential aggressors. Perhaps instead the establishment of military units dedicated to computer network operations such as Cyber Command in the US, or the Strategic Support Force in China offers a more visible form of capability that could create a deterrent effect. The next part of the analysis will explore this possibility.

Relative active cyber capability and cyber conflict?

In this analysis, I examine how the mutual possession of military CNO units among dyads affects the occurrence of cyber conflict. This indicator might be more strongly related to deterrence than latent capability because it is more observable and can be used to signal capability. Applying power parity and preponderance theories to this indicator creates two possible scenarios. The balance of power perspective would suggest that cyber conflict should decrease between states that both possess a military CNO unit since both countries have the capacity to deter one another. The power preponderance perspective on the other hand would suggest that cyber conflict will be more likely when only one state possesses this capability, because it will be undeterred against its weaker rival.

The cross tabulation in table 43 shows the number and proportion of cases where a cyber incident occurred or did not occur according to whether neither, one, or both countries had a military CNO unit in a given year.

Table 44.
Relative active cyber capabilities and incident onset among rival dyads (2000-2016)

<i>Cyber incident</i>	No CNO unit		One CNO unit		Both CNO unit	
	<i>Number</i>	<i>%</i>	<i>Number</i>	<i>%</i>	<i>Number</i>	<i>%</i>
Incident = 0	1322	99.55	556	92.51	158	68.70
Incident = 1	6	0.45	45	7.49	72	31.30
Total	1328	100.00	601	100.00	230	100.00

$\chi^2 = 352.31$
 $p = 0.000$

The results show a very strong positive relationship between mutual CNO unit possession and cyber incident occurrence. Only 0.45% of dyads where neither state has this capability engaged in a cyber incident and 7.49% of dyads where one state had this capability initiated a cyber incident. When both states possess a military CNO unit, however, the increase in the proportion of dyads engaging in cyber conflict jumps to 31.30%. The chi-square test suggests this is a statistically significant relationship ($\chi^2 = 352.31$; $p = 0.000$).

Table 45.
Conditional probabilities of cyber incident by relative active capability

<i>Relative active capabilities</i>	<i>Observations with cyber incident</i>	<i>Total observations</i>	<i>Conditional probability of incident</i>	<i>Z</i>	<i>p</i>
No CNO unit	6	1328	0.005	-8.371	<0.000
One CNO unit	45	601	0.075	1.726	0.084
Both CNO unit	72	230	0.313	16.474	<0.000

Table 45 assesses this relationship in terms of conditional probabilities. The unconditional probability of a cyber-incident occurring in any year from 2000 to 2016 between rival dyads is 0.058. These results show that the probability of an incident falls from 0.058 to 0.005 when neither country in the dyad has a military CNO unit and this is statistically significant ($Z = -8.371$; $p < 0.000$). One obvious explanation is that neither rival has the capacity to conduct a successful cyber operation against the other.

When one country has a CNO unit the probability increases to 0.075 but the result is not statistically significant ($Z = 1.726$; $p = 0.084$). This suggests that power preponderance in active capabilities has no effect in deterring cyber conflict.

The probability of a cyber incident increases substantially to 0.313 when both countries have a CNO unit. This is significantly greater than the baseline probability of 0.058 ($Z = 16.474$; $p < 0.000$) and shows that cyber conflict is much more likely when countries both possess military cyber capabilities. The findings undermine the deterrence-based logic that mutual possession of capabilities can prevent conflict. The presence of more capabilities makes conflict more likely, and the absence of any capabilities makes conflict less likely.

Multivariate analysis

In this section I describe the results of a multivariate model which can identify whether the bivariate relationships persist, through the addition of control variables and other robustness checks. The aim of this model is not to build an exhaustive explanation of the cyber conflict, but to ascertain whether there is any robust association between the dyadic balance of capabilities and conflict onset. I first summarise my methods again that were first explained in chapter 5 and then discuss the results.

The regressions are run on a non-directed dyad year dataset with 2210 observations. To gauge the onset of cyber conflict, the dependent variable is the occurrence of at least one cyber incident between a pair of rival states in a given year. My two independent variables measure latent and active relative cyber capabilities to test whether a preponderance or balance of capability is linked to conflict. *Relative latent cyber capability* is measured by the ratio of the stronger state's latent cyber capability t-score to that of the weaker state. *Relative active cyber capability* is measured with a categorical variable where a value of '0' indicates that neither state has a military CNO unit, '1' indicates that one of the states has a military CNO unit, and '2' indicates that both of the states have a military CNO unit.

The problem of reverse causality in relation to the military CNO unit variable is accounted for by lagging this variable by one year. As chapter 7 showed, external threat environment was positively correlated with the development of military CNO units. It is therefore possible that rather than CNO units causing cyber incidents, cyber incidents against the state cause the creation of military CNO units. To ensure the correct temporal sequencing, I lag the military CNO unit variable by one year so that each incident or non-incident is being compared with the military CNO unit possession of the previous year.

Building on the previous chapter, I also include indicators for the mutual possession of defensive cyber capabilities to determine if they have an impact at reducing conflict at the dyadic level. The variables *both have national CSIRT* and *both have NCSS* take a value of 1 if both countries have these assets and 0 if otherwise.

I control for *rivalry intensity* in a dyad by adding a variable for the total number of MIDs they have engaged in between 2000 and 2010. Conflict-prone states may be more likely to build capability and engage in cyber conflict. I control for *joint democracy* by obtaining the polity scores for each state which range from -10 (most autocratic) to 10 (most democratic). Using the same methodology as Bremer (1992, 324), I consider a state to be democratic if its polity score is greater than or equal to 5 and then code a dyad as being jointly democratic if both states meet this threshold, and not jointly democratic if otherwise. Pairs of democracies may be more likely to develop capability and refrain from cyber conflict. Furthermore, I control for *joint major power status* under the assumption that major powers might be more war prone. This takes a value of 1 if both countries are major powers under the Correlates of War classification.

Quantitative studies on the causes of dyadic conflict usually add a series of *peace year* variables into the regression to control for temporal dependence between instances of conflict. Rather than being independent events, previous instances of cyber conflict, like conventional conflict, are likely correlated to the future occurrence of conflict because they are part of a series of hostile interactions between rivals. This violates the logistic regression assumption of independence of observations. This is dealt with by adding the number of years the dyad has been at peace and its squared and cubed versions, under the assumption that the longer there is peace the less likely an incident will occur (Beck, Katz and Tucker 1998). I include a peace years variable counting the number of years since the WWW was invented that there was an absence of cyber conflict and include its squared and cubed terms. All regressions are run with robust standard errors clustered by dyad to account for heteroscedasticity.

Results

Table 46.
Logistic regression of relative capabilities and cyber conflict among non-directed dyads (2000-2016)

	(1)	(2)
Latent capability ratio	0.291 (0.581)	
One CNO unit		1.643*** (0.489)
Both CNO unit		1.970*** (0.504)
Both national CSIRT	0.189 (0.338)	0.145 (0.356)
Both national strategy	0.273 (0.400)	0.162 (0.421)
Rivalry intensity	0.133* (0.062)	0.129* (0.0629)
Both democratic	-0.955 (0.532)	-0.610 (0.528)
Both major powers	0.513 (0.359)	0.427 (0.331)
Peace years	-0.528*** (0.151)	-0.512** (0.165)
Peace years ²	0.030 (0.017)	0.0288 (0.0178)
Peace years ³	-0.001 (<0.001)	-0.001 (<0.001)
Constant	-0.592 (0.449)	-2.188*** (0.525)
Observations	1641	2032
Pseudo R ²	0.373	0.419

Notes: Robust standard errors in parenthesis. Statistical significance denoted by * p<0.05, ** p<0.01, and *** p<0.001.

The results of two logistic regression models are highlighted in table 46. Model one uses latent capability as the key independent variable and model two uses active capability. These are separated because active capability is likely a mediating variable between latent capability and conflict their inclusion in the same model might create misleading findings. Moreover, there is more missing data on the latent capability variable and since Stata deals with missing data on any variable through listwise deletion (excluding whole rows of observations), the inclusion of latent capability in the same model could reduce the explanatory power of the other variables.

Although the bivariate tests suggested cyber conflict was most likely among dyads where there was a large imbalance between the stronger and weaker state, Model 1 shows that the latent capability ratio has no effect on the likelihood of a cyber incident, when controlling for other factors ($\beta = 0.291$; $p > 0.05$). When predicting the occurrence of cyber conflict, the balance of capability in terms of programming skill and computer science knowledge provides little to no information.

Model 2, however, shows that the likelihood of a cyber incident is statistically greater when either one state or both states in the dyad possess a military CNO unit, compared to no states. The impact is largest when both states have a military CNO unit ($\beta = 1.970$; $p \leq 0.001$). This suggests that the mutual possession of military capabilities increases conflict. Moreover, this holds when controlling for joint democracy, and rivalry intensity, and major power status. Given that this variable has been lagged a year so that the incidents are preceded by CNO units, it gives more certainty to the notion that capabilities drive conflict. Confirming the findings of the previous chapter, mutual possession of national CSIRTs and strategies do not have any significant effect on conflict.

Given that a preponderance of CNO unit and mutual possession (balance) of CNO unit both increase the probability of conflict from its baseline level, it suggests that neither the preponderance or balance of power perspectives are explaining the relationship between capability and conflict well. What matters is how many states possesses a military CNO unit, as this provides the capacity to conduct computer network operations.

As for the effect of the control variables, rivalry intensity, as measured by the total number of MIDs experienced by each dyad over a ten-year period is associated with an increase in the likelihood of cyber conflict at a statistically significant level in both regression models ($\beta = 0.129$; $0.01 < p \leq 0.05$). This supports the notion that rivals engaged in a greater degree of competition and conflict are more likely to use cyber tools against one another also.

Joint democracy has a negative coefficient in both models, but they do not reach a statistically significant level. Undermining democratic peace theory when applied to the cyber domain, states that are both democratic are not less conflict-prone, when controlling for other factors. Joint major power status also has no significant, independent effect.

To give intuitive interpretation of these results, Figure 23 illustrates the substantive impact of CNO unit status on the predicted probability of a cyber incident, while keeping all other variables at their mean levels.³⁸

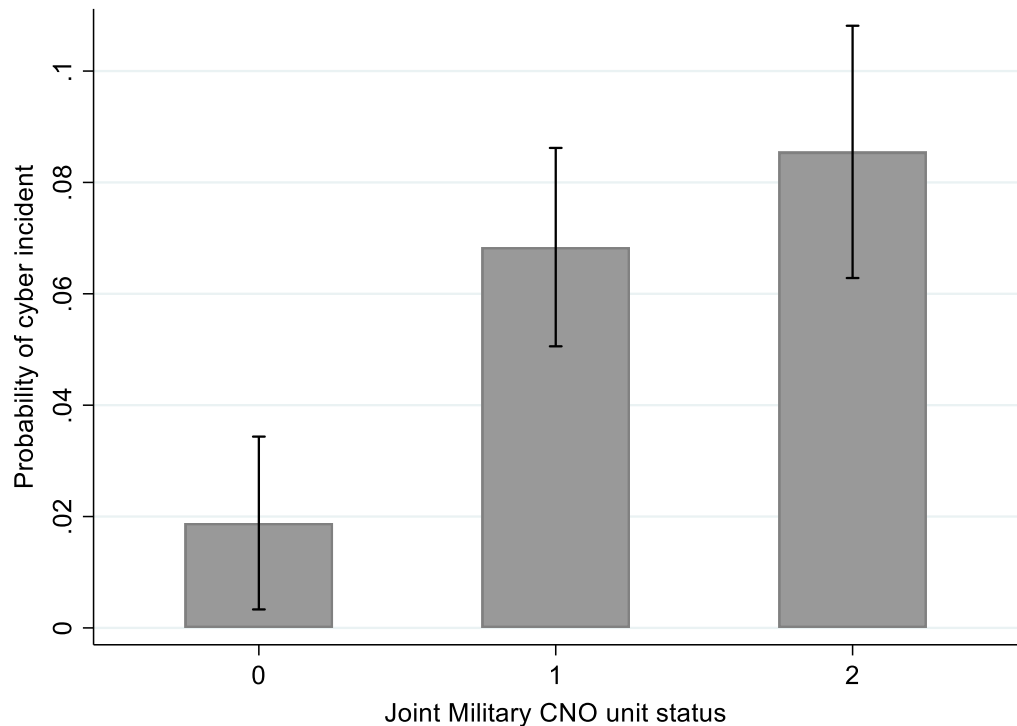


Figure 22. Substantive impact of dyadic military CNO unit possession on cyber incident occurrence³⁹

Cyber incidents become substantially more likely as more countries in a dyad adopt a military CNO unit. The predicted probability of a cyber incident when neither country has a unit is less than 0.02, which increases to around 0.07 when one country possesses a unit. When both countries have this capability, the probability of a cyber incident increases further to 0.09, meaning that a cyber incident is expected to occur in almost one in ten of such cases.

Discussion

Hypothesis 4 as set out in chapter 3 is confirmed. Neither the preponderance nor balance of relative capabilities is associated with a reduction in cyber incidents between states. In fact, relative

³⁸ Using the results from regression model 2

³⁹ Vertical bars highlight the 95% confidence intervals. I.e. We can be 95% sure that the actual probability falls within these limits.

capabilities are of little use for understanding cyber conflict. While the bivariate tests suggested that conflict increased when there was a disparity in power, this comes about because preponderant dyads tend to have more latent capability on the whole. Moreover, relative latent cyber capability had no impact on cyber incidents when controlling for other factors in a multivariate regression model. In terms of active capability, conflict is not deterred by either an imbalance of military CNO unit possession or equality in mutual CNO unit possession. Rather, conflict increases the more states in the dyad possess a military CNO unit.

The findings undermine deterrence through punishment. If countries develop military cyber units to threaten their rivals and prevent being attacked, it is certainly not having this effect. A pair of rival states, both with military CNO units, do not deter one another – they are in fact significantly more likely to carry out operations against one another. Active capabilities therefore seem to promote rather than deter conflict. States will likely try to harass their rivals in cyberspace regardless of their relative capability relationship. The reason for this is the failure of deterrence through a lack of credible threat posed by cyber capabilities.

Opportunity-Willingness Theory has more predictive capacity. It is not the balance or preponderance that dictates the initiation of conflict, but the number of countries that have the capacity to carry out operations. As more countries adopt cyber capabilities, there is greater opportunity to carry out operations, and thus its likelihood increases.

There is also evidence that rivalry promotes conflict. This analysis was performed on rival states so they all presumably had the willingness to conduct CNO against one another. But an alternative measure of rivalry intensity based on the level of conventional disputes was positively and significantly associated with cyber conflict suggesting that the level of hostility between states outside the cyber domain will influence the willingness to conduct computer network operations. Opportunity and willingness therefore can be applied to the engagement in cyber conflict as well as the proliferation of capabilities.

A problem with the non-directed analysis is that we cannot distinguish the capability or the political willingness of the attacker from the defender. In the next analysis I use a directed-dyad dataset to assess how the capability of the initiator affects the occurrence of conflict and further investigate the willingness side of the debate that conflict is promoted by the rivalry perceived from the initiator against the target.

CHAPTER X

Capability and Conflict: The Initiator's Capability and Cyber Conflict

Introduction

So far in the analysis on the effect of capabilities on conflict, I have shown that neither a state's defensive capabilities nor the relative latent capabilities between two states have a significant impact on limiting cyber conflict. This suggests decisions to initiate conflict are clearly not shaped by the defensive capabilities of the target or of the balance of capabilities between conflicting states. The analysis instead suggests that conflict is promoted by increases in capability. In this chapter I investigate this issue further by testing the relationship between a state's capability and its initiation of cyber conflict. This will test hypothesis 5: *As the capability of the state increases it is more likely to conduct cyber operations against another state.*

I expand my theoretical framework of opportunity and willingness to cyber conflict by first providing evidence that rather than deter conflict, cyber capabilities (that could be employed towards offensive computer network operations) makes cyber conflict more likely by increasing the opportunity for action. In particular I am interested in the initiator's capabilities rather than relative capabilities, and I argue that the more capabilities a country has the more likely it will initiate cyber incidents against its rival, regardless of the defender's capabilities.

Yet, this is only one side of the theory. Chapter 7 showed that the adoption of active cyber capabilities was determined not just by the state's latent capability but by its external rivalry environment. The same might be true for the initiation of cyber incidents. States are enabled by their capabilities and motivated by their external relations with other states. Pairs of countries that have a more intense rivalry should be more likely to engage in cyber conflict than dyads that are less conflictual. This was summarised by hypothesis 6 in the theoretical framework: *Rivalry intensity will increase the likelihood of cyber conflict.*

I first proceed through bivariate tests of the relationship between a state's cyber capability and the initiation of cyber incidents, then bivariate tests of rivalry intensity on conflict. Then I build a multivariate regression model to determine the robustness of the findings. Finally, I assess whether capabilities have an impact on the severity of cyber incidents, as well as frequency.

System level capabilities and the initiation of cyber incidents

If capabilities promote conflict, then one should observe a high frequency of cyber incidents when total system-wide capabilities are at greater levels. If on the other hand, cyber deterrence is effective at the global level, then greater levels of capability internationally should not be associated with an increase in the frequency of cyber-attacks. If cyber-attacks are more frequent when capabilities are higher, it would suggest capabilities are failing to deter conflict.

The system level of analysis can show how aggregated cyber capabilities in the international system relate to the occurrence of cyber conflict in a given year. Since the unit of analysis here is the system-year and the only variance is over time, I am limited to just 17 data points – one for every year from 2000 to 2016. The dependent variable here is the number of cyber incidents initiated by states that have rivals, of which there are a total of 96.

My independent variables are the latent capability and active capabilities that could be applied towards offensive cyber operations. The latent capability indicators are computer science knowledge, measured by the total number of computer science journal articles published annually, maths and computer programming skill, measured by the total number of medals won annually at the International Olympiad of Informatics and International Olympiad of Mathematics, and the size of the global software industry, measured by the number of established companies.⁴⁰ The indicator of active cyber capability is the total number of states that possess a military CNO unit as of that year.

I conduct the analysis using line graphs to plot the relationship between capabilities and the number of cyber incidents and through correlation analysis. This system level analysis is limited as it cannot gauge the characteristics of specific countries or pairs of countries, just that of the international system taken as a whole. Furthermore, this analysis can only establish a bivariate correlation, not a causal link. In the later multivariate analysis, the causal link can be further examined with the additional of control variables and temporal ordering of variables. Nevertheless, I carry out the analysis while acknowledging the limitations to get a preliminary understanding of what the available data suggests.

Figures 24 to 27 show the changes in capabilities and incidents from 2000 to 2016. The overall number of cyber incidents has increased across this time period, although with a substantial fluctuation including a notable fall in 2012, rising again in 2014, and falling again thereafter. The level of capabilities in the international system increased more consistently over this time. To provide

⁴⁰ The latent capability index, which compares each country's programming knowledge and computer science knowledge to all other states, is not suitable for this analysis because it is not an indicator of cumulative resources in the international system at a given point in time. For this reason, I use the individual components of latent capability.

a measure of the statistical relationship between capabilities and incident onset, table 47 also gives the correlation coefficients between each variable and the number of cyber incidents.

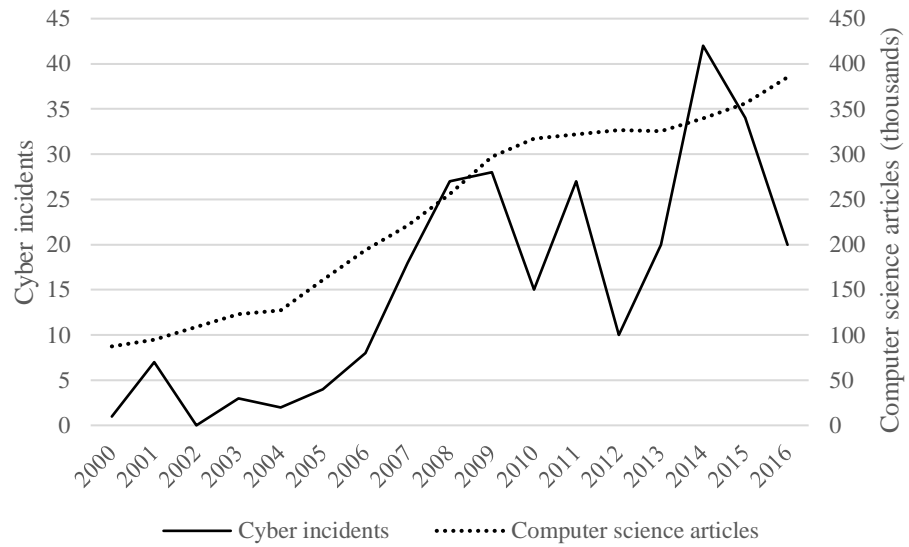


Figure 23. Computer science articles and incident frequency, 2000-2016

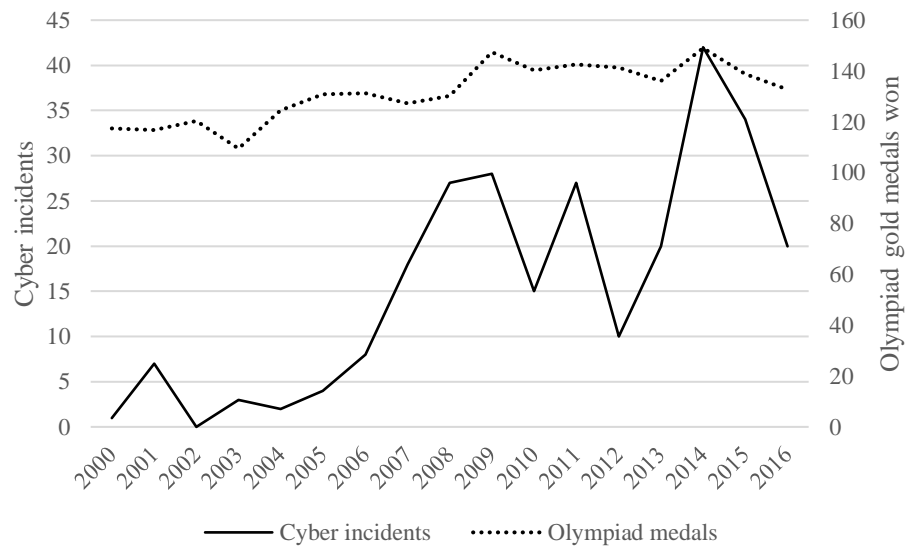


Figure 24. IMO and IOI medals and incident frequency, 2000-2016

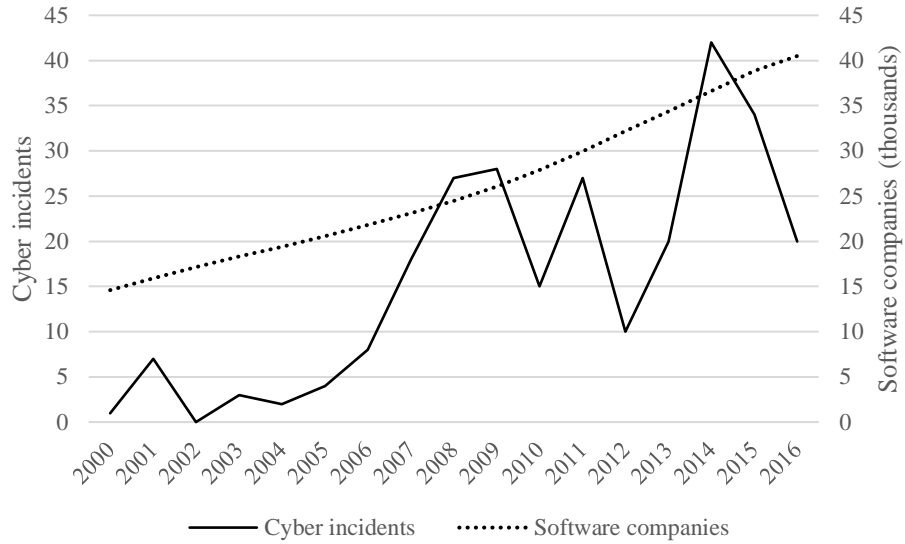


Figure 25. Software companies and incident frequency

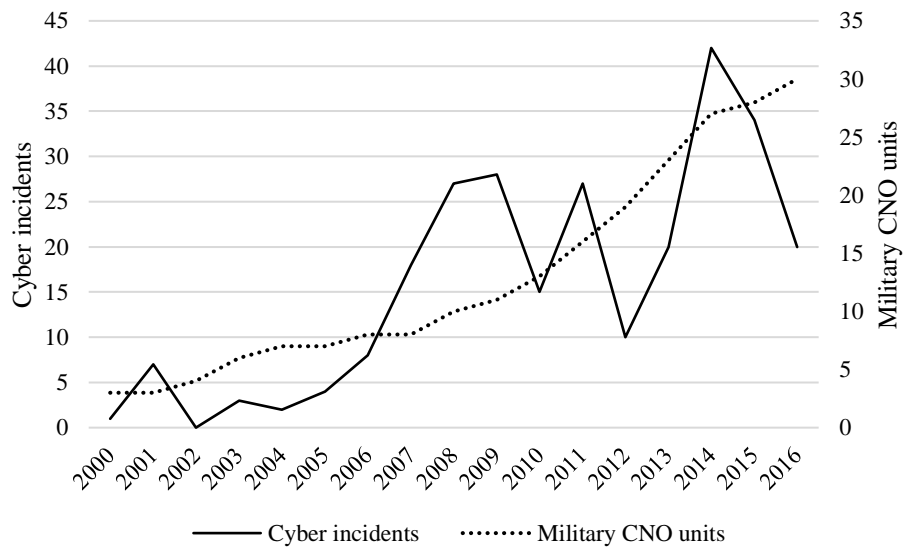


Figure 26. Military CNO unit countries and cyber incidents, 2000-2016

Table 47.
Correlations between capabilities and incident frequency, 2000-2016

<i>Variable</i>	<i>Correlation</i>	<i>Observations</i>
Computer science articles	0.797	17
Olympiad medals	0.764	17
Software industry	0.760	17
CNO unit countries	0.727	17

The correlations suggest a strong and positive relationship between latent capabilities and conflict in cyberspace. Computer science articles have the strongest correlation with a coefficient of 0.80. It is

possible that the expansion of scientific knowledge relating to computer processes has enabled the proliferation of cyber conflict as more states have learnt how to conduct computer network operations. There is also a strong positive correlation (0.78) between Olympiad medals and cyber conflict. One potential explanation is that increases in skill in computer programming and mathematics has given states greater opportunity to apply this expertise in cyber operations. The growth of software industry is correlated at a level of 0.76 with the number of incidents. This could be because as industry has grown, technology and expertise has diffused in the international system enabling states to conduct cyber operations.

Turning to active cyber capabilities, the results show a moderate to strong positive relationship between CNO units and incidents (0.73), suggesting that the proliferation of military cyber capabilities are a potential driver of cyber conflict since they create more opportunity to carry out operations. However, it is possible the relationship could run reverse in that the escalation of cyber conflict has motivated the build-up of military units as a defensive response to increased threat, rather than capabilities increasing the rate of cyber incidents. Nevertheless, it suggests that the proliferation of military operations capability has not led to a reduction in cyber conflict through deterrence mechanisms.

The aggregate cyber capabilities in the international system in a given year are strongly and positively correlated with the number of incidents. Capabilities therefore may be a driving factor for the increase in cyber incidents, which fits with the theoretical argument that capabilities are an enabler of cyber operations. However, there is not much else that can be concluded from this analysis. The results could be spurious if there is a third confounding variable, perhaps also associated with time, that has a causal impact on incident frequency. The system level of analysis is also limited as it provides very few data points, and thus less statistical certainty, and does not provide any information on the characteristics and behaviour of specific countries or pairs of countries involved in cyber conflict.

The initiator's capability and the frequency of cyber incidents

An alternative way to test the research question is to compare each country's capability with the total number of cyber operations it has conducted. If the relationship between capabilities and conflict is strong, we should observe a higher frequency of cyber incidents conducted among countries that have more capability.

Greater levels of latent capability should increase the state's opportunity to initiate cyber incidents because it gives the state more technical expertise to successfully conduct a computer network operation. The state need not necessarily have translated its latent capability into a military operations unit before it initiates a cyber incident since the state may rely on a proxy actor or its intelligence

agencies to launch cyber operations. Nevertheless, states that have established military operations units should also have initiated cyber incidents at a higher frequency than states without these units, because they are more likely to possess the organisational capacity to engage in computer network operations. Again, since cyber-attacks need not originate from a military unit, they are not a necessary condition for the initiation of a cyber incident, and we may expect some states without military units to have engaged in cyber operations. Nevertheless, I expect that on average, states with these organisations to have initiated more incidents than other states.

The dependent variable is the number of cyber incidents initiated by a state against a rival across the entire period (2000-2016) which are drawn from the DCID dataset (Valeriano and Maness 2014). Latent capability is the first independent variable, measured by the combined Olympiad skill and computer science knowledge variables converted to t-scores. A value less than 40 corresponds to below average capability amongst all countries in that year and a value greater than 40 corresponds to above average capability. As this is cross sectional design, I take a country's capability information from the median year, 2008.

Figure 28 highlights the relationship between each country's latent capability and the number of cyber incidents it has initiated in a scatter plot with a line of best fit to indicate the direction and size of the relationship. The line of best fit indicates that the relationship is positive although the pattern of data does not show a strong relationship as data points are scattered quite randomly. To quantify the statistical association, table 48 shows that the correlation between these variables is 0.47 which can be interpreted as a weak, yet positive correlation.

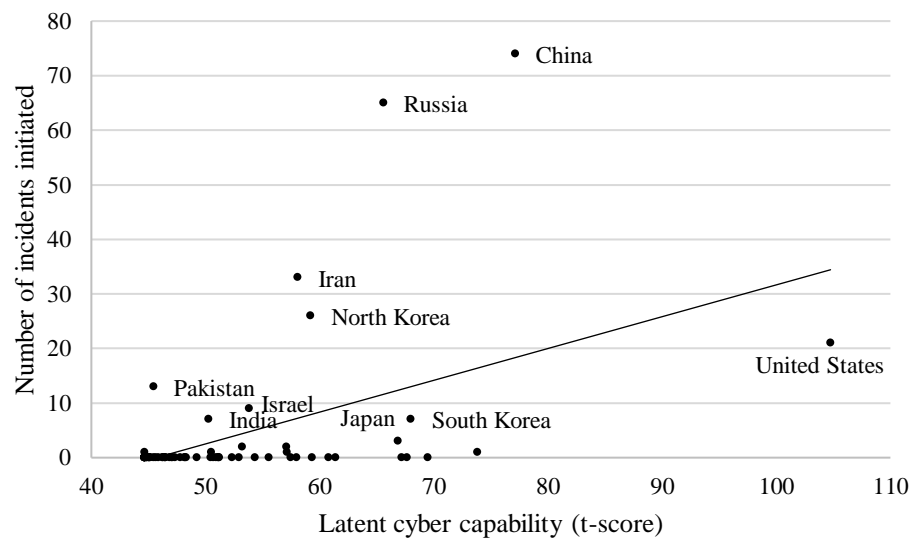


Figure 27. Scatter plot of latent cyber capability and incident initiation (2000-2016)

Table 48.
Correlation between latent cyber capability and number of cyber incidents initiated (2000-2016)

<i>Variable</i>	<i>Correlation (-1 to 1)</i>	<i>Observations</i>
Latent cyber capability t-score	0.47	73

The presence of several outliers suggests that latent cyber capability is not a very reliable predictor of a state's total initiations of cyber operations. Despite being the most capable state in cyberspace, the United States has shown relative restraint whereas states like Russia and China with less cyber capability have initiated many more cyber incidents. Some countries such as Japan or South Korea are also outliers given that they have relatively high capability yet have initiated few cyber incidents. Just because a state has high skill and knowledge does not mean it will conduct cyber operations with high frequency. Pakistan is an outlier in the alternative sense that it has very low latent capability but has engaged in relatively high levels of offensive activity, suggesting that certain countries may not derive their capability from the skill and knowledge in society and may outsource cyber weapons and techniques. Moreover, the majority of countries in the dataset have never initiated a cyber incident despite a large variation in capability amongst these countries.

There are clearly other explanations for conflict frequency aside from capability which could include how restrained a country is by its domestic political structure or motivated by its geopolitical interests. These will be assessed later in this chapter.

For now, I turn to the relationship between active capability, as measured by the presence of a military CNO unit, and cyber incident initiations. Perhaps there will be a stronger relationship here if a military CNO unit signifies a maturation in the capability to carry out computer network operations. I compare the distribution of cyber incidents initiated between countries with military CNO unit and countries without them (as of 2016) using a density plot in figure 29.

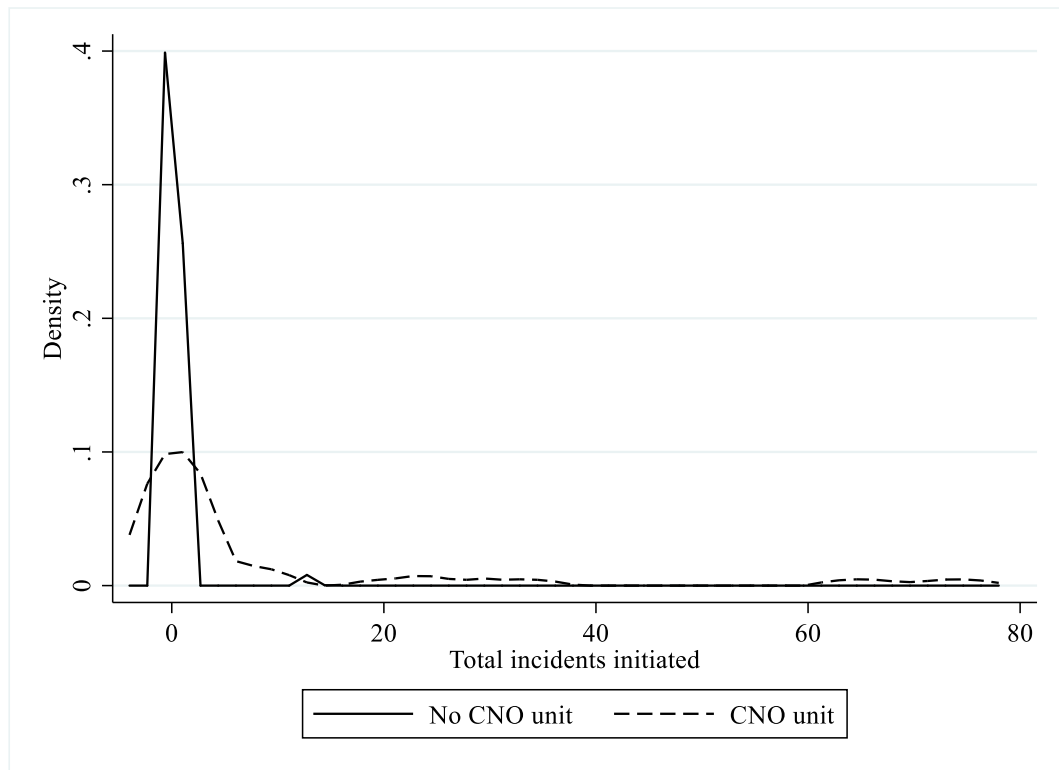


Figure 28. Density plot of cyber incident initiations by CNO unit status

The results demonstrate that most observations of countries lacking a CNO unit lie in the low end of the incident initiation scale. Countries with this active capability on the other hand are more evenly distributed along the x-axis, suggesting they initiate on average greater numbers of cyber incidents.

A cross sectional design (no yearly information) is not very informative with the CNO unit variable because there is no information about when the incident occurred or the CNO unit was created. The cyber unit may be created after a country initiates a cyber-attack and therefore cannot be thought of as a cause of the conflict, despite the correlation. The research question cannot be fully explored using these methods. The cross-sectional nature of the dataset means we are lacking information about when capabilities were established or increased and when cyber incidents took place.

The initiator's capability and the likelihood of cyber incidents

The relationship between capabilities and total incidents is weak yet positive. Rather than compare capabilities with total incidents, I conduct the next analysis by asking instead whether capabilities influence the likelihood of a cyber incident being initiated by one state against a rival in a given year.

I utilise a directed dyad dataset for this purpose because it allows me to incorporate information on cyber incidents between two states as well as on the capabilities of a potential initiator. According to Bennet and Stam (2003) “a directed dyad-year is a pair of states in a given year, observed from the

perspective of one of the two states.” Rather than there being only one observation per dyad-year (for instance, United States – Russia 2010), in the directed dyad data set there are two observations per dyad-year (United States – Russia 2010, Russia – United States 2010), where each state is observed once as a potential attacker and once as a potential defender. The directed dyad level of analysis therefore allows the researcher to observe country-specific characteristics as well as dyadic characteristics. Moreover, I use the full time series range of the dataset allowing me to identify relations that exist across time as well as space.

I first determine if a state is more likely to initiate a cyber incident if it has greater latent capability than its rival. According to deterrence theory, a state will be less likely to initiate a cyber incident if its rival has greater capabilities than it as it will be either threatened by punishment or expect not to make worthwhile gains. Relative latent capability is measured by dividing the potential initiator’s latent capability index value by that of the potential defender. For the bivariate analysis I recode this into a dichotomous indicator taking the value of 0 if the initiator has greater latent capability than the defender and 1 if the defender has a greater latent capability than the initiator.

The cross tabulation of table 49 shows how the initiation of cyber-attacks varies according to whether the potential initiator has higher or lower latent capabilities than its rival.

Table 49.
Initiator/defender preponderance in latent capability and incident initiation

<i>Cyber incident by initiator</i>	Initiator has more capability		Defender has more capability	
	<i>Number</i>	<i>%</i>	<i>Number</i>	<i>%</i>
Incident = 0	1579	96.22	1575	95.98
Incident = 1	62	3.78	66	4.02
Total	1641	100.00	1641	100.00

$$\chi^2 = 0.130$$

$$p = 0.718$$

3.78% of countries initiate a cyber incident against a weaker defender. 4.02% of countries initiate a cyber incident against stronger defender. The chi square and associated p value however suggest that this is not a statistically significant difference ($\chi^2 = 0.130$; $p = 0.718$). This supports the findings from the previous chapter that the balance of capability is not a good predictor of conflict in cyberspace. Deterrence is undermined because cyber incidents are not less likely to be conducted by a weaker state against a stronger rival. Relatively weaker states are just as likely to initiate cyber incidents against a rival as relatively stronger states.

The overall capability of a state should be a stronger predictor of the initiation of cyber conflict because it determines the opportunity a state has to carry out cyber operations. To assess this, I split

the data into three equally sized groups according of a country's latent capability index value. Group 1 represents the lowest capability, group 2 medium, and group 3 high. Table 49 conveys the relationship between capability and incident initiation.

Table 50.
Initiator's latent capability and incident initiation (2000-2016)

<i>Cyber incident initiated</i>	Low capability		Medium capability		High capability	
	<i>Number</i>	<i>%</i>	<i>Number</i>	<i>%</i>	<i>Number</i>	<i>%</i>
Incident = 0	1201	99.42	1191	98.76	1100	91.14
Incident = 1	7	0.58	15	1.24	107	8.86
Total	1208	100.00	1206	100.00	1207	100.00

$\chi^2 = 148.937$
 $p = 0.000$

A country's latent capability is positively related with initiation against a rival. In a given year, a cyber incident was initiated in 0.58% of cases among countries with low latent capability, 1.24% among countries of medium capability, and 8.86% among of countries with high capabilities. Expressed another way, 107 of the 129 total cyber incidents were initiated by a country with high latent capability. Moreover, these differences are statistically significant according to the chi square test ($\chi^2 = 148.937$; $p = 0.000$). As countries become stronger in cyberspace, they tend to conduct computer network operations with more frequency.

Turning to active capabilities, we have seen in the previous chapter that countries with mutual possession of military CNO units are more likely to engage in conflict, but how does the initiator's capability influence its initiation rate of cyber conflict? This can be compared simultaneously with the defender's capability. There are four possible situations: neither the initiator or the defender has a unit, only the defender has one, only the attacker has one, or both have one. The proportion of times the attacker initiated a cyber incident according to each category is shown in table 51 to test the relationship.

Table 51.
Initiator's military CNO unit possession and incident initiation

<i>Cyber incident initiated</i>	Neither		Defender only		Attacker only		Both	
	<i>Number</i>	<i>%</i>	<i>Number</i>	<i>%</i>	<i>Number</i>	<i>%</i>	<i>Number</i>	<i>%</i>
Incident = 0	2650	99.77	589	98.00	568	94.51	388	84.35
Incident = 1	6	0.23	12	2.00	33	5.49	72	15.65
Total	2656	100.00	601	100.00	601	100.00	460	100.00

$\chi^2 = 355.243$
 $p = 0.000$

A state initiated a cyber incident in only 0.23% of cases when neither it nor its rival had a military CNO unit. A state initiated a cyber incident in 2% of cases when it did not have a military CNO unit, but the defender did. This increased to 5.49% of cases when it did have a military CNO unit, but the defender did not. Finally, a state initiated a cyber incident in 15.65% of cases when both it and the defender had a military CNO unit. This means that the attacker initiates a cyber incident in 21.14% of cases when it possesses a CNO unit compared with only 2.23% of cases when it does not possess a CNO unit. This suggests that states are increasingly emboldened into conducting offensive operations once they acquire military operations capabilities.

Yet, why are incidents most likely when both states have a military unit rather than just the attacker? It suggests first that the defender's capability does not deter aggression from the attacker. This is supported by the results of a difference in proportions test in table 52. Here I examine the effect and the statistical significance of each condition separately, by comparing the baseline probability of a cyber incident under no condition ($123/4318 = 0.028$) to the probability when neither, the defender only, the attacker only, or both have this capability. It shows that when the defender has a military CNO unit and the attacker does not the probability of a cyber incident being initiated by the weaker attacker is not significantly reduced ($z = -1.255$; $p = 0.209$).

Table 52.
Conditional probabilities of cyber incident by relative power

<i>Relative active capabilities</i>	<i>Incident initiated</i>	<i>Total observations</i>	<i>Conditional probability</i>	<i>Z</i>	<i>p</i>
Neither	6	2656	0.002	-8.125	<0.000
Defender only	12	601	0.020	-1.255	0.209
Attacker only	33	601	0.055	3.894	0.000
Both	72	460	0.157	16.507	<0.000

This supports the notion that the defender's capabilities do not deter the aggressor. Moreover, the mutual possession of CNO units has a larger effect on cyber conflict initiation than in cases of attacker preponderance, suggesting that in these cases the defender's capabilities is actually

promoting cyber conflict being conducted against it. Perhaps the defender’s establishment of a military unit is reflective of a more intense rivalry with the initiator which drives the initiation of conflict. In the next section I investigate how the initiator’s willingness to conduct operations, as driven by rivalry intensity, feeds into the conflict process.

Rivalry intensity and cyber incidents

Here I examine the bivariate relationship between the level of hostility among rivals and cyber conflict. Since all the dyads in this analysis are already classified as rivals, I require another measure to distinguish between varying levels of rivalry intensity or conflict-proneness of each dyad. For this I account for the total number of militarised interstate disputes (MIDs) conducted between rival states between 2000 and 2010.⁴¹ A militarised interstate dispute is an event where there was a threat or display of military force short of war and comes from the Correlates of War MID dataset. This is a suitable proxy for the level of animosity between two states.

Figure 30 shows first how the number of MIDs involving each rival dyad relates to the total number of cyber incidents they have engaged in between themselves, followed by the correlation between these variables in table 53.

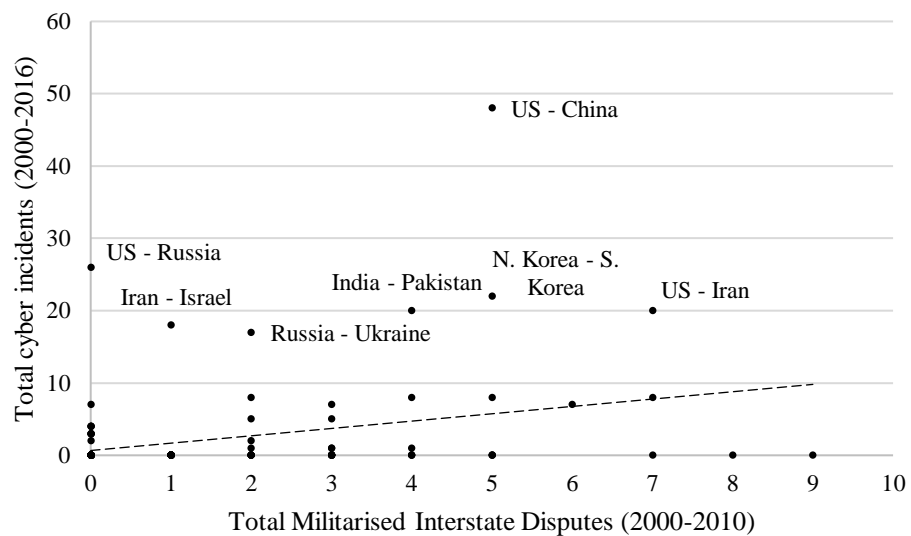


Figure 29. Total MIDs and cyber incidents between rival dyads.

⁴¹ The MID data only covers up to the year 2010 at the time of writing.

Table 53.
Correlation of total MIDs with cyber incidents.

<i>Variable</i>	<i>Correlation (-1 to 1)</i>	<i>Observations</i>
Total cyber incidents (2000-2016)	0.32	130

Both analyses show a very weak positive relationship between rivalry intensity and cyber conflict. Data points are scattered at random and the correlation is just 0.32. The level of conventional conflict between states is not a good predictor of how many cyber incidents they will engage in.

Again, the total number of cyber incidents is not predicted well by theoretically important variables such as capability and rivalry intensity. However, I can assess instead how rivalry intensity relates to the likelihood of a cyber incident being initiated which may produce stronger results.

To do this, I simplify the MID range by creating a scale of 4 categories. A value of 0 in this new scale corresponds to the dyad having 0 disputes, 1 corresponds to the dyad having 1-3 disputes, 2 corresponds to 4-6 disputes, and 4 corresponds to 7-9 disputes. Table 54 compares the number of dyads in each category to the occurrence of a cyber incident in a given year from 2000 to 2016.⁴²

Table 54.
MID frequency and cyber incidents between rival states (2000-2016)

<i>Cyber incident</i>	0 Disputes		1-3 disputes		4-6 disputes		7-9 disputes	
	<i>Number</i>	<i>%</i>	<i>Number</i>	<i>%</i>	<i>Number</i>	<i>%</i>	<i>Number</i>	<i>%</i>
Incident = 0	1094	97.50	743	95.19	175	79.19	69	81.18
Incident = 1	28	2.50	39	4.99	46	20.81	16	18.82
Total	1122	100.00	782	100.00	221	100.00	85	100.00

$\chi^2 = 140.098$
 $p = 0.000$

There is a positive relationship between the total number of MIDs experienced in a dyad and the likelihood of a dyad experiencing a cyber incident. Among dyads with no MID conflict between 2000-2010, only 2.5% engaged in cyber conflict. For states with between 1 to 3 MIDs, this percentage increases to 4.99%. For dyads within the 4-6 dispute category, the proportion of them experiencing a cyber incident rises sharply to 20.81%. This percentage then drops slightly to 18.82% among dyads in the most conflict-prone rivalries, however. There is a levelling off effect therefore in the effect of rivalry intensity on cyber conflict.

⁴² I use a non-directed dyad dataset here (one observation per dyad year) because I am not distinguishing attacker from defender at this stage.

I can also assess this relationship from the attacker’s perspective.⁴³ A state should be more likely to initiate a cyber incident if it is the more aggressive state in the rivalry. The dependent variable is whether a state initiated a cyber incident in a given year against a rival. The independent variable is how many militarised interstate disputes were initiated by this state against its rival, using the same categorisation as before. The frequency of MIDs serves as a proxy for how motivated a state is to engage in aggressive policies against a competitor. The results are shown in table 55.

Table 55.
Number of MIDs from initiator and cyber incident initiation in directed rival dyads (2000-2016)

	0 Disputes		1-3 disputes		4-6 disputes		7-9 disputes	
<i>Cyber incident by initiator</i>	<i>Number</i>	<i>%</i>	<i>Number</i>	<i>%</i>	<i>Number</i>	<i>%</i>	<i>Number</i>	<i>%</i>
Incident = 0	2115	97.96	1862	97.79	225	88.24	89	87.25
Incident = 1	44	2.04	42	2.21	30	11.76	13	12.75
Total	2159	100.00	1904	100.00	255	100.00	102	100.00

$\chi^2 = 140.551$
 $p = 0.000$

Only 2.04% of states that carried out no MIDs in this period initiated a cyber incident. This only slightly increased to 2.21% among states that had initiated between 1 and 3 disputes. However, states that initiated 4-6 disputes were 11.76% likely to carry out a cyber-attack against a rival, increasing further to 12.75% among states that initiated over 6 disputes. The differences are statistically significant ($\chi^2 = 140.551$; $p = 0.000$). The results show therefore that the more aggressive a state becomes in the arena of conventional conflict against a rival, the greater chance it will initiate a cyber operation against this rival. This suggests that rivalry intensity as well as capabilities promotes the initiation of cyber conflict. But a more robust analysis is required before making a definitive conclusion.

Multivariate analysis

The goal of this multivariate analysis is to provide more robust evidence to the analysis of the following question: how does a state’s level of capabilities and rivalry intensity with a rival impact its propensity to initiate cyber conflict? To do this, I run a logistic regression model on a data set of 4420 directed dyads where for each dyad there is one observation from the perspective of the

⁴³ For this I use a directed-dyad dataset (two observations per dyad-year – one from the attacker’s perspective and one from the defender’s perspective) to distinguish MIDs and cyber incidents from an initiator against a defender.

defender and one observation from the perspective of the attacker. This allows me to use information on the attacker's capabilities and relate this to its initiation of conflict against the defender.

The *dependent variable* is whether or not a cyber incident was initiated by a state against its rival in a given year. My *independent variables* are the initiator's latent and active capabilities. The first is the latent capability index score composed of programming skill and computer science knowledge. The second is whether the country has a military CNO unit. My interest is to examine how a potential initiator's capabilities affect the chances that it conducts cyber operations against its rival, and these are the most relevant capabilities for being able to carry out computer network operations. The directed nature of the dataset allows me to use the regression analysis to test how the defender's capabilities relates to cyber conflict with a greater level of robustness. Therefore, I add in the latent capability of the defender, and whether the defender has a military CNO unit.

My other explanatory variable of interest is conventional conflict which gauges the motivation of the initiator to conduct cyber operations based on its background level of hostility against its rival. I conduct this regression with the purpose of testing the robustness of the finding that states engaged in higher levels of conventional conflict are more likely to pursue cyber conflict. To account for this I add the total number of MIDs directed from the initiator to the defender from 2000-2010.

I run one model first with these five independent variables and then I run a second model with the addition of the control variables. The control variables are firstly the regime type of the initiator. This could have a confounding influence in the relationship between conventional conflict and cyber conflict. We might expect cyber conflict to be reduced when a state has lower levels of hostility with its rival. But given the democratic peace literature, a state might refrain from conducting cyber-attacks not because it has less conflict with the target state but because it is more democratic, and democratic states may be less likely to initiate cyber incidents. Less democratic states might on the other hand be more hostile, both conventionally and in cyberspace. To test this proposition, I add the Polity V autocracy-democracy scores which range from -10 (most authoritarian) to 10 (most democratic) to measure the regime type of the potential initiator. The other control variable is the major power status of the initiator from the Correlates of War's classification. Cyber conflict might be better explained by whether a country is a major power focused on prestige and status rather than its capabilities or dyadic rivalry intensity. This is dichotomous indicator taking a value of 1 if the country is a major power and 0 if otherwise.

Like before, all models here are run with peace years, peace years squared, and peace years cubed to control for temporal dependence. Moreover, I run all regressions with robust standard errors clustered by dyad to control for heteroscedasticity. To get the temporal sequencing right between CNO unit variable and conflict I lag the CNO variable so that each cyber incident is compared with the CNO

status of the initiator in the previous year. This ensures that the country had already established the capability before conducting the cyber operations.

In this regression table, I use the abbreviation A when the variable refers to the initiator of cyber conflict and B when the variable refers to the defender. CNO unit A therefore is whether the initiator has a military CNO unit and CNO unit B is whether the defender has a military CNO unit.

Results

Table 56 present the results of the logistic regression. Model one describes the regression results without controlling for regime type or major power status of the initiator. The coefficient values are not that informative by themselves at this stage because they are difficult to interpret and are dependent on the measurement scale of the explanatory variables. They are useful nonetheless to determine the direction of the effect, however, and to determine their statistical significance. In this model, the coefficients for the variables CNO unit A ($\beta = 1.680$), latent capability B ($\beta = 0.023$), and MIDs by A ($\beta = 0.172$) are all statistically significant given their respective p-values are lower than the conventional cut off point of 0.05. Of these two explanatory variables, CNO unit A and MIDs by A are more strongly significant given they have p-values less than or equal to 0.001.

Table 56.
Logistic regression of cyber incident initiation among directed dyads (2000-2016)

	(1) <i>No controls</i>	(2) <i>With controls</i>
CNO unit A	1.680*** (0.492)	1.677*** (0.507)
CNO unit B	-0.033 (0.387)	0.103 (0.378)
Latent capability A	-0.012 (0.010)	-0.004 (0.011)
Latent capability B	0.023** (0.008)	0.018** (0.007)
MIDs by A	0.172*** (0.050)	0.086 (0.057)
Major power A	-	0.429 (0.391)
Democracy A	-	-0.081*** (0.020)

Peace years	-0.302* (0.150)	-0.226 (0.172)
Peace years ²	0.012 (0.016)	0.006 (0.0185)
Peace years ³	-0.000 (0.000)	-0.000 (0.000)
Constant	-3.497** (1.076)	-3.960*** (0.842)
Observations	3,008	2,398
Pseudo R ²	0.333	0.375

Notes: Robust standard errors in parenthesis. Statistical significance denoted at the 0.05, 0.01, and 0.001 levels by *, **, *** respectively

The possession of a military CNO unit by the initiator significantly increases the likelihood of a cyber incident targeting the defender. Latent capability A, on the other hand, is not significantly associated with initiation of cyber incidents. Perhaps latent capability is more decisive in enabling a country to establish their operational capacity through military units than it is in determining which states will carry out operations.

Interestingly the latent cyber capability of the defender (Latent capability B) is positively and significantly associated with cyber incidents ($\beta=0.023$; $0.001 < p \leq 0.01$ in model 1). This means that as the capability of the defender grows it is more likely to be targeted. This may reflect the fact that most cyber conflict targets more powerful, industrialised states. CNO B is not a significant variable, suggesting that the initiation of cyber operations is undeterred by whether the defender possesses military active capability. Military build-ups in cyberspace therefore do not make the state more secure. In fact, they promote the escalation of cyber conflict.

The other explanatory variable of interest is the MIDs by A which measures the level of conventional conflict between the rivals when A was on the initiating side. Model 1 shows that this variable is positively associated with conflict initiation, in that the more aggressive a state has been towards its rival in the conventional conflict domain, the more likely it is to conduct a cyber operation against its rival also. This appears to support my theory that rivalry intensity drives cyber conflict.

MIDS by A loses its statistical significance however when looking to the second model which adds in two control variables, democracy, and major power status of A. The coefficient for the level of democracy of the initiator ($\beta = -0.081$) instead is statistically significant ($p \leq 0.001$) and predicts a negative relationship between how democratic a state is and its propensity to carry out cyber operations against a rival. Major power status of A is not significant, which suggests that democracy

is the variable which is having the confounding effect and resulting in a spurious relationship between MIDs by A and cyber conflict.

This raises the interesting finding that the initiation of cyber conflict is determined more by whether the attacker is democratic or authoritarian country, than its level of hostility against its rival. More specifically, the more democratic a country is, the less likely it will initiate cyber conflict against a rival. On the other hand, the countries that initiate cyber conflict most are autocratic regime types. Therefore, MIDs by A may only have been significant in the first regression model because the countries that engage in more conventional conflict tend to be less democratic and therefore tend to initiate more cyber conflict.

The initiator’s capability and the severity of cyber incidents

Given that the presence of active capability increases the frequency of cyber conflict, it seems logical to ask whether capabilities increase the severity of cyber conflict also. Fortunately, the DCID not only counts the number of cyber incidents but also classifies them by their severity, which allows me to compare the initiator’s capability during a cyber incident to what level of disruption or damage is inflicted on the defender.

Valeriano, Jensen, and Maness (2018) code the severity of each cyber incident on a ten-point scale. The definition and the frequency at which each appears in the incident dataset is shown in table 57. According to their assessment, cyber conflict has not risen above the level of 6 which is when there is widespread destruction of data as a result of a cyber incident. An example of this is the “Shamoon” virus allegedly used by Iran against the Saudi Aramco oil company which wiped data from their servers and disrupted one of the biggest financial assets to Saudi Arabia (Valeriano and Maness 2015, 156). Severity above a level of six is reached when deaths occur, but this has never happened.

Table 57.
Frequency of DCID incidents by severity scale

<i>Severity scale</i>	<i>Definition⁴⁴</i>	<i>Frequency</i>	<i>Cumulative %</i>
1	Probing without kinetic cyber	9	3.38
2	Harassment, propaganda, nuisance disruption	92	37.97
3	Stealing targeted critical information	97	74.44

⁴⁴ Definitions are quoted from Valeriano, Jensen and Maness (2018, 224)

4	Widespread government, economic, military, or critical private sector theft of information	53	94.36
5	Single critical network and physical attempted destruction	12	98.87
6	Single critical network widespread destruction	3	100.00
7	Minimal death as a direct result of cyber incident	0	-
8	Critical national economic disruption as a result of cyber incident	0	-
9	Critical national infrastructure destruction as a result of cyber incident	0	-
10	Massive death as a direct result of cyber incident	0	-

While cyber conflict has not reached the highest levels of severity imaginable, it is possible that they can explain variation in the lower levels of conflict that have occurred. For simplicity, I recode this scale into a binary indicator where a value of 1 corresponds to high severity and includes incidents that are above two on the severity scale. A value of 0 corresponds to low severity and includes incidents that reach no more than two on the severity scale. This seems a logical cut off because incidents above a value of two begin to include the theft of data which indicates greater sophistication of attack. Incidents below three on the other do not extend past simple website defacements and disruption.

Table 58 highlights the cross tabulation between the initiator's possession of a military CNO unit and how severe each cyber incident was. The chi square test statistic ($\chi^2 = 20.818$) reports a statistically significant value ($p = 0.000$), suggesting that the differences across categories is meaningful. Only 22.22% of incidents when the initiator did not have a military unit achieved a high severity level, compared with 62% of incidents when the initiator did have a military unit. It is possible therefore that the proliferation of military capabilities not only leads to a greater frequency of cyber incidents but a greater severity.

Table 58.
Initiator's Military CNO unit status and incident severity

<i>Severity</i>	No Military CNO unit		Military CNO unit	
	<i>Number</i>	<i>%</i>	<i>Number</i>	<i>%</i>
Low	21	77.78	78	37.50
High	6	22.22	159	62.50
Total	27	100.00	237	100.00

$\chi^2 = 20.818$
 $p = 0.000$

Discussion

While the balance or preponderance of capabilities is of limited importance in explaining the occurrence of cyber conflict though the causal mechanism of deterrence, the capabilities of individual states are key. Hypothesis 5 is therefore supported. As the capability of the state increases it is more likely to conduct cyber operations against another state. The most robust predictor of conflict onset is the possession by the initiator of a military CNO unit. The establishment of a CNO unit likely has a causal impact on cyber incidents because it reflects a growing capacity of the state to carry out cyber-attacks. The reverse causal relationship – that the initiation of a cyber incident causes a military CNO unit is less plausible.

This finding increases the validity of this measure as an effective way to gauge the capacity of a state to conduct computer network operations. A country that has created a dedicated agency for conducting computer network operations is better able to conduct cyber operations. Not all operations are conducted through military agencies of course, but perhaps this indicator also works well as a proxy for the general level of capacity to engage in operations within government.

There is no evidence that capabilities help create stability in the cyber domain through the mechanism of deterrence. The likelihood of cyber conflict is not reduced if the defender possesses a military CNO unit and it is increased among states with a mutual possession of this capability. Despite the purpose of military capabilities to build deterrent capacity, the findings show that they do not provide an effective means of signalling credible threats and dissuading attack.

In terms of latent capability, although the capability of the initiator does not have a significant impact on conflict initiation, the defender's latent capability does. Conflict is more likely when the defender has larger capability. This undermines deterrence yet again. Countries are not dissuaded by a more powerful target, instead they appear to be attracted towards attacking a more powerful state.

This can be explained by the fact that states with higher latent capability tend to more technologically advanced which creates a larger target for cyber espionage. For instance, China is weaker than the

United States in the cyber domain but frequently carries out cyber operations against United States to steal data from its industries and redress its technological deficiencies. This has included the alleged theft of the plans of for the F-35 fighter jet from Lockheed Martin in 2009 which may have helped China design similar military hardware (Lindsay and Cheung 2015, 58; Gady 2015). With its technological superiority, the US on the other hand has less interest in conducting this kind of cyber espionage against China. This shows that political or economic motivations are more important than relative capability in explaining cyber conflict.

This analysis however did not lead to robust findings on the relationship between rivalry intensity and cyber conflict. Therefore hypothesis 6 is not supported. Rivalry intensity does not increase the likelihood of cyber conflict from the initiator's perspective. Instead, the bivariate association between the level of conventional conflict initiated against a rival and the level of cyber conflict initiated against a rival appears to be explained by the regime type of the initiator. Non-democracies are both more likely to engage in conventional conflict and more likely to initiate cyber incidents. Countries like Russia, China, North Korea, and Iran could therefore be engaging frequently in offensive cyber activity not because of their rivalry with western countries, but because they are authoritarian and therefore less institutionally restrained. In the next chapter I assess how Iran's external relations has influenced its cyber conflict to provide greater understanding of this issue. Nevertheless, the cumulative findings suggest so far that while democracies and autocracies are equally likely to invest in active cyber capability, democracies appear to be more restrained about using these capabilities against other countries.

This chapter is the final part of the quantitative analysis on the effects of capabilities and conflict which has provided robust evidence that capabilities promote conflict, and that deterrence has no explanatory relevance. The next chapter is the final analytical component of the dissertation which illustrates the quantitative findings through a case study of Iran.

Chapter XI

The Case of Iran: Illustrating the Findings

Introduction

This chapter provides an illustrative case study of Iran which has been a prolific actor in the cyber arena, having engaged in the process of capability adoption and cyber conflict to a relatively high degree. An “illustrative” case-study is one that gives the reader a “feel” for the application of a theory in a relevant case (Levy 2008, 6). This study will therefore illustrate the cumulative findings of this thesis by showing how they apply in a real-world example in order to further develop the Opportunity-Willingness Theory for cyber actions in contrast to the perspectives of deterrence.

The previous quantitative analyses have been key for identifying the impact of opportunity and willingness variables on cyber capability proliferation and the effects of cyber capabilities on cyber conflict across a large number of cases. Fully explaining a phenomenon, however, is not only about highlighting the causal effects of an independent variable on a dependent variable but establishing the causal mechanisms behind the process and telling a story which highlights the theory.

I use this case study to illustrate my key findings from the previous empirical chapter and the chapter is structured according to these findings. In chapter 6, I mapped out the countries that had high latent cyber capabilities and the countries that had developed active capabilities. I will use this study to first describe in more depth the aspects of Iran’s latent cyber capability and the active cyber capabilities and policies it has adopted. I can also show how Iran compares in its latent cyber capability to other measures of cyber capacity and material resources.

In chapter 7 I showed that countries with higher latent capability and a more intense external threat environment were more likely to adopt active capabilities. I will therefore use the case of Iran to demonstrate how Iran’s high latent capability and its rivalry context has led it to adopting active cyber capabilities. The case study is not meant as a strict test of theory, which cannot be achieved with just one case. Instead, it illustrates to the reader in more detail how the theory works in one relevant case and traces the causal processes rather than the causal effects which were identified already by the statistical analyses.

In chapter 8, I demonstrated that my proxy measures of defensive capability did not correlate to a reduction in the frequency or success of cyber incidents. To investigate this issue in more detail, I use the case study to illustrate how Iran has dealt with cyber-attacks against it and whether its efforts to improve national cyber security have helped it reduce these threats. Chapter 9 showed that

countries are not deterred from cyber conflict by the relative capabilities of their rivals. I will therefore show how Iran has engaged its rivals in cyberspace despite being relatively weaker than many of them, including the United States. The Iran case is therefore relevance for demonstrating the failure of cyber deterrence mechanisms.

Finally, in chapter 10 I showed that the initiator's active/military capabilities provide the best predictor for whether it will initiate cyber incidents. This supported the opportunity side of the theory, that increased capability provides greater scope for action. The willingness-derived argument that rivalry intensity would promote cyber conflict however did not receive robust support. Instead the regime type of the state appeared to be a better predictor of the initiation of cyber operations.

In this case study I examine this issue in more depth by highlighting how Iran's active capabilities and its external threat environment have promoted its engagement in offensive computer network operations against its rivals. Overall, the case study generally supports the previous empirical findings, while also highlighting the significance of specific cyber-attacks in promoting the proliferation of cyber capability and conflict.

Describing Iran's cyber capabilities

Where does Iran sit in terms of cyber capability? While not being considered a top-tier cyber power alongside the United States, China, or Russia, commentators and experts generally accept that Iran has rapidly developed into at least a moderately capable actor in cyberspace over the last decade. Back in 2010, Clarke and Knake (2010, 35) acknowledged that Iran was amongst the world's 20 to 30 countries with "respectable" cyber warfare capabilities. More recently, the Centre for Strategic International Studies has argued that Iran is "ahead of most nations in strategy and organization for cyber warfare" (Lewis 2019). Iran's rapid evolution in cyberspace now figures prominently in threat assessments by other states. The 2019 CIA threat assessment warns that "Iran uses increasingly sophisticated cyber techniques to conduct espionage; it is also attempting to deploy cyber-attack capabilities that would enable attacks against critical infrastructure in the United States and allied countries" (Coats 2019, 6).

While these statements may reflect the kind of threat inflation to be expected from a rival state, my capability assessments generally support the notion that Iran is a capable actor in cyberspace. In terms of latent cyber capability, Iran scores well above average. It is ranked 15th out of the 126 countries assessed in terms of its production of computer science knowledge and its performance in Informatics and Mathematics Olympiads. This puts Iran within the top 12% of countries worldwide.

According to the active capability component of the dataset, Iran has established a national CSIRT and a military CNO unit. Iran established a national CSIRT in 2008 called MAHER (Radkani 2013), at a time when only 58 countries in the world had this type of active capability compared to the 130 countries that had a national CSIRT in 2017. In terms of military CNO units, in 2010 Iran reportedly established a “Cyber Defence Command” while in 2011/12 it is reported that a “Joint Chiefs of Staff Cyber Command” was also set up (BBC Persian n.d.; International Institute of Strategic Studies 2016, 331). In 2010 only 26 states had a military CNO unit compared with 63 states as of 2017. Iran therefore has established operational cyber units and has done so relatively early on. Iran has not yet published a national cyber security strategy however – at least one that is publicly available.

How does this compare with other measures of cyber capacity? Iran has a global rank of 60 according to the 2017 Global Cybersecurity Index by the ITU (International Telecommunications Union n.d.). This divergence can be explained by a difference in methodology and approach. My methods emphasise the skill and knowledge of potential hackers and the presence of military and government agencies at the operational level, while the ITU focuses on aspects that I do not cover such as legal frameworks. Cyber capability assessments can therefore vary widely depending on how capacity is defined and measured. Iran is not assessed by the National Cyber Security Index, presumably because of a lack of information.

Iran is ranked slightly lower (5 positions) in latent cyber capability as it is in material capability measured by CINC scores, suggesting it slightly underperforms compared to what its demographic, industrial, and military assets might suggest. This implies that Iran is not an example of a weak country that has been able to leap to the forefront in the cyber domain (Singer and Friedman 2014, 150), at least in terms of its underlying potential to conduct computer network operations based on programming ability and computer science knowledge. As will be shown later, it is quite clear on the other hand that Iran has been very willing to engage in cyber operations against its rivals. Nevertheless, cyber technology has not overturned Iran’s relative power position in world politics.

Having described Iran’s cyber capability as it stands, in the next section I examine the process by which Iran developed active cyber capabilities. I show that this process was driven by a combination of strong latent capabilities and a hostile rivalry environment, as predicted by Opportunity-Willingness Theory.

How latent capability and rivalry has driven Iran’s active cyber capabilities

Iran conforms to the expectations dictated by the opportunity and willingness theory for the proliferation of active cyber capabilities in the sense that first of all Iran has high levels of scientific and technical (S&T) knowledge and interstate rivalry, and secondly, Iran has established active

capabilities including military units, incident response teams, and other organisations and policies aimed at projecting or resisting influence in cyberspace. While the causal effects of opportunity and willingness-based factors on active cyber capabilities have been established in previous chapters, the process by which latent capacity and rivalry translate into active cyber capability has not been illustrated in a real-world example. So, how has Iran developed operational capacity in cyberspace? I begin by establishing Iran's science and technological capacity and then reviewing its rivalry experience.

Iran's scientific and technological context

Iran has been able to develop capabilities because it possesses strong levels of underlying S&T knowledge and skill. The Military Balance annual report, which records detailed information on military capabilities worldwide, states that "Iran has a well-developed capacity for cyber operations" given its "well-educated and computer-literate young population" (Military Balance 2016, 331).

Despite its economic stagnation due to prolonged periods of economic sanctions since the 1979 revolution – itself a consequence of its rivalry with the United States – Iran is a highly educated and skilled society. 15.77% of Iran's population in 2010 had completed tertiary education which, with the exception of Israel, is the highest educational attainment rate of any other country in the Middle East and North Africa (The World Bank n.d.). Iran produced 25 thousand scientific and technical journal articles in 2010, which was 17th highest of any country in that year (The World Bank n.d.). This translates into 338 per million of its population which is substantially higher than its regional rival Saudi Arabia which had a per capita output of 110 articles. More impressive yet is the statistic that Iran has the most engineering graduates in the world per capita (Myers 2015).

These underlying conditions put Iran on a strong footing for the development of active cyber capabilities. Indeed, at the International Olympiad in Informatics (which can be used as an indicator of programming ability) Iran is placed 8th in terms of overall medals won, coming behind only China, Russia, Poland, Romania, Bulgaria, South Korea, and Vietnam (International Olympiad of Informatics n.d.). Iran clearly has an above average number of computer literate and skilled citizens that could be applied to computer network operations.

Iran's scientific and technical knowledge provide a more plausible explanation for its cyber capabilities than its economic or industrial capacity. While Iran has a relatively large overall economy worth \$446.5bn – 18th largest in the world – it has a per capita GDP of just \$5.491 thousand – 96th in the world. Iran's economy has deteriorated partly because of economic sanctions from the United States (Johnson 2019), yet despite limited financial resources, Iran has established active

cyber capability which shows that cyber capabilities is not primarily driven by economic development.

Iran has not achieved its capabilities because of its IT industry either. The software industry in Iran is weak due to economic sanctions harming export opportunities and backward Internet infrastructure limiting domestic demand (Nicholson and Sahay 2017, 2). This is despite recent efforts by the Iranian government to promote its ICT sector and invest in infrastructure as a means of becoming less dependent on oil exports (Small Media 2017). Iran therefore conforms to the findings of chapter seven in that its knowledge and skills provide a better explanation for its cyber capabilities than other types of resources.

A counter argument is that Iran has purchased its cyber tools. Yet, according to a report by the Carnegie Endowment for International Peace:

“No publicly documented or privately observed attack has demonstrated the use of tools or resources that are beyond the capacity of Iranian threat actors” (Anderson and Sadjadpour 2018, 18).

Furthermore, the authors point out that:

“Tehran’s political and economic isolation has further constrained it from acquiring technology and expertise from foreign governments or companies, and little evidence exists that would indicate substantial cooperation with other nations in the development of its offensive cyber capabilities” (Anderson and Sadjadpour 2018, 14).

This suggests instead that Iran has domestically developed its capabilities. The most obvious explanation for Iran’s cyber capability build-up from the opportunity perspective is its own latent scientific knowledge and skill.

Iran’s latent cyber capability should not be overstated. According to some, Iran faces a “ceiling of capability and opportunity in its ability to threaten opponents” given its lack of organisation and budget (Anderson and Sadjadpour 2018, 13). This is reflected in my quantitative assessment showing Iran does not reach the top of the rankings alongside countries like the United States and China. Nevertheless, Iran clearly possesses adequate levels of latent capability to develop active capability and engage in computer network operations.

Iran’s rivalry context

Iran’s underlying capacity has combined with an intense international rivalry context to drive its quest for active cyber capabilities. Strategic rivalries are defined as “relationships in which decision

makers have singled out other states as distinctive competitors and enemies posing some actual or potential military threat” (Colaresi, Rasler and Thompson 2008, 3). According to the peace scale dataset, Iran was rivalled with five other nation states as of 2015, including the United States, Israel, and Saudi Arabia. To put this into perspective, the average number of rivals among all countries was less than one, and Iran is joint second only to the United States under this metric. Iran therefore possess a strong strategic motivation to invest in cyber capabilities as a means to manage its relations with its numerous competitors which includes establishing a defence and deterrent against cyber-attacks and an offensive capacity to conduct operations. The willingness condition is therefore in place in this case.

All interstate rivalries emerge out of a contentious issue such as territory, relative power and influence, or ideology (Colaresi, Rasler and Thompson 2008). The Iran-USA rivalry was initiated on the basis of divergent political ideologies and a backlash against historical US influence in the country. This can be traced back to the regime change that resulting from the 1979 revolution in Iran which overthrew the monarchy and instituted an Islamic republic under the theocratic rule of the Ayatollah Khomeini (Arjomand 1988).

Prior to this revolution, Iran had maintained very strong ties and a closely aligned foreign policy with the United States since 1953 when the United States and the UK governments organised a coup deposing Iran’s prime minister Mosaddeq in response to his policy of nationalising Iran’s oil industry (Kinzer 2003, 3). The revolution can be seen as a backlash to perceived US imperialism and the pro-western policies of the Shah Mohammad Reza Pahlavi. There is lasting resentment towards the United States within Iranian society with the slogan: “Death to America” being promoted by the leadership at various stages in the rivalry, which may reflect a policy by the regime to maintain domestic support through its cultivation of a sense of unity against external enemy (Beeman 2005, 38).

Numerous incidents and ongoing policies have kept relations at a generally poor level ever since. These include the Iranian hostage crisis of 1979-1980 where Iranian students took hostages in the US embassy in Tehran (Farber 2005), the shooting down of an Iranian passenger jet in 1988 (Fisher 2013), the labelling of Iran as part of the Axis of Evil in the aftermath of 9/11 for its sponsorship of terrorist organisations (Bush 2002), and the shooting down of US drones carrying out surveillance operations over Iran in 2019 (Gibbons-Neff, Sanger and Perez-Pena 2019). Since 2003, the US-Iran rivalry has been mainly driven by US concerns over Iran’s nuclear development programme and the continued economic sanctions by the US to deter this (Laub 2015). As I will soon explain, this aspect of the rivalry played a key role in the cyber conflict between these two states.

Iranian-Saudi relations are shaped by differences in Islamic religious ideology, the struggle for regional influence between the two leading powers in the Middle East, and Saudi’s close relationship

with the United States (Halliday 2005; Wehrey, et al. 2009). Until the revolution, Iran also maintained cordial relations with Saudi Arabia which turned to rivalry after 1980. After the revolution, Iran became the prime state sponsor of the Shia Islamic tradition and engaged in competition and a proxy conflict with Saudi Arabia – a Sunni Islamic state – over the influence of their respective religious ideologies in the Middle East (Wehrey, et al. 2009, 11). More recently both sides have fought a proxy war in Yemen since 2009, which has led Saudi Arabia to militarily intervene to support the Yemen state against Houthi rebels backed by Iran (Gardner 2015).

Turning to Iranian Israeli relations, this rivalry also derives from ideological differences that emerged after the 1979 revolution and Israel's close relationship with the United States. Israel became the "little Satan" to America's "great Satan" (Beeman 2005, 49). Their fraught relationship is also closely linked with Israel's conflict with Hamas and Hezbollah who Iran have supported or sponsored, for instance during the 2006 Israel-Lebanon war where Iran fought a proxy conflict with Israel through Hezbollah (Zisser 2011). Tensions have been particularly high since 2005 when the hardliner Ahmadinejad came to power and called for the destruction of Israel and engaged in a more aggressive foreign policy against Israel which including training and arming Hezbollah fighters during the 2006 Israel-Lebanon war (Kazemzadeh 2007). During this time, Iran began enriching uranium for its nuclear programme which has threatened Israel and exacerbated tensions.

Although regime change in Iran may have sparked many of these tensions, it is emergence of rivalry that is important, rather than the domestic political structure of Iran. In fact, Iran was already authoritarian before the Islamic revolution, so this is not a variable that changed. What mattered was the change from a regime that had friendly relations with the United States to one that was deeply hostile. The next section discusses how Iran's rivalries and external threat environment promoted the development of its active cyber capabilities.

Iran's quest for cyber capability

Before 2010, there was not much evidence that Iran had developed active cyber capability. Moreover, its cyber operations were infrequent and unsophisticated and therefore did not figure highly on threat assessments. There are only three recorded cyber incidents by Iran during this time which includes DDoS operations and website defacements against Israel in the context of Israel's conflict with the Palestinians. Another attack came in 2009 when the self-proclaimed Iranian "cyber army" redirected traffic on Twitter to a different website (Valeriano and Maness 2014). These incidents do not highlight substantial capability since they use unsophisticated methods, are easily and quickly reversible, and do not require specially designed malware and intelligence operations against the target.

A specific incident, emerging out the rivalry context, was crucial for the subsequent build-up in capability. The “Stuxnet” cyber-attack was pivotal in Iran’s change of policy towards becoming the capable cyber power as it is recognised today. One of the most contentious issues at stake in Iran’s rivalries is its nuclear development programme, which it has allegedly been developing since 2003. The United States and its allies oppose nuclear proliferation in Iran because it will change the balance of power in the Middle East, threaten other states, embolden Iran, and encouraging further proliferation to states such as Turkey, Egypt, and Saudi Arabia. Tensions were high regarding Iran’s pursuit of nuclear weapons since 2003 when the International Atomic Energy Agency began reporting that Iran was clandestinely enriching uranium and contravening the Non-proliferation Treaty (International Atomic Energy Agency 2003). The actions of Iran’s rivals to address this issue has directly led to Iranian cyber activity.

At the same time as increasing tensions over the nuclear programme, the United States was already engaged in costly wars in Iraq and Afghanistan and was unwilling to engage in a third, despite pressure from Israel to act. As an alternative tactic, the United States began work on a covert operation around 2006 to develop a cyber weapon which would offer a means of disrupting and delaying the speed of Iran’s uranium enrichment without the need for kinetic warfare. If successful, it could buy the United States more time in dealing with Iran before nuclear proliferation occurred, relieve pressure to take military action from Israel, and potentially sow discontent within Iran against the leadership. The planned cyber operation was part of Operation Olympic Games for which President Bush in 2007 had requested \$400 million from Congress to develop (Zetter 2015).

The result was the computer virus “Stuxnet” which took affect sometime between November 2009 and January 2010. The cyber weapon was specifically designed to target the Programmable Logic Controller (PLC) – a type of computer which automates industrial processes – at one of Iran’s nuclear enrichment facilities in the city of Natanz. These PLCs determined the speed at which the centrifuges enriching the uranium operated. The malware reprogrammed the PLCs to cause the centrifuges to rapidly increase and decrease in speed which resulted in the destruction of around one fifth of the total centrifuges installed at the plant (Slayton 2017, 95). It was a highly sophisticated operation not only in the design of the malware but because of the intelligence that was undertaken on the vulnerabilities of the targeted systems and that it most likely required an undercover agent with physical access to the computer systems which were air locked, or disconnected from the wider web (Lindsay 2013).

While expert opinion varies on the extent to which the cyber-attack set back Iran’s nuclear program, Stuxnet may help to explain the subsequent direction of Iranian cyber warfare capabilities and activities given that several organisations within Iran’s military structure were established soon after Stuxnet. For instance, between 2010 and 2011, Iran established the “Cyber Headquarters” (also

known as the “Cyber Defence Command”) which is situated under the Passive Civil Defence Organisation, itself subordinate to the Joint Staff of the Armed Forces. Its role is mainly to defend the country’s infrastructure against future cyber-attacks (Bucala 2015).

In 2010 the Islamic Revolutionary Guard Corp reportedly established a “Cyberspace Council” within the “Basij” paramilitary militia and announced that it had trained 1,500 hackers (Cohen 2019). Iranian threat rhetoric was also stepped up during this time which provides evidence that these developments were in response to Stuxnet. For instance, Brigadier General Gholamreza Jalali, the head of the Passive Civil Defence Organisation, warned that the Iranian military was prepared “to fight our enemies” in “cyberspace and Internet warfare” (The Irish Times 2012). Moreover, in 2013 an Iranian general boasted that it possessed the fourth largest cyber army (Brunner 2015). This public proclamation of capability and resolve is indicative of Iran trying to signal a deterrent threat in response to Stuxnet.

Iran also engaged in cyber capacity-building in the civilian sector. In 2012, it created the Supreme Council of Cyberspace which became the highest government authority on cybersecurity and directed the process of centralising control over Internet policy in Iran. Under the Council is the National Centre for Cyberspace whose role is to oversee the implementation of policies such as the creation of the national information network (SHOMA) that would be closed off from the wider global network (Small Media 2014).

Iran’s motives in building defensive cyber capability are twofold. The first is to gain greater control over Internet content and protect the regime against internal dissent taking place online, especially after the Green Revolution of 2009 where Iranians protested the controversial re-election of Mahmoud Ahmadinejad (Tofangsazi 2020, 7-10). The second reason is to reduce the vulnerability of Iran’s infrastructure against external cyber threats like Stuxnet. Reflecting this motivation, in Iran’s 2011-2016 ICT development plan, SHOMA was defined as “an IP-based Internet supported by data centres that are completely undetectable and impenetrable by foreign sources and allow the creation of private, secure intranet networks” (Freedom House 2017). The Iran case therefore shows that there can be a mixture of internal and external motivations for developments in capability.

Iran’s response is also evident through its increased financial investments in cyber security. Between President Rouhani coming to power in 2013 and 2015, Iran’s cyber security budget reportedly increased from \$3.4 million to \$19.8 million (Small Media 2015). A US House of Representatives hearing on the Iranian cyber threat also suggested that Iran had invested \$1 billion in “new technologies, investments in cyber defence, and the creation of a new cadre of cyber experts” (House of Representatives 2012), reflecting the increased threat perceptions in the United States by the growing cyber capabilities of Iran. Similarly, General William Shelton of the US Air Force Space Command, reported in 2013 that “it’s clear that the Natanz situation generated a reaction by them”

and warned Iran would be “a force to be reckoned with, with the potential capabilities that they will develop over the years and the potential threat that will represent to the United States” (Shalal-Esa 2013).

There is also evidence that Iran draws on a broad network of societal actors to develop the means to conduct cyber operations (Anderson and Sadjadpour 2018), highlighting the causal mechanism between latent capability and active capability. According to a think tank report, The Iranian Revolutionary Guard Corps has a cyber army which relies on 120,000 militia consisting of ‘university teachers, students, and clerics’ (UNIDIR 2013). Moreover, its top engineering university, Sharif University of Technology reportedly holds modules in “Security and Counter-infiltration” to promote hacking abilities among students (Article 19 2017). Iran clearly exploits and promotes the talent in broader society to establish the means to conduct computer network operations.

The close correlation between the cyber-attacks against Iran and its subsequent development of military and governmental active cyber capabilities, as well as various statements from Iranian and US officials, provide strong evidence that the external threat environment promoted capability proliferation in the Iran case. Specifically, it was the Stuxnet operation that prompted Iran to convert its already strong latent capability into institutional changes. While Stuxnet may have temporarily set back Iran’s nuclear capabilities, it clearly had the opposite effect on the direction of its cyber capabilities.

This analysis shows that cyber capabilities are subject to the same kind of action-reaction dynamics that shape security seeking behaviour in world politics generally (Jervis 1978). Real or perceived threats in the cyber domain are responded to with internal capacity-building efforts. The next question to ask is whether Iran’s development of cyber capabilities has had any impact on either its experience of cyber conflict as a victim, or its engagement in cyber conflict as an aggressor.

Has Iran’s cyber defence succeeded?

Chapter 8 of this dissertation demonstrated that a country’s level of secure Internet infrastructure or its efforts to improve cyber security at the institutional and policy levels had no impact on the frequency of cyber-attacks, which highlighted the inherent difficulty of cyber defence. This discussion will apply this issue to the Iran case to assess if its development of capabilities has led to a reduction in cyber threat.

Throughout the period under study and before embarking on the process of active capability development at around 2010/11, Iran has been very vulnerable to cyber threats. Iran has been a frequent target of cyber espionage, as disclosed by Edward Snowden – the NSA employee who in

2013 leaked classified documents uncovering the surveillance activities of the US government and its “five-eyes” partners: the UK, Canada, Australia, and New Zealand. These leaks include a presentation by the Canadian signals intelligence agency discussing a cyber espionage operation called “snowglobe” which they believed was developed by the French government and used to target Iranian institutions including the ministry of Foreign Affairs, the Atomic Energy Organization of Iran, and several universities around the year 2008 (Communications Security Establishment Canada n.d.). The Snowden leaks also revealed that in general Iran was the country from which the NSA collected the most pieces of intelligence (14 billion), as shown by a data visualisation tool known as “Boundless Informant” (Greenwald and MacAskill 2013).

As the previous section discussed, Iran was also the target of sabotage operations aimed at causing damage to its nuclear development program. Yet Stuxnet was just one incident in a broader campaign – known as “Olympic Games” – of cyber-attacks and espionage against Iran initiated by the Bush Administration and stepped up under Obama (Sanger 2012). Before the 2009 Stuxnet incident there was in fact an earlier version of Stuxnet (Stuxnet 0.5) which was released as early as 2007 (McDonald, et al. 2013). This version was programmed to target the Programmable Logic Controller (PLC) which controlled the valves which in turn determined the amount of uranium hexafluoride gas being fed into the centrifuges, as a means of disrupting the enrichment process. After a change of tactic, a second version of the Stuxnet worm that was reconfigured to influence the speed of the centrifuges was released in 2009. The Duqu malware which was discovered in 2011 by Hungarian researchers which also targeted Iran is thought to have been developed by the same creators of Stuxnet, but its role was to collect data rather than disrupt the operations of a PLC (Bencsath, et al. 2011).

Another operation, nicknamed “Flame” was active between 2009 and 2012 and collected intelligence on Iranian systems including those of Iran’s national oil company and oil ministry (Nakashima, Miller and Tate, US, Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say 2012). Flame is considered one of the most sophisticated espionage tools ever created. It was detected by Iran’s national CSIRT in 2012 (Iran National CERT 2012), which reportedly developed a removal tool for the malware (Zetter 2012) and identified the perpetrator, noting that “its encryption has a special pattern which you only see coming from Israel” (Erdbrink 2012). While this may indicate a growing capability to detect malware, preventing the operation in the first place was nevertheless still extremely challenging. Researchers believe that both the Stuxnet and the Flame operations were executed by someone with physical access to the system, who could overcome the “air-gap” between the target network and the wider Internet and infect machines with a device such as a USB stick (Langer 2013). This highlights one of the problems of cyber security – that despite best efforts to isolate critical systems, attackers can exploit alternative vectors of infiltration to overcome them.

As previously discussed, Iran increased its defensive efforts post Stuxnet. Between 2010 to 2012, Iran had established new military and governmental agencies and units to better defend infrastructure and centralise Internet policy, had begun developing a national intranet, and sought to foster a domestic IT industry to reduce vulnerability and prevent influence and cyber-attacks from its external rivals. However, it is very difficult to know if these efforts have had any impact.

One set of evidence is that since Iran has become more sensitive to cyber threats and pursued active capabilities, it has begun to declare frequently that it has prevented cyber-attacks. For instance, in June 2012, the Iranian intelligence agency announced they had detected a cyber-attack during negotiations on Iran's nuclear programme, claiming that "America and the Zionist regime (Israel) along with the MI6 planned an operation to launch a massive cyber-attack against Iran's facilities following the meeting between Iran and the P5+1 in Moscow", adding that "they still seek to carry out the plan, but we have taken necessary measures" (Reuters 2012). In 2016, Iran "detected and removed malicious software from two of its petrochemical complexes" (Reuters 2016). In December 2019, the ICT minister claimed that Iran "recently faced a highly organized and state-sponsored attack on our e-government infrastructure which was successfully identified and repelled by the country's security shield" (Corfield 2019). These announcements certainly suggest a heightened awareness of cyber threats and might indicate an improved capacity to prevent and manage them.

On the other hand, incidents against Iran have continued. For example, Project Sauron emerged in 2015 which targeted military and government institutions, telecoms companies, in several countries including Iran. It was very sophisticated given it went hidden for five years (Baraniuk 2019). More recently, in 2019, Iran was targeted by US cyber command in response to Iran shooting down a US drone and its mine attacks against oil tankers in the Straits of Hormuz. This cyber-attack targeted the Iranian intelligence agency responsible for planning their attacks and the computer systems that controlled Iranian missile launches. While this recent incident is considered a de-escalatory step by the United States to prevent conventional military action (Valeriano and Jensen 2019), it nevertheless demonstrates Iran's continued vulnerability to cyber threats.

The data suggests that overall incidents decreased after 2010. Figure 32 provides a timeline of the number of ongoing cyber incidents against Iran from 2000 to 2016. It shows that cyber-attacks reached a peak of 6 during 2010 and then fell down again to zero by 2013 before picking up slightly over the next couple of years. If Iran's institutional changes to build cyber defences began in earnest after 2010 then we can say there is a correlation between these capacity-building efforts and a reduction in the number of cyber incidents.

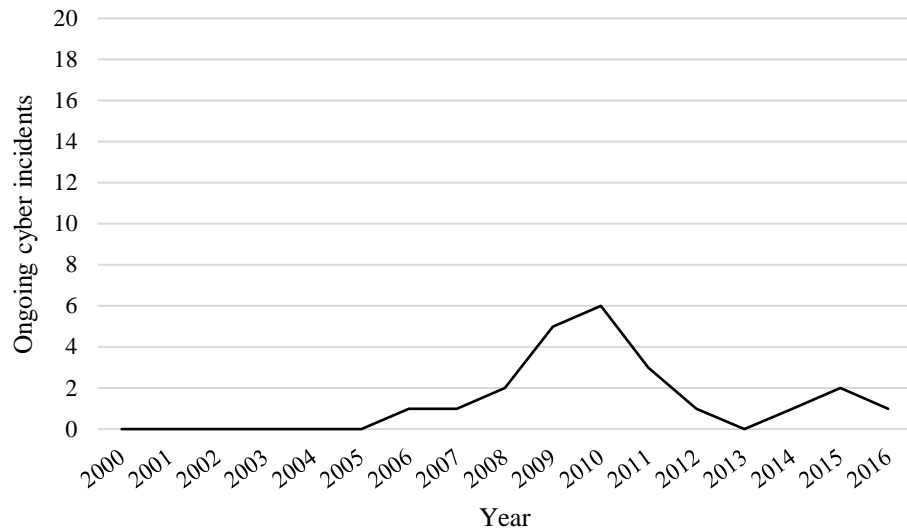


Figure 31. Ongoing cyber incidents against Iran (2000-2016)

However, it is very difficult with the available evidence to determine whether Iran’s defensive efforts and capabilities caused a reduction in cyber threat. While the number of cyber incidents decreased after 2010, this cannot necessarily be put down to improved defences. Shifts in the level of cyber incidents can also be explained by the motivations of Iran’s rivals, rather than an increase in defensive capability. In other words, the frequency of successful cyber-attacks is a function of the initiator’s decisions to employ them in addition to the defender’s actions to prevent them.

With continued moves toward control, perhaps in the future we will see a reduction of threats against Iran. However, this is too early to say because Iran has only recently begun implementing its National Information Network with the first phase being completed in 2016 (Small Media 2016). Closing off the Internet to external influence might be an effective step to reduce vulnerability, but this comes at the expense of the digital rights of Iranian citizens (Deibert 2018). Unfortunately, many authoritarian governments are taking the cyber sovereignty approach to Internet governance including China and Russia (Singer and Brooking 2018, 89). Even if Iran succeeds, incidents like Stuxnet show that sophisticated state actors with strong offensive capability like Israel and especially the United States will likely find a way to conduct CNO against Iran. This case study highlights the difficulty in achieving a deterrence by denial capacity, despite efforts by Iran at implementing institutional cyber defensive measures.

Iran’s capabilities and offensive operations

Chapter 9 of this dissertation highlighted that cyber conflict was not determined by relative capabilities between a state and its rivals. Chapter 10 showed instead that cyber conflict increased

when the initiator had greater capabilities, especially in relation to the military CNO unit indicator of active capability. Iran illustrates these findings first because Iran has engaged offensively with countries that are more capable than it in cyberspace, and second, because as Iran has increased its offensive cyber capabilities, its initiation of conflict has subsequently risen.

Iran is not just a victim in cyberspace and has frequently engaged in offensive computer network operations against its rivals. According to the data, Iran has been on the offence more than the defence. Iran is a victim in ten of the cyber incidents recorded in the DCID but is an initiator in thirty-three (Valeriano and Maness 2014).

Iran has clearly not been deterred by its rivals in cyberspace. The countries Iran has initiated cyber incidents against between 2000 and 2016 (and the number of incidents) are the United States (13), Israel (11), Saudi Arabia (7), Turkey (2). Evidently, the United States has most frequently been targeted by Iran having experienced 13 of the 33 cyber incidents initiated by Iran, which demonstrates that relative cyber capabilities have little effect in deterring cyber conflict. The United States is ranked number one in the world in latent cyber capabilities. It has a latent cyber capability score of 102.98 compared with Iran's 58.41. Moreover, it has long established and well-funded military units for conducting computer network operations going back to the 1990s (Healey 2015), while Iran only established military units around the year 2011. Iran is clearly not deterred by the dominance of the United States in cyberspace or the fear that the United States could retaliate with sufficiently negative consequences to make Iran rethink its activities.

That is not to say Iran does not initiate cyber incidents against states that have similar capabilities or are weaker than it. Israel has a latent capability of 54.17 and is ranked at 24 compared with Iran's ranking of 16 (although it has arguably better developed active capabilities). Saudi Arabia and Turkey have a latent capability of 47.77 and 51.22, respectively. Nevertheless, there is no evidence that Iran takes decisions to carry out computer network operations based on the relative capabilities of its rivals. It has conducted operations against states weaker, similar, and most frequently, against a state that is substantially stronger than it.

The Iran case therefore illustrates the findings of chapter 9. Deterrence does not operate in cyberspace in the same way it might in conventional warfare. The precise capabilities of the defender are nebulous, the impact of deterrent strikes is dubious, and there is a widespread acceptance that cyber incidents will be tolerated as operations that fall well below the threshold for escalation to armed conflict. Cyber capabilities have so little credibility that they do not provide a mechanism for the dissuasion of cyber conflict.

But capabilities do matter for explaining the low-level cyber activity of the initiator. Rather than deter conflict, the capabilities of a state embolden it to engage in cyber conflict. This is also illustrated by the Iran case because its cyber capability adoption has led to an increase in the frequency and

severity of its cyber incidents. This case study also demonstrates the relevance of rivalry to explain engagement in cyber conflict, thus supporting the opportunity and willingness theory.

Before its build-up of capabilities which began around 2011 in the aftermath of Stuxnet, Iran conducted very few offensive operations, and these were of a very low-level of sophistication. These incidents include the “Twitter hack” of 2009 when the “Iranian Cyber Army” redirected Internet traffic from Twitter to a different website where users were confronted with anti-American propaganda (Arthur 2009).

After Stuxnet, Iran began improving its offensive cyber capabilities which is evidenced in part by the establishment of units within the Iranian armed forces. Iran’s growing capability was also acknowledged by the United States. Speaking before the Senate Intelligence Committee in 2012, the Director of National Intelligence, James Clapper, warned that “Iran’s intelligence operations against the United States, including cyber capabilities, have dramatically increased in recent years in depth and complexity” (Shachtman, 2012).

Iran’s growing capacity to conduct CNO combined with its motivation to hit back at a rival state led to an increase in offensive activity. The first major incident was a Denial of Service attack against several US banks in September 2012. Institutions including the Bank of America, JPMorgan Chase, and Wells Fargo were flooded by requests, causing them to shut down and disrupting online banking (Nakashima 2012). While DDoS is an unsophisticated method, the incident highlights how Iran’s operations are linked to pre-existing interstate rivalry, specifically in this case as a response to the Obama administration’s tightening of economic sanctions against Iran in June 2012 (Perlroth and Hardy 2012).

The “Shamoon” incident demonstrated that Iran was now able to carry out more sophisticated attacks than it had done before. In 2012, Saudi Aramco – one of the largest oil companies in the world – was affected by malware which caused the destruction of data on over 30,000 computers belonging to the company (Bronk and Tikk-Ringas 2013). According to the DCID, this incident reached the highest severity level that has been witnessed in a cyber operation. The targeting of the Saudi company which was of national security importance given Saudi’s economic dependence on oil, clearly had political motivations and was linked to Iran’s broader rivalry context. Valeriano and Maness (2015, 57) suggest that “Shamoon was simply the tool of a weak state attempting to damage a rival and harm, by proxy, its large state sponsor and greatest consumer of oil, the United States.” Weak state or not, Iran had grown relatively in terms of offensive cyber capability. Shamoon showed that Iran could breach a network of critical economic interest to its rival and destroy data.

To demonstrate the increase in Iran’s offensive cyber operations and its correlation with capability developments, I plot the number of incidents initiated by Iran from 2000 to 2016 in figure 33. Iranian cyber conflict was very low until 2011 where there was no more than one ongoing incident against

a rival in any given year. This progressively increases after 2010 reaching a height of 17 in 2015, before falling again to 10 as of 2016.

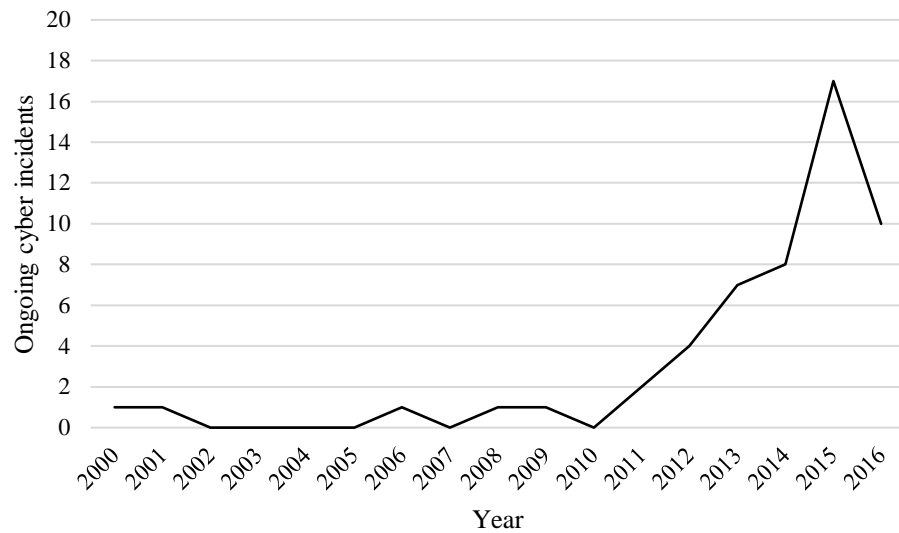


Figure 32. Ongoing cyber incidents initiated by Iran (2000-2016)

Does opportunity or willingness best explain this trend? In other words, has Iran increased its cyber operations because it has more motivated to or because it is better able to. One clue is that we have no evidence that Iran has substantial active cyber capabilities pre 2010, yet Iran's external rivalries and threat environment long predate this time. On the other hand, given that Stuxnet and the development of capabilities occurred within just a year or two of each other, it is difficult to distinguish their effects on the subsequent rise in Iran's offensive activity. As the opportunity and willingness theory suggests however, both factors are necessary. If Iran possessed the will (retaliation for Stuxnet) but not the capability, it would not have been able to conduct cyber operations. If Iran possessed the capability but not the will, it would not have been interested in conducting cyber operations. Both factors must be accounted for when explaining cyber conflict.

The severity has also increased in Iran's operations as table 34 shows. Here I have averaged the severity levels of the incidents Iran has initiated in each year from 2000 to 2016. Where there is a severity of zero, no incident took place in that year. It shows an overall increased in severity over time, which adds further evidence of Iran's growing capability alongside an increased frequency of initiations.

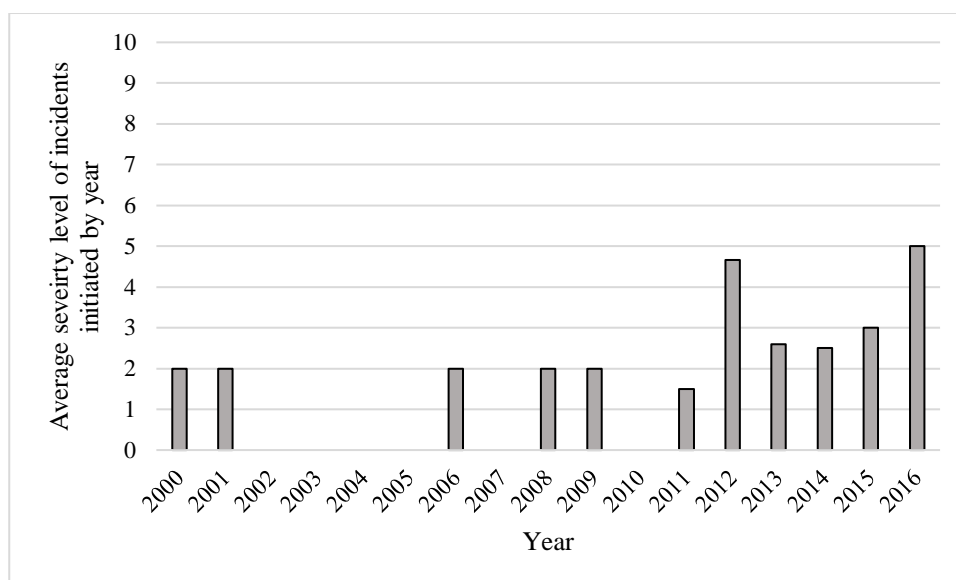


Figure 33. The severity of Iran’s offensive cyber operations (2000-2016)

A final puzzle is whether Iran’s initiation of cyber incidents is because it is authoritarian rather than because it is engaged in rivalry. While authoritarian regimes might be less constrained against conducting cyber-attacks in general as my statistical analysis suggested, this variable cannot explain the across-time variation in Iran’s cyber conflict. The regime type variable has remained constant. In other words, Iran has not become more or less democratic between 2000 and 2016. The factor that did change was its advances in capability that occurred after Stuxnet. This case points towards the importance of one cyber incident in driving a state’s capabilities and engagement in conflict, as Iran sought to become more secure but also sought to develop offensive capabilities to retaliate against its rival.

Discussion

The Iran case serves as an illustrative lesson for several reasons. It demonstrates how a state’s underlying science and technological human capital is more critical than financial or industrial resources in acquiring cyber capabilities. This case helps justify my methods of focusing on skill and knowledge as the key ingredients of latent cyber capability. Although a strong economy and software industry will undoubtedly help a country become a strong cyber power, these conditions are not necessary for establishing active capabilities. Iran’s opportunity has come primarily from its relatively well-educated society with particular strengths in engineering and computer science. This has allowed Iran to develop skills in cyber security and hacking.

Yet even if a country possesses strong latent capability, it will not necessarily adopt active cyber capabilities, at least at such a rapid rate as Iran. The Iran case highlights the importance of

international rivalry in creating the willingness for capability acquisition, although rivalry alone might not provide the most detailed explanation. Specifically, given the close correlation between events, the Stuxnet worm and the broader Olympic Games campaign from Iran's rivals may have driven the leap in Iran's military and government-led cyber security initiatives. So, while Stuxnet emerged out of rivalry, the cyber incident itself is more likely the proximate cause for proliferation.

Looking to the effects of Iran's capabilities, the case study reflects the inherent difficulty of achieving cyber defence or at least knowing if defensive initiatives have succeeded. While Iran saw a reduction in incidents after engaging in cyber capability investments, and official announcements of improved detection became more frequent, it is impossible to say if Iran's defensive capabilities has reduced the frequency of incidents or whether the motivation to attack Iran has decreased. The most significant incidents affecting Iran involved physical breaches of air gapped systems, moreover, which suggests that determined actors can find a way past cyber defences.

The case also illustrates the failure of deterrence by punishment. Iran has conducted many cyber incidents against the United States, despite the ability of the United States to retaliate with superior capabilities. There is no global system of cyber deterrence based on relative capabilities. Instead, countries develop cyber capabilities because it enables them to carry out their offensive aims. Iran fits with my earlier quantitative findings showing a strong positive correlation between a country's military/active capabilities and the frequency of offensive cyber operations. Since developing active capabilities, the number of incidents Iran has initiated greater increased and they have moreover increased in severity hinting at a growing capability. This process also seems to be motivated by a country's rivalry context, specifically in this case to the desire to retaliate to Stuxnet, which suggests that the Opportunity-Willingness framework can also be applied to a state's level of engagement in cyber conflict. In short, the Iran case provides a compelling argument that cyber activity can be explained to a high degree by the variables of capability and international political motivations.

Is the Iran case generalisable to most countries that develop capabilities and engage in conflict? On the one hand the answer is yes because the quantitative analysis showed that when countries have interstate rivals they are more likely to pursue capabilities. On the other hand, Iran is a unique case because of the Stuxnet incident which is possibly an outlier in terms of sophistication and impact. Most other countries have not suffered a cyber incident on the same scale. Perhaps the shock of Stuxnet has led Iran to build capability at a faster rate than would be expected under normal rivalry conditions. This question is beyond the scope of my quantitative analysis as the data cannot gauge the rate of cyber capability development, only its acquisition or non-acquisition. Nevertheless, this raises an interesting question for future research. What conditions lead to a rapid cyber build-up and do these processes have any independent effect on conflict spirals as suggested in the traditional arms race literature (Sample 1997).

Chapter XII

Conclusion: What Do We Know About Cyber Capability and Conflict Now?

Introduction

The global build-up of cyber capabilities has been ongoing for over a decade, but there has been little understanding of the causes and consequences of cyber capability proliferation based on extensive empirical analysis. This study is the first quantitative effort to measure national cyber capabilities and investigate their significance from a macro-perspective. It has introduced a new dataset that encompasses most states in the international system and spans a period of eighteen years from 2000 to 2017. This research therefore brings new empirical knowledge about the impact of cyber technology in international politics.

The central purpose of this thesis has been to establish a measurable concept of cyber capability to determine how capabilities have been acquired, why they have been acquired, and to assess their role in explaining the dynamics of cyber conflict. My findings confirm that there is indeed a rapid proliferation of cyber capabilities globally which appears to be motivated by international rivalry and enabled by skills and knowledge relating to computer technology. The findings also show that rather than deter conflict, capabilities are more likely to lead to an escalation in offensive cyber activity.

In this concluding chapter I summarise my approach and findings, reflect on the thesis' theoretical contribution, and outline the policy implications of my findings. Finally I discuss the limitations of this research and suggest areas for future research in order to further accumulate knowledge on cyber security and international politics.

Summary of approach and findings

My overarching approach has been to address the issue of cyber security from an international security perspective, drawing on relevant theories for the causes and effects of military capabilities, and applying a mainly quantitative approach to establish the general trends of competition and conflict in cyberspace. To carry out the analysis, I first established a definition of national cyber capability based on a state's resources and assets and then set out a method for measuring the concept in a way that could be applied to all countries across time.

I argued that capabilities can be assessed from two perspectives. First, I defined latent cyber capability as the resources relevant to computer technology that exist across society. Secondly, I defined active cyber capability as the government established organisations and policies that can be employed more directly by the state to defend or attack in cyberspace. This distinction is crucial for explaining how the former effects the adoption of the latter, and therefore for understanding the process of cyber capability proliferation. I have therefore introduced new quantitative measures of cyber capability based on the latent capacities of computer science skill and knowledge, industrial potential in software, and Internet infrastructure, and indicators of active cyber capability as measured by the creation by governments of military and civilian computer network operations units and strategies.

Using this data, this dissertation provided empirical evidence that the international system is indeed witnessing a rapid and widespread increase in cyber capabilities. This is the first time that an extensive array of evidence has been marshalled to provide a picture of the cyber capability landscape. This research has enabled an assessment of how countries compare in terms of their latent potential to project and resist influence in cyberspace and confirmed the continued dominance of states like the United States in the cyber domain. The descriptive analysis also highlights the rapid build-up of military and civilian units for cyber offence and defence and of national cyber security strategies. The increasing militarised nature of national cyber security policy as countries increasingly perceive cyberspace as the fifth domain of warfare is also confirmed through an analysis of the military organisations being established to counter growing threats. Moreover, these organisations have been adopted over wide geographical areas in very different political and economic contexts. Therefore, we now know how capabilities have proliferated, and given current trends in the data, we can expect more and more countries to acquire capabilities into the future.

To explain why a state develops cyber capabilities, I applied Opportunity-Willingness theory to argue that the adoption of active cyber capabilities is driven by its external threat environment and by its level of latent cyber capability. Countries that face more international rivals, experience greater levels of cyber threat, or are fearful of their rivals' capabilities should be more willing to pursue these assets because they provides the state with the ability to defend against the cyber-attacks from rivals or to carry out offensive operations to harm their rivals interests. Moreover, a country's latent cyber capability, especially programming skill and computer science knowledge, should promote the development of capabilities by establishing the opportunity for action.

The findings suggest that states require relatively high levels of computer science-related knowledge and ability to first have the opportunity to develop capabilities. Secondly, they are primarily motivated into investing in cyber capabilities because of the pre-existence of international rivalry. Latent capabilities are therefore a key explanatory variable for active cyber capabilities, and

proliferation is fundamentally based on existing international political tensions because these new capabilities provide another avenue to manage interstate relations. For instance, 84% of countries with above average publication output in computer science have established a national CSIRT while only 20% of countries with below average publication output have done the same. 6% of countries with no international rival have created a military CNO unit, but 15% of countries with at least one rival have created one. Using multivariate regression methods to ensure robustness, we can be more confident that these are important factors driving the proliferation process.

The next part of the analysis examined the impact of capabilities on cyber conflict. I investigated how defensive capabilities, how the balance of capability, and how the initiator's offensive capability effects the frequency of cyber incident between states. To structure this analysis, I drew on deterrence theory which suggests the risk of war can be minimised through creating a shift in the cost-benefit calculations of the aggressor. Deterrence offers a causal mechanism between capabilities and the frequency of cyber-attacks because capabilities create the means of blocking aggressive efforts or dissuading them by threatening punishment. Specifically, defensive cyber capabilities could signal to the potential aggressor that a cyber-attack would not be worthwhile, while offensive capabilities could signal that the defender has the capacity to threaten punishment. I argued instead that deterrence does not operate in cyberspace and therefore capabilities should not reduce the rate of cyber conflict. Returning to Opportunity-Willingness theory, I argued that capability should increase offensive activity by providing more opportunity and that rivalry intensity should increase offensive activity by providing more willingness to carry out cyber-attacks.

The findings largely support these hypotheses. They show that the efforts states make into improving cyber defences including the establishment of national CSIRTs and national cyber security strategies, as well as levels of secure infrastructure, do not have an impact on the frequency of cyber incidents. My findings also showed that more military capability between rivals was associated with more conflict. For instance, when two rival states rather than one possess a military CNO unit, the occurrence of cyber incidents increases from 7.5% to 31.3% of cases. Despite states building capability to become more secure, they are in fact making it more likely that they will enter into cyber conflict. So, we now know that the cyber domain has not established a successful system of deterrence based on relative cyber capabilities

While bivariate tests showed that the most antagonistic pairs of states were most likely to conduct cyber operations against one another, the multivariate analysis has suggested that the authoritarianism (or lack of democracy) of the initiator was a better explanation for this initial finding. In other words, authoritarian regimes were more likely to initiate cyber conflict than democracies. This could be explained by the fact democracies face greater domestic constraints

against the use of force even in the cyber domain. Further research is therefore needed to understand the domestic determinants of cyber conflict.

Finally, I adopted an illustrative case study of Iran which highlights the theory and findings in action. Iran is a state that has above average latent capacity in science and engineering as well as an intense rivalry context with the United States, Israel, and Saudi Arabia which correlates to the development of its cyber security capabilities and policies. The case suggested that the Stuxnet operation in particular was crucial in explaining Iran's cyber security behaviour. As for the effect of Iran's defensive capabilities on its experience of cyber-attacks, the evidence suggests Iran's improvements in capability might have led to a reduction in cyber incidents, which goes against the earlier quantitative findings, yet establishing causality here is difficult. On the other hand, Iran is certainly undeterred by the capabilities of more powerful rivals and in fact Iran has initiated more cyber conflict as its own capabilities have increased, which supports the results from statistical tests.

Theoretical significance

This thesis has made a theoretical contribution by applying long-established frameworks from the International Relations discipline to help explain state behaviour in cyberspace. This has demonstrated the continued relevance of certain approaches over others to account for cyber security processes in global politics. These include Opportunity-Willingness theory, neorealism, power analysis, and deterrence. Furthermore, it has demonstrated the feasibility and utility of applying quantitative research methodologies to cyberspace activity.

The framework of Opportunity-Willingness (Most and Starr 1989) has been shown to be a particularly useful tool with which to understand behaviour in cyberspace. Simply put, it says the probability of a state acquiring capabilities and engaging in conflict depends on its capacity and its interests to do so. The framework encourages researchers to clearly conceptualise the relevant factors to help explain behaviour empirically and allows variables from different levels of analysis to be incorporated in a study. Its use in this research has led to a clearer understanding of the national resources that enable action and the political factors that incentivise action in cyberspace.

Within this framework, this thesis has also engaged with realist assumptions of international politics. Central to realist theory is the idea that state behaviour and international conflict is driven by power and capability (Morgenthau 1948, Geller and Singer 1998, 56). Indeed, one of the key takeaways from this research is the importance of capabilities in driving state behaviour and conflict in cyberspace. The reason for this is simple. In a domain where aggressive action cannot be feasibly deterred, capability is the pivotal variable determining whether states can carry out cyber operations

and therefore whether they will do so. Given the absence of constraints on behaviour, cyberspace can be described as anarchical with the implications for competition and conflict that this entails.

Yet, this thesis also shows that cyber capabilities are of a very different nature to the traditional definition of capability as material resources. One of the most interesting findings from the capability analysis was the statistical significance of a country's computing skill and knowledge in explaining proliferation and conflict. This is the fundamental ingredient in a country's ability to project influence in cyberspace. However, this type of immaterial resource lacks serious attention in the broader IR field. The most common quantitative measure of national capability only accounts for the material factors of population, industrial resources and production, and military forces (Bremer 1980). These resources might become increasingly outdated in the digital age. Instead, scientific and technical knowledge is going to become increasingly central in the future with the emergence of Artificial Intelligence and robotics and should be properly accounted for by IR scholars.

Realist-inspired hypotheses of capability build-ups from the willingness side of the argument, on the other hand, receive mixed support. The analysis tested the neorealist idea that external security threats created the willingness to adopt military build-ups (Richardson 1960; Jervis 1978), but neither the number of cyber-attacks experienced, or the military capability of a rival were robust predictors of capability adoption. There is also no evidence that states are acquiring cyber capability to balance against the United States, as a neorealist perspective might argue (Schweller 2016). Realist hypotheses about military build-ups, when applied to cyberspace (Craig and Valeriano 2018), therefore do not stand up well to empirical tests.

Nevertheless, this is not to say that the build-up of cyber capabilities is not driven by strategic interests. The number of rivals a country has was a robust predictor of its adoption of capabilities. Rivalry basically "characterizes a competitive relationship between two actors over an issue that is of the highest salience to them" (Vasquez 2009, 78), but the range of behaviour observed within each rivalry relationship as well as the factors that caused the rivalry in the first place will be highly variant across cases. It is therefore not inconsistent with these findings that cyber capabilities are driven by some form of threat posed by a rival. But given the lack of evidence that actual threats (cyber-attacks and military units of rivals) matter, one might suggest that it is perceptions of threat between rivals that drives behaviour. This makes sense in the cyber domain where the precise, technical capability of a rival to inflict harm is unknown. There is much work to be done therefore on exploring how cyber threats come into existence from a social constructivist perspective (Rousseau 2006)

Domestic drivers of capability and conflict were also examined, which engages with Liberal theoretical arguments that different regime types engage in different foreign policies (Russett and O'Neal 2001). The findings showed that while democracies are not any less likely to acquire

capabilities than authoritarian regimes, democracies were significantly less likely to engage in cyber conflict than their non-democratic counterparts. This suggests that domestic politics could offer a good explanation for cyber security behaviour, and more research is needed to understand why this is the case. It may be that elected governments are more accountable to their constituents and therefore more restrained in cyberspace, or at least more likely to conceal their activity.

This research has also made a theoretical contribution to the emerging cyber security and IR literature by testing longstanding questions about the nature and impact of digital technology in global affairs. For instance, cyber deterrence has been an enduring source of debate amongst IR scholars for several years (Stevens 2012; Harknett and Nye 2017; Brantly 2018; Gartzke and Lindsay 2019), and while there is a general consensus that the concept is ill-suited to the cyber domain, it has been subjected to very little empirical testing. The findings of this analysis show clearly that cyber capabilities do not have a deterrent effect on cyber conflict. Despite states building capability to become more secure, they are in fact making it more likely that they will enter into cyber conflict. These findings therefore support the calls to move beyond deterrence-based frameworks (Fischerkeller and Harknett 2017).

For decades, the central debate in cyber security has been what impact the advent of cyber technology will have on interstate relations. This has divided IR scholars who believe the digital revolution will bring about some form of revolution in military affairs and increase the scope for interstate conflict (Kello 2018; Nye 2011, 125; Arquilla and Ronfeldt 1993) and those who believe that the effects of cyber operations are too limited to alter the balance of power or the change the nature of warfare (Rid 2013; Gartzke 2013; Lindsay 2013).

There are elements of truth to both perspectives. One of the testable hypotheses that can be derived from this body of literature is the notion that emergence of cyber capability will increase the prevalence of war including computer network attacks (Liff 2012; 426). Sceptics would argue not. As Gartzke (2013, 52) writes, “the mere capacity to harm is just not a very good predictor of aggression”. While it remains the case that cyber-attacks have not risen to anything near the catastrophic levels evoked by the cyber Pearl-Harbour or 9/11 analogies (Betz and Stevens 2013), my analysis suggests that the presence of capabilities does help to predict the occurrence of the cyber conflict that has been occurring in the international system over the past several years. This does not paint an optimistic picture and there is some cause for concern about the future of cyber conflict, given the rapid proliferation of cyber capabilities including those in the military sector. However, the idea that cyber power favours weaker states (Nye 2011), is not borne out by the data. While countries like North Korea and Iran do have significant capability, on the whole it is the large and developed economies that possess the most latent resources in cyberspace. Consequently, we should not expect cyber technology to substantially alter the distribution of power in the international system.

Lastly, this research has contributed to the quantitative study of cyber security and IR. Prior to this research, the international relations discipline knew very little about cyber capabilities and most assessments had been based on anecdotal accounts, small-N case studies, or from non-academic sources such as the media, cyber security firms, or governments, which might have a financial or political incentive towards threat inflation (Brito and Watkins 2011). Through the collection and analysis of cyber capability data, this thesis advances the quantitative approach to cyber security and international relations by provided a definition and way of measuring cyber capability, which is an essential step towards establishing a pathway for future empirical research on this topic.

Policy implications

The acquisition of cyber capabilities is likely to continue as long as states have the means and the political will. More importantly, this process is likely to generate more incidents of computer network conflict between states rather than create a deterrent effect. This is not to say that cyber capabilities will transform international warfare or replace traditional military means. Cyber incidents have not yet risen to the threshold of warfare and there is no evidence that they will. Nevertheless, the frequency of low-level cyber incidents is likely to continue or even increase as the capacity to conduct them continues its unconstrained proliferation to more and more international actors. If cyber capabilities therefore lead to more conflict rather than stability, what policy solutions do we have to control either the proliferation of cyber weapons or the onset of cyber conflict?

The increased integration of cyber security operations into the military sector should be of particular concern to policy makers worldwide and raises the prospect for an escalation in cyber conflict. If the international community believes cyber conflict ought to be reduced, then they should turn their attention to the phenomenon of military capability adoption and the proliferation of cyber weapons generally. One policy that has been proposed is cyber arms control (Stevens 2017; Maybaum and Tolle 2016), but it is very difficult to imagine how a system of enforceable checks and limitations on a state's arsenal of malicious code could be successfully implemented given their non-physical nature making them difficult to verify in the same way as traditional weapons (Denning 2001; Buchanan 2016, 167). As this research has shown, skill and knowledge on how to create malware and conduct operations is the fundamental basis of cyber capability. So even if the spread of malware is prevented, the skill to recreate it remains. The development of skills cannot feasibly be restrained, nor would that be sensible given the advantages knowledge brings to society.

If arms control is not possible perhaps policy makers should look towards preventing the malicious use of technology instead. It is clear a system of deterrence cannot be established through a balance of cyber capability in the international system, but norms may offer a solution instead. They can

work by imposing reputational costs on the initiation of cyber-attacks by developing widely accepted rules of proper behaviour in cyberspace (Stevens 2012; Nye 2016/2017). A taboo could be established against the most harmful types of cyber-attack that target critical infrastructure that more and more states eventually adhere to. There have already been efforts in this area including the bilateral agreement in 2015 between the United States and China for the cessation of cyber espionage (Brown and Yung 2017) and the 2015 meeting of the UN Group of Government Experts which set out principle of responsible state behaviour in cyberspace (United Nations 2015).

We should also recognise, based on the findings of this research, that offensive cyber capabilities are partly driven by pre-existing tensions and that cyber conflict is an extension of international rivalry. If policy makers want to limit the proliferation of cyber capabilities, they should turn their attention to solving pre-existing conflict and rivalry. This is a more fundamental issue of international politics and the answers do not lie in the cyber domain.

Ultimately, states must develop better security against intrusions. My findings were inconclusive about whether cyber reduce could deter conflict. While state level developments that I used as proxies for defence (national CSIRTs and strategies) were not linked to a reduction in cyber incidents, changes at the level of individual organisations and businesses might be a more effective solution. Governments should continue to encourage or compel the private sector to implement basic cyber security practices (password changes, two step verification, software updates etc.) within organisations. This type of strategy, rather than the pursuit of offensive and military capabilities, can help reduce vulnerability and keep data secure, without intensifying international rivalry and conflict. Public-private coordination on cyber security will also be essential to ensure the practices of critical infrastructure operators and private companies are in line with national security objectives (Carr 2016).

On a more positive note, we know what factors could help states develop cyber security capacity and these findings can help inform the growth of initiatives aimed at building capacity globally. These include the “Operational Guidance for EU’s International Cooperation in Cyber Capacity Building” by the European Commission (European Commission 2018) and the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford which has developed the “National Cybersecurity Capacity Building Model” (Dutton 2017). Furthermore, the Global Forum on Cyber Expertise (GFCE), originally launched by the Dutch Ministry of Foreign Affairs in partnership with several Foreign Ministries worldwide, aims to create a global platform for coordinating on best practices in the field of cyber capacity building (Calderaro and Craig 2020).

Science and technical knowledge, not economic development, were significant predictors of cyber capability in this study. This suggests that economically underdeveloped states lack cyber security capability because they lack the skills and knowledge of the technology. To aid the development of

cyber security capacity globally and across different geographical, economic, and cultural contexts, policy makers need to prioritise the development of technical education and skills so that societies are better equipped to build resilience to cyber threats.

Caveats and future research

To conclude this dissertation, I reflect on the limitations of this project and suggest avenues for future research that could help account for these weaknesses and further advance our knowledge of cyber security and international politics. The first set of limitations relate to methodology. Firstly, do the indicators of capability used here capture what they intend to? Clearly a country's entire cyber capability is not completely reflected in the presence of an organisation such as a military CNO unit or national CSIRT. My indicators of active cyber capability should instead be seen as proxy variables for capability which help capture part of the general efforts by a state to build capacity for seeking influence in cyberspace.

Measuring capabilities in the cyber domain is extremely difficult given the non-physical and "transitory" (Smeets 2018) nature of computer software and malware. Despite their limitations, my methods have helped overcome these challenges with a set of indicators of cyber capability that could be reliably assessed across time and space. Nevertheless, future research efforts can be expanded to other sources of capability not measured directly here. These include the signals intelligence organisations of each country from which many computer network operations are planned and conducted (Gioe, Goodman and Stevens 2020), the proxy-actors that many states derive capability from rather than their own institutions (Maurer 2018), and the sale of off-the-shelf malware from IT firms. Quantitative researchers will have to think of innovative methods for capturing these concepts empirically.

Future research could also develop better indicators of cyber security and defence. My analysis showed that developments like national cyber security strategy and national CSIRT formation did not reduce threats, but perhaps it is unwise to think they could. These are state-level indicators, and while they might correlate with broader levels of cyber security preparedness, they do not directly gauge what is going on at the level of individual organisations and businesses to reduce vulnerabilities and secure data through basic hygiene practices. We need more research not at the state level but on how prepared the private sector is to reduce cyber threats.

Another limitation is my focus on state actors and the exclusion of non-state actors from my analysis. Reliable information cannot easily be collected on non-state actors because they lack public records and institutions. While non-state actors lack access to the same level of resources as states the possibility of terrorist groups acquiring cyber weapons through off-the-shelf means remains. This is

concerning if terrorist actors are less constrained than states in their use of cyber tools – although some have cast doubt on this perspective given the unlikelihood that cyberterrorists could create public fear and thus achieve their aims (Stevens 2019). Future research should nevertheless explore the capacity and motives of these actors in the cyber domain in more depth.

The cyber incident data used here could also be a point of weakness. Like my data on capabilities, the Cyber Operations Tracker and the DCID rely on publicly exposed cyber incidents. Moreover they focus on political operations between rival states, and ignore the thousands of cyber-attacks that target businesses and organisations every day. Although most of these will not be politically motivated, they might still be very relevant for explaining the process of capability development by a state. We therefore need better cross-national estimates of cybercrime to control for this factor in explaining why countries adopt cyber capabilities.

The second set of limitations are theoretical. Theory narrows down on a few key variables but undoubtedly misses other important factors. In investigating the drivers of cyber capability, for instance, I have argued that a state derives its capability from its own domestic resources, not through external means. Others might argue that this ignores the possibility that a state acquires capability from the international cyber arms trade and through off-the-shelf malware (Maurer 2018, 27).

I argue, however, that the purchasing of malware from a foreign software company does not indicate the capability of the client government. They indicate the capability of the country in which they were formed (NSO Group were ex members of the Israeli intelligence agencies for example) (Brewster 2016). Moreover, these hacking tools are unlikely to be the most highly sophisticated cyber weapons. The countries that develop these weapons will not want to give away their most valuable hacking tools to a weaker country thus giving it an advantage. Governments that have to purchase off the shelf malware are doing so because they are not domestically capable, so I stand by my approach of focusing on domestic resources as the key aspect of cyber capability.

My theory also focused on the external political factors, like interstate rivalry, in driving proliferation and I have paid much less theoretical attention to the role of domestic political factors in this process. While I controlled for the effects of regime type when explaining the determinants of capability and their effect on conflict, the domestic explanations for cyber activity certainly needs further research. For instance, many countries presumably seek capabilities to carry out operations against their own citizens in acts of cyber repression (King, Pan and Roberts 2013). Moreover, there is a burgeoning cyber security industry in many countries which might promote the state's acquisition and use of offensive cyber technology in something akin to the military-industrial complex (Deibert 2011). Future research can investigate the role of domestic repression and the domestic cyber arms industry on the proliferation of capabilities.

Finally, more research is needed on the relationship between capabilities, deterrence, and conflict. I showed that intra-domain deterrence is unlikely to be feasible because cyber capabilities do not dissuade cyber-attacks. Yet cross-domain deterrence may be a more relevant mechanism towards managing interstate relations, where cyber conflict is deterred through non-cyber military means, or where conventional conflict is deterred through cyber means (Gartzke and Lindsay 2019). Rather than view cyber capabilities in isolation, we should understand that they are just one component in a state's foreign policy toolbox alongside economic sanctions, diplomatic actions, and military actions. We must therefore develop an understanding of how cyber capabilities fit into a broader political strategy of deterrence.

List of References

- Anderson, Collin, and Karim Sadjadpur. 2018. *Iran's Cyber Threat: Espionage, Sabotage, and Revenge*. Washington DC: Carnegie Endowment for International Peace.
<https://carnegieendowment.org/2018/01/04/iran-s-cyber-threat-espionage-sabotage-and-revenge-pub-75134>.
- Arjomand, Said Amir. 1988. *The turban for the crown: the Islamic revolution in Iran and The Iranian military in revolution and war*. Oxford: Oxford University Press.
- Arquilla, John. 2015. "Deterrence after Stuxnet." *Communications of the ACM*, August 4.
<https://cacm.acm.org/blogs/blog-cacm/190371-deterrence-after-stuxnet/fulltext>.
- . 2012. "Cyberwar is Already Upon Us: But can it be controlled?" *Foreign Policy*, February 27.
- Arquilla, John, and David Ronfeldt. 1993. "Cyberwar is Coming!" *Comparative Strategy* 12 (2): 141-165.
- Arthur, Charles. 2009. "Twitter hack by 'Iranian Cyber Army' is really just misdirection." *The Guardian*, December 18.
<https://www.theguardian.com/technology/blog/2009/dec/18/twitter-hack-iranian-cyber-army-dns-mowjcamp>.
- Article 19. 2017. "Tightening the Net, Part 2: The Soft War and Cyber Tactics in Iran."
https://www.article19.org/data/files/medialibrary/38619/Iran_report_part_2-FINAL.pdf.
- Australian Government. 2016. Australia's Cyber Security Strategy: Enabling Innovation, Growth & Prosperity. Available at: <https://www.homeaffairs.gov.craau/cyber-security-subsite/files/PMC-Cyber-Strategy.pdf>.
- Azmi, Riza, William Tibben, and Khin Than Win. 2016. "Motives behind Cyber Security Strategy Development: A Literature Review of National Cyber Security Strategy." *Australasian Conference on Information Systems*.
- Bachrach, Peter, and Morton S Baratz. 1962. "Two Faces of Power." *The American Political Science Review* 56 (4): 947-952.
- Baldwin, David A. 2002. "Power and International Relations." In *Handbook of International Relations*, edited by Walter Carlsnaes, Thomas Risse and Beth A Simmons. Sage.
- . 2016. *Power and International Relations: A Conceptual Approach*. Princeton: Princeton University Press.
- Ball, Desmond. 2011. "China's Cyber Warfare Capabilities." *Security Challenges* 7 (2).
- Baraniuk, Chris. 2019. "'Project Sauron' malware hidden for five years." *BBC News*, August 9.
<https://www.bbc.co.uk/news/technology-37021957>.
- Barbieri, Katherine. 2002. *The Liberal Illusion: Does Trade Promote Peace*. Ann Arbor: University of Michigan Press.
- Barnett, Michael, and Raymond Duvall. 2005. "Power in International Politics." *International Organization* 59 (1): 39-75.
- Bartos, Christopher A. 2016. "Cyber Weapons are not Created Equal." *US Naval Institute Proceedings* 142.

- BBC Persian. n.d. "Structure of Iran's Cyber Warfare." Accessed September 7, 2020.
https://nligf.nl/v1/upload/pdf/Structure_of_Irans_Cyber_Operations.pdf.
- Beck, Nathaniel, Jonathan N Katz, and Richard Tucker. 1998. "Taking Time Seriously: Time-Series-Cross-Section Analysis with a Binary Dependent Variable." *American Journal of Political Science* 42 (4): 1260-1288.
- Beckley, Michael. 2018. "The Power of Nations: Measuring What Matters." *International Security* 43 (2): 7-44.
- Beeman, William O. 2005. *The "Great Satan" vs the "Mad Mullahs"*. Chicago: University of Chicago Press.
- . 2005. *The "Great Satan" vs. the "Mad Mullahs"*. Westport: Praeger.
- Bellovin, Steven M, Susan Landau, and Herbert S Lin. 2017. "Limiting the undesired impact of cyber weapons: technical requirements and policy implications." *Journal of Cybersecurity* 59-68.
- Bencsath, Boldszsar, Gabor Pek, Levente Buttyan, and Mark Felegyhazi. 2011. "Duqu: A Stuxnet-like malware found in the wild." Technical Report by the Laboratory of Cryptography and System Security, Department of Telecommunications, Budapest University of Technology and Economics. Accessed December 2019.
<https://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf>.
- Bennet, D Scott, and Alan C Stam. 2004. *The Behavioural Origins of War*. Cambridge (Mass.): The University of Michigan Press.
- Betz, David. 2012. "Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed." *Journal of Strategic Affairs* 35 (5): 689-711.
- Betz, David J, and Tim Stevens. 2013. "Analogical reasoning and cyber security." *Security Dialogue* 44 (2): 147-164.
- Betz, David J, and Tim Stevens. 2011. "Chapter One: Power and Cyberspace." *Adelphi Series* 51 (424): 35-54.
- Biddle, Stephen. 2004. *Military Power*. Princeton: Princeton University Press.
- Billo, Charles G, and Welton Chang. 2004. *Cyber Warfare: Analysis of the Means and Motivations of Selected Nation States*. Hanover: Insitute for Security Technology Studies at Dartmouth College.
- Blainey, Geoffrey. 1973. *The Causes of War*. New York: The Free Press.
- Bolks, S, and R. J Stoll. 2000. "The Arms Acquisition Process: The Effects of Internal and External Constraints on Arms Race Dynamics." *Journal of Conflict Resolution* 44 (5): 580-603.
- Booth, Ken, and Nicholas Wheeler. 2017. *The Security Dilemma: Fear, Cooperation, and Trust in World Politics*. London: Red Globe Press.
- Bowler, Tim. 2020. "Huawei: Why is it being banned from the UK's 5G network?" *BBC News*, July 14. <https://www.bbc.co.uk/news/newsbeat-47041341>.
- Brady, Henry E. 2008. "Causation and Explanation in Social Science." In *The Oxford Handbook of Political Methodology*, edited by Janet M Box-Steffensmeier, Henry E Brady and David Collier, 217-270. New York: Oxford University Press.

- Brantly, Aaron. 2018. "The Cyber Deterrence Problem." Edited by T Minárik, R Jakschis and Lindström L. *2018 10th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE Publications. 31-54.
- Brantly, Aaron. 2014. "The Cyber Losers." *Democracy and Security* 10 (2): 132-155.
- Bremer, Stuart A. 1992. "Dangerous Dyads: Conditions Affecting the Likelihood of Interstate War, 1816-1965." *The Journal of Conflict Resolution* 36 (2): 309-341.
- Bremer, Stuart A. 1980. "National Capabilities and War Proneness." In *The Correlates of War: II, Testing Some Realpolitik Models*, edited by J David Singer. New York: The Free Press.
- Brewster, Thomas. 2016. "Everything We Know About NSO Group: The Professional Spies Who Hacked iPhones With A Single Text." August 25.
<https://www.forbes.com/sites/thomasbrewster/2016/08/25/everything-we-know-about-nso-group-the-professional-spies-who-hacked-iphones-with-a-single-text>.
- Brito, Jerry, and Tate Watkins. 2011. "Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy." *Harvard National Security Journal* 3: 39-84.
<https://harvardnsj.org/wp-content/uploads/sites/13/2012/01/Vol-3-Brito-and-Watkins.pdf>.
- Brodie, Bernard. 1946. *The Absolute Weapon: Atomic Power and World Order*. New York: Harcourt, Brace and Co.
- Bronk, Christopher, and Eneken Tikk-Ringas. 2013. "The Cyber Attack on Saudi Aramco." *Survival* 55: 81-96.
- Brooks, Harvey. 1980. "Technology, Evolution, and Purpose." *Daedalus* 109 (1): 65-81.
- Brooks, Stephen G, and William C Wohlforth. 2016. *America Abroad: The United States' Global Role in the 21st Century*. Oxford: Oxford University Press.
- Brown, Gary, and Christopher D Yung. 2017. "Evaluating the US-China Cybersecurity Agreement, Part 1: The US Approach to Cyberspace." *The Diplomat*, January 19.
<https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1-the-us-approach-to-cyberspace/>.
- Brunner, Jordan. 2015. "Iran Has Built an Army of Cyber-Proxies." *The Tower*, August.
<http://www.thetower.org/article/iran-has-built-an-army-of-cyber-proxies/>.
- BSA: The Software Alliance. 2015. *Asia-Pacific Cybersecurity Dashboard*. BSA: The Software Alliance.
http://cybersecurity.bsa.org/2015/apac/assets/PDFs/study_apac_cybersecurity_en.pdf.
- BSA: The Software Alliance. 2015. *EU Cybersecurity Dashboard: A Path to a Secure European Cyberspace*. BSA: The Software Alliance.
http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf.
- Bucala, Paul Pendleton, Caitlin, Shaida. 2015. "Iranian Cyber Strategy: A View from the Iranian Military." *Critical Threats*, November 24. <https://www.criticalthreats.org/analysis/iranian-cyber-strategy-a-view-from-the-iranian-military>.
- Buchanan, Ben. 2016. *The Cybersecurity Dilemma*. New York: Oxford University Press.
- Bundeswehr. n.d. *Cyber and Information Command*. Accessed December 2019.
<https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-cyber-und-informationsraum>.

- Bush, George W. 2002. "President Delivers State of Union Address." *The White House*. Accessed September 6, 2020. <https://georgewbush-whitehouse.archives.gov/news/releases/2002/01/20020129-11.html>.
- Buzan, Barry, and Eric Herring. 1998. *The Arms Dynamic in World Politics*. London: Lynne Reinner.
- Cabaj, Krzysztof, Dulce Domingos, Zbigniew Kotulski, and Ana Respicio. 2018. "Cybersecurity education: Evolution of the discipline and analysis of masters programs." *Computers and Security* 75: 24-35.
<https://www.sciencedirect.com/science/article/pii/S0167404818300373#:~:text=The%20CSEC2017%20defines%20cybersecurity%20as,testing%20of%20secure%20computer%20systems>.
- Calderaro, Andrea, and Anthony J S Craig. 2020. "Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building." *Third World Quarterly* 41 (6): 917-938.
<https://www.tandfonline.com/doi/abs/10.1080/01436597.2020.1729729>.
- Cameron, A Colin, and Pravin K Trivedi. 2005. *Microeconometrics: Methods and Applications*. Cambridge: Cambridge University Press.
- Capraro, Robert M, and Z Ebrar Yetkiner. 2010. "P Value." In *Encyclopedia of Research Design*, edited by Neil J Salkind, 1143-1148. Los Angeles: Sage.
- Carle, Jill. 2015. *Climate Change Seen as Top Global Threat*. Pew Research Center.
<https://www.pewresearch.org/global/2015/07/14/climate-change-seen-as-top-global-threat/>.
- Carr, Jeffrey. 2012. *Inside Cyber Warfare: Mapping the Cyber Underworld*. 2nd. Cambridge: O'Reilly.
- Carr, Madeline. 2016. "Public-private partnerships in national cyber-security strategies." *International Affairs* 92 (1): 43-62.
- Caruana, Anthony. 2020. "Kaspersky speaks on US government ban and a closed Russian internet." *ZDNet*, March 16. <https://www.zdnet.com/article/kaspersky-speaks-on-us-government-ban-and-a-closed-russian-internet/>.
- Cavelty, Myriam Dunn. 2008. *Cyber-Security and Threat Politics: US efforts to secure the information age*. New York: Routledge.
- Choucri, Nazli. 2012. *Cyberpolitics in International Relations*. Cambridge, Mass: MIT Press.
- Clarke, David D, and Susan Landau. 2010. "Untangling Attribution." *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy (2010)*. The National Academies Press. 41-52. <https://doi.org/10.17226/12997>.
- Clarke, Richard A, and Robert K Knake. 2010. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: Ecco.
- Coats, Daniel R. 2017. *Worldwide Threat Assessment of the National Intelligence Community*. Senate Select Ccommittee on Intelligence.
<https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20FR%20-%20Final.pdf>.

- Coats, Daniel R. 2019. *Worldwide Threat Assessment of the US Intelligence Community*. Senate Select Committee on Intelligence. Accessed January 29.
<https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf>.
- Cohen, Sam. 2019. "Iranian Cyber Capabilities: Assessing the Threat to Israeli Financial and Security Interests." *Cyber, Intelligence, and Security* 3 (1).
- Colaresi, Michael P, Karen Rasler, and William R Thompson. 2008. *Strategic Rivalries in World Politics: Position, Space and Conflict Escalation*. Cambridge: Cambridge University Press.
- Comin, Diego, and Marti Mestieri. 2014. "Technology Diffusion: Causes and Consequences." *Handbook of Economic Growth* 2B: 565-622.
- Communications Security Establishment Canada. n.d. "'SNOWGLOBE: From Discovery to Attribution'." a presentation discussing the French malware otherwise known as Babar. Accessed December 2019. <http://www.spiegel.de/media/media-35683.pdf>.
- Corfield, Gareth. 2019. "Iran says it staved off cyber attack but doesn't blame US." *The Register*, December 12.
https://www.theregister.co.uk/2019/12/12/iran_cyberattacked_no_attribution/.
- Correlates of War Project. n.d. *Correlates of War Data Bibliograph*. Accessed September 24, 2020.
<https://correlatesofwar.org/correlates-of-war-bibliography>.
- . 2017. "State System Membership List." <http://correlatesofwar.org>.
- Craig, Anthony J S, and Brandon Valeriano. 2016. "Conceptualising Cyber Arms Races." *CCDCOE CyberCon, 8th International Conference on Cyber Conflict: Cyber Power*. 141-158.
- Craig, Anthony J S, and Brandon Valeriano. 2018. "Realism and Cyber Conflict: Security in the Digital Age." In *Realism in Practice: An Appraisal*, edited by Davide Orsi, J R Avgustin and Max Nurnus, 85-101. Bristol: E-International Relations.
- Cylance. 2014. "Operation Cleaver." Threat Report.
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf.
- Dahl, Robert A. 1957. "The Concept of Power." *Behavioural Science* 2 (3).
- Deibert, Ronald. 2018. "Toward a Human-Centric Approach to Cybersecurity." *Ethics and International Affairs* 32 (4): 411-424. <https://www.cambridge.org/core/journals/ethics-and-international-affairs/article/toward-a-human-centric-approach-to-cybersecurity/4E8819984202A24186BB0F52E51BC1E4>.
- Deibert, Ronald. 2011. "Tracking the emerging arms race in cyberspace." *Bulletin of the Atomic Scientists* 67 (1).
- Denning, Dorothy E. 2001. "Obstacles and Options for Cyber Arms Control." *Arms Control in Cyberspace, Heinrich Boll Foundation*. Berlin.
<https://faculty.nps.edu/dedennin/publications/Berlin.pdf>.
- Department of Defense. 2018. "Cyber Strategy (Summary)." Accessed December 2019.
https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

- Department of Defense. 2015. "The DoD Cyber Strategy." Accessed December 2019.
https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf.
- . n.d. *U.S Cyber Command Mission and Vision*. Accessed December 2019.
<https://www.cybercom.mil/About/Mission-and-Vision/>.
- Digester, Peter. 1992. "The Fourth Face of Power." *Journal of Politics* 54 (4).
- Dutton, William H. 2017. *Cyber Security Capacity: Does it Matter?* SSRN Scholarly Paper, Rochester: Social Science Research Network .
- Early, Bryan R. 2014. "Exploring the Final Frontier: An Empirical Analysis of Global Civil Space Proliferation." *International Studies Quarterly* 58: 55-67.
- Eckstein, H. 1975. "Case Studies and Theory in Political Science." In *Handbook of Political Science*, edited by F Greenstein and Polsby N, 79-138. Reading MA: Addison-Wesley.
- Economist Intelligence Unit. 2011. *Cyber Power Index: Findings and Methodology*. Booz Allen Hamilton. <https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/eiu-cyber-power-index-findings-and-methodology>.
- E-Governance Academy. n.d. *National Cyber Security Index*. Accessed December 2019.
<https://ncsi.ega.ee/country/gr/>.
- Egozi, Arie. 2019. "How Israel is leading the global cyberwarfare race." *Defence IQ*, January 5.
<https://www.defenceiq.com/cyber-defence-and-security/articles/how-israel-is-leading-the-global-cyberwarfare-race>.
- Elgot, Jessica. 2016. "UK must build cyber-attack capability, chancellor says." *The Guardian*, November. <https://www.theguardian.com/politics/2016/nov/01/uk-must-build-cyber-attack-capability-chancellor-says-cybersecurity>.
- ENISA. 2012. *Deployment of Baseline Capabilities of National/Governmental CERTs*. Status Report, European Network and Information Security Agency.
<https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/baseline-capabilities>.
- Erdbrink, Thomas. 2012. "Iran Confirms Attack by Virus That Collects Information." *The New York Times*, May 29. https://www.nytimes.com/2012/05/30/world/middleeast/iran-confirms-cyber-attack-by-new-virus-called-flame.html?_r=1&hp.
- European Commission. 2017. "A Strategic Approach to Resilience in the EU's external action." Joint Communication to the European Parliament and the Council, Brussels.
https://eeas.europa.eu/sites/eeas/files/join_2017_21_f1_communication_from_commission_to_inst_en_v7_p1_916039.pdf.
- European Commission. 2018. *Operational Guidance for the EU's International Cooperation on Cyber Capacity Building* . Paris: European Union Insitute for Security Studies.
- Evangelista, Matthew. 1989. *Innovation and the Arms Race: How the United States and the Soviet Union Develop New Military Technologies*. Ithaca: Cornell University Press.
- Farber, David. 2005. *Taken hostage: the Iran hostage crisis and America's first encounter with radical Islam*. Princeton: Princeton University Press.
- Feakin, Tobias. 2013. "Playing Blind-Man's Buff: Estimating North Korea's Cyber Capabilities." *International Journal of Korean Unification Studies* 22 (2): 63-90.

- Finnemore, Martha, and Duncan B Hollis. 2016. "Constructing Norms for Global Cybersecurity." *The American Journal of International Law* 110 (3): 425-479. <https://www.iilj.org/wp-content/uploads/2017/01/Finnemore-Hollis-Constructing-Norms-for-Global-Cybersecurity.pdf>.
- Fischerkeller, Michael P, and Richard J Harknett. 2017. "Deterrence is Not a Credible Strategy for Cyberspace." *Foreign Policy Research Institute* 381-393.
- Fisher, Max. 2013. "The forgotten story of Iran Air Flight 655." *The Washington Post*, October 16. <https://www.washingtonpost.com/news/worldviews/wp/2013/10/16/the-forgotten-story-of-iran-air-flight-655/>.
- Freedom House. 2017. "Iran: Country Profile." Freedom on the Net report. https://freedomhouse.org/sites/default/files/FOTN%202017_Iran.pdf.
- Fruhlinger, Josh. 2018. "The OPM hack explained: Bad security practices meet Chinas Captain America." *CSO*, November 6. <https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html>.
- Furhmann, Matthew, and Michael C Horowitz. 2017. "Droning On: Explaining the Proliferation of Unmanned Aerial Vehicles." *International Organization* 71 (2): 394-418.
- Furlong, Kathryn, Nils Petter Gleditsch, and Havard Hegre. 2006. "Geographic Opportunity and Neomalthusian Willingness: Boundaries, Shared Rivers, and Conflict." *International Interactions* 32 (1): 79-108.
- Gady, Franz-Stefan. 2015. "New Snowden Documents Reveal Chinese Behind F-35 Hack." *The Diplomat*, January 27. <https://thediplomat.com/2015/01/new-snowden-documents-reveal-chinese-behind-f-35-hack/>.
- Gardner, Frank. 2015. "Yemen crisis: An Iranian-Saudi battleground?" *BBC News*, March 25. <https://www.bbc.co.uk/news/world-middle-east-32044059>.
- Gartzke, Eric. 1998. "Opportunity, Willingness, and the Origins of the Democratic Peace." *American Journal of Political Science* 42 (1): 1-27.
- Gartzke, Erik. 2013. "The Myth of Cyberwar: Bringing War on the Internet Back Down to Earth." *International Security* 38 (2): 41-73.
- Gartzke, Erik, and Jon R Lindsay. 2019. *Cross-Domain Deterrence: Strategy in an Era of Complexity*. Oxford: Oxford University Press.
- Geller, Daniel S. 1993. "Power Differentials and War in Rival Dyads." *International Studies Quarterly* 37 (2): 173-193.
- Geller, Daniel S, and David J Singer. 1998. *Nations at War: A Scientific Study of International Conflict*. Cambridge: Cambridge University Press.
- George, Alexander L, and Andrew Bennett. 2005. *Case Studies and Theory Development in the Social Sciences*. Cambridge (Mass): MIT Press.
- Gibbons-Neff, Thomas, David E Sanger, and Richard Perez-Pena. 2019. "Trump Says U.S. Shot Down Iranian Drone as Both Nations Dig In." *The New York Times*, July 18. <https://www.nytimes.com/2019/07/18/us/politics/iranian-drone-shot-down.html>.

- Gibler, D. M., Rider T. J., and Hutchison M. L. 2005. "Taking Arms Against a Sea of Troubles: Conventional Arms Races During Periods of Rivalry." *Journal of Peace Research* 42 (2): 131-147.
- Gibson, John, and David McKenzie. 2011. "Eight Questions about Brain Drain." *Journal of Economic Perspectives* 25 (3): 107-128.
- Gilady, Lilach. 2018. *The Price of Prestige: Conspicuous Consumption in International Relations*. Chicago: University of Chicago Press.
- Gioe, David, Michael S Goodman, and Tim Stevens. 2020. "Intelligence in the Cyber Era: Evolution of Revolution?" *Political Science Quarterly* 135 (2): 191-224.
- Glaser, Charles L. 1992. "Political Consequences of Military Strategy: Expanding and Refining the Spiral and Deterrence Models." *World Politics* 44 (4): 497-538.
- Glaser, Charles L. 2000. "The Causes and Consequences of Arms Races." *Annual Review of Political Science* 251-276.
- Glaser, Charles L. 2004. "When are Arms Races Dangerous? Optimal versus Suboptimal Arming." *International Security* 28 (4).
- Glaser, Charles L, and Chaim Kaufmann. 1998. "What is the offense-defense balance and can we measure it?" *International Security* 22 (4): 44-82.
- Goertz, Gary, Paul F Diehl, and Alexandru Balas. 2016. *The Puzzle of Peace: The Evolution of Peace in the International System*. New York: Oxford University Press.
- Goldsmith, Benjamin E. 2003. "Bearing the Defense Burden, 1886-1989: Why Spend More?" *Journal of Conflict Resolution* 47 (5): 551-573.
- Goldstein, Joshua S, and Jon C Pevehouse. 2007. *International Relations*. New York: Pearson.
- Gortzak, Yoav, Yoram Z Haftel, and Kevin Sweeney. 2005. "Offense-Defense Theory: An Empirical Assessment." *Journal of Conflict Resolution* 49 (1): 67-89.
- Gorwa, Robert, and Max Smeets. 2019. "Cyber Conflict in Political Science: A Review of Methods and Literature." (SocArXiv). Accessed July 25. doi:10.31235/osf.io/fc6sg.
- Greenwald, Glenn, and Ewan MacAskill. 2013. "Boundless Informant: the NSA's secret tool to track global surveillance data." *The Guardian*, June 11.
<https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining>.
- Guitton, Clement. 2012. "Criminals and Cyber Attacks: The Missing Link between Attribution and Deterrence." *International Journal of Cyber Criminology* 6 (2): 1030-1043.
- Haggard, Stephen, and John R Lindsay. 2015. "North Korea and the Sony hack : exporting instability through cyberspace." AsiaPacific Issues, East-West Center.
<https://scholarspace.manoa.hawaii.edu/bitstream/10125/36444/api117.pdf>
- Halliday, Fred. 2005. *The Middle East in International Relations: Power, Politics and Ideology*. Cambridge: Cambridge University Press.
- Harknett, R J, and E O Goldman. 2016. "The Search for Cyber Fundamentals." *Journal of Information Warfare* 15 (2): 81-88. <https://www.jstor.org/stable/pdf/26487534.pdf>.

- Harknett, Richard J, and Joseph S Nye. 2017. "Correspondence: Is Deterrence Possible in Cyberspace." *International Security* 42 (2).
- Harknett, Richard J, John P Callaghan, and Rudi Kauffman. 2010. "Leaving Deterrence Behind: War Fighting and National Cybersecurity." *Journal of Homeland Security and Emergency Management* 7 (1).
- Healey, Jason. 2013. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Cyber Conflict Studies Association.
- Healey, Jason. 2018. *Not The Cyber Deterrence the United States Wants*. Blog Post by Guest Blogger for Net Politics, The Council on Foreign Relations. <https://www.cfr.org/blog/not-cyber-deterrence-united-states-wants>.
- Healey, Jason. 2019. "The implications of persistent (and permanent) engagement in cyberspace." *Journal of Cybersecurity* 5 (1): 1-15.
- Hensel, Paul. 1999. "An Evolutionary Approach to the Study of Interstate Rivalry." *Conflict Management and Peace Science* 175-206.
- Hensel, Paul. 2012. "Review of Available Data Sets." In *Guide to the Scientific Study of International Process*, edited by Sarah McLaughlin Mitchell, Paul F Diehl and James D Morrow, 43-62. Oxford: Wiley-Blackwell.
- Herr, Trey. 2013. "PrEP: A Framework for Malware & Cyber Weapons." *The Journal of Information Warfare* 13 (1).
- Herr, Trey, and Ryan Ellis. 2016. "Disrupting Malware Markets." In *Cyber Insecurity: Navigating the Perils of the Next Information Age*, edited by Richard M Harrison and Trey Herr. New York: Rowman and Littlefield.
- Herrera, Geoffrey L. 2006. *Technology and International Transformation: The Railroad, the Atom Bomb, and the Politics of Technological Change*. Albany: State University of New York Press.
- Herz, John H. 1950. "idealist Internationalism and the Security Dilemma." *World Politics* 2 (2): 157-180.
- HM Government. 2018. "Cyber security skills strategy." Policy Paper. <https://www.gov.uk/government/publications/cyber-security-skills-strategy>.
- HM Government. 2016. "National Cyber Security Strategy 2016." <https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021>.
- Hohn, Carl H. 2011. "Geopolitics and the Measurement of National Power." PhD Thesis, Hamburg University. <https://d-nb.info/1047440237/34>.
- Holsti, Kalevi J. 1964. "The Concept of Power in the Study of International Relations." *International Studies Quarterly* 7 (4): 179-194.
- Horowitz, Michael. 2010. *The Diffusion of Military Power: Causes and Consequences for International Politics*. Princeton: Princeton University Press.
- House of Representatives. 2012. *Iranian Threat to the U.S. Homeland*. U.S. Government Printing Office. Accessed April 26, 2012. <https://www.hsdl.org/?abstract&did=743035>.

- Hutchins, Eric. 2015. *Understanding the Cyber Kill Chain™: Applying Intelligence to Computer Network Defense*. RSA Conference.
https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Seven_Ways_to_Apply_the_Cyber_Kill_Chain_with_a_Threat_at_Intelligence_Platform.pdf.
- Huth, Paul. 1988. "Extended Deterrence and the Outbreak of War." *American Political Science Review* 82 (2): 423-443.
- ICPC. n.d. *International Collegiate Programming Contest*. Accessed December 2019.
<https://icpc.baylor.edu/>.
- IISS. 2014. *The Military Balance: The Annual Assessment of Global Military Capabilities and Defence Economics*. The International Institute for Strategic Studies.
- IMO. n.d. *International Mathematics Olympiad*. Accessed December 2019. <https://www.imo-official.org/general.aspx>.
- Inkster, Nigel. 2016. *China's Cyber Power*. London: Routledge.
- International Atomic Energy Agency. 2003. "Implementation of the NPT Safeguards Agreement in the Islamic Republic of Iran." Report by the Director General of the IAEA. Accessed December 2019. <https://www.iaea.org/sites/default/files/gov2003-75.pdf>.
- International Cyber Policy Centre. 2017. *Cyber Maturity in the Asia-Pacific Region*. Australian Strategic Policy Institute.
- International Institute of Strategic Studies. 2016. *The Military Balance 2016*. London: Routledge.
- International Olympiad of Informatics. n.d. *Website of the IOI*. Accessed December 2019.
<https://ioinformatics.org/>.
- International Telecommunications Union. n.d. *Global Cybersecurity Index*. Accessed December 2019. <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>.
- . n.d. *National Cybersecurity Strategies Repository*. Accessed September 24, 2020.
<https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx>.
- Iran National CERT. 2012. *Identification of a New Targeted Cyber-Attack*. MAHER Computer Emergency Response Team Coordination Centre. Accessed December 2019.
<https://www.webcitation.org/682bfkhaU?url=http://www.certcc.ir/index.php?name=news&file=article&sid=1894&newlang=eng>.
- Jagers, Keith, and Ted Robert Gurr. 1995. "Tracking Democracy's Third Wave with the Polity III Data." *Journal of Peace Research* 32: 469-82.
- Jensen, Benjamin, Chris Whyte, and Scott Cuomo. 2019. "Algorithms at War: Promise, Peril, and Limits of Artificial Intelligence." *International Studies Review*.
- Jervis, Robert. 1978. "Cooperation Under the Security Dilemma." *World Politics* 30 (2): 167-214.
- . 1976. *Perception and Misperception in International Politics*. Princeton: Princeton University Press.
- Jo, Dong-Joon, and Erik Gartzke. 2007. "Determinants of Nuclear Weapons Proliferation." *Journal of Conflict Resolution* 51 (1): 167-194.

- Johnson, Keith. 2019. "Iran's Economy Is Crumbling, but Collapse Is a Long Way Off." *Foreign Policy*, February 13. <https://foreignpolicy.com/2019/02/13/irans-economy-is-crumbling-but-collapse-is-a-long-way-off-jcpoa-waivers-sanctions/>.
- Junio, Timothy J. 2013. "How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate." *Journal of Strategic Studies* 36 (1): 125-133.
- Kallberg, Jan, and Thuraisingham. Bhavani. 2012. "Towards cyber operations - The new role of academic cyber security research and education." *2012 IEEE International Conference on Intelligence and Security Informatics*. Arlington, VA: IEEE. <https://ieeexplore.ieee.org/abstract/document/6284146/>.
- Kazemzadeh, Masoud. 2007. "Ahmadinejad's Foreign Policy." *Comparative Studies of South Asia, Africa and the Middle East* 27 (2): 423-449. <https://muse.jhu.edu/article/220766/summary>.
- Kello, Lucas. 2013. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." *International Security* 38 (2): 7-40.
- . 2018. *The Virtual Weapon and International Order*. New Haven and London: Yale University Press.
- Killcrece. 2004. *Steps for Creating National CSIRTs*. White Paper, Pittsburgh: Carnegie Mellon Software Engineering Institute.
- King, Gary, Jennifer Pan, and Margaret E Roberts. 2013. "How Censorship in China Allows Government Criticism but Silences Collective Expression." *American Political Science Review* 107 (2): 1-18.
- Kinsella, David. 2000. "Arms Production in the Third Tier: An Analysis of Opportunity and Willingness." *International Interactions* 26 (3): 253-286.
- Kinzer, Stephen. 2003. *All the Shah's Men: An American Coup and the Roots of Middle East Terror*. Hoboken: John Wiley & Sons, Inc.
- Klein, James P, Gary Goertz, and Paul F Diehl. 2006. "The New Rivalry Dataset: Procedures and Patterns." *Journal of Peace Research* 43 (3): 331-348.
- Klimburg, Alexander, and Louk Faesen. 2018. "A Balance of Power in Cyberspace." *Hague Centre for Strategic Studies*. <https://www.jstor.org/stable/pdf/resrep19350.pdf?refreqid=excelsior%3A3c53ffe7c1747ef6f731cc506627ace6>.
- Knorr, Klaus. 1956. *The War Potential of Nations*. Princeton: Princeton University Press.
- Koblentz, Gregory, D, and Brian M Mazanec. 2013. "Viral Warfare: The Security Implications of Cyber and Biological Weapons." *Comparative Strategy* 32 (5): 418-434. <https://www.tandfonline.com/doi/pdf/10.1080/01495933.2013.821845?needAccess=true>.
- Koerner, Brandon I. 2016. "Inside the Cyberattack That Shocked the U.S. Government." *Wired*, 10 23. <https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government>.
- Kostyuk, Nadiya, and Yuri M Zhukov. 2017. "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?" *Journal of Conflict Resolution* 63 (2): 317-347. <https://journals.sagepub.com/doi/full/10.1177/0022002717737138>.

- Kuehl, Daniel T. 2009. "From Cyberspace to Cyberpower: Defining the Problem." In *Cyberpower and National Security*, by Franklin D Kramer, Stuart Starr and Larry K Wentz, 26-28. Washington DC: National Defense University Press.
- Langer, Ralph. 2013. *To Kill a Centrifuge: A technical Analysis of What Stuxnet's Creators Tried to Achieve*. Arlington: Langer Group. Accessed September 8, 2020. <https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf>.
- Lango, Hans. 2016. "Academic approaches to cybersecurity." In *Conflict in Cyber Space: Theoretical, strategic and legal perspectives*, edited by Karsten Friis and Jens Ringsmose. London: Routledge.
- Laub, Zachary. 2015. "International Sanctions on Iran." *Council on Foreign Relations*. <https://www.cfr.org/backgrounder/international-sanctions-iran>.
- Lawlor, Alison. 2014. *Cyber Blockades*. Washington DC: Georgetown University.
- Lawson, Sean. 2013. "Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats." *Journal of Information Technology and Politics* 10 (1): 86-103.
- Ledbetter, James. 2011. *Unwarranted Influence: Dwight D. Eisenhower and the Military Industrial Complex*. London: Yale University Press.
- Lee, Dave, and Nick Kwek. 2015. "North Korean hackers could kill, warns key defector." *BBC News*, May 29. <http://www.bbc.co.uk/news/technology-32925495>.
- Lee, Hyung-Soeg. 2005. "Information Technology Progress in North Korea and Its Prospects." In *Bytes and Bullets in Korea*, edited by Alexandre Y Mansourov, 100-122. Honolulu: Asia-Pacific Center for Security Studies.
- Leung, Frederick K S. 1998. "The implications of confucianism for education today." *Journal of Thought* 33 (2): 25-36.
- Leung, Frederick K S. 2017. "Making Sense of Mathematics Achievement in East Asia: Does Culture Really Matter?" *Proceedings of the 13th International Congress on Mathematical Education*. 201-218. https://link.springer.com/chapter/10.1007/978-3-319-62597-3_13.
- Levy, Jack. 2008. "Case Studies: Types, Designs, and Logics of Inference." *Conflict Management and Peace Science* 25: 1-18.
- Levy, Jack S, and William R Thompson. 2010. *Causes of War*. Oxford: Wiley-Blackwell.
- Lewis, James. 2019. *Iran's Cyber Power*. Center for Strategic and International Studies. Accessed June 25, 2019. <https://www.csis.org/analysis/iran-and-cyber-power>.
- Libicki, Martin C. 2017. "The Convergence of Information Warfare." *Strategic Studies Quarterly* 11 (1): 49-65.
- Libicki, Martin C, David Senty, and Julia Pollak. 2014. *Hackers Wanted: An Examination of the Cybersecurity Labour Market*. RAND.
- Libicki, Martin. 2009. *Cyberdeterrence and Cyberwar*. Santa Monica: RAND Corporation.
- Lieber, Kier. 2014. "The Offense-Defense Balance and Cyber Warfare." In *Cyber Analogies*, edited by Emily O Goldman and John Arquilla, 96-107. Monterey: Naval Postgraduate School.

- Liff, Adam P. 2012. "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War." *Journal of Strategic Studies* 35 (3): 401-428.
- Lindsay, Jon R. 2013. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* 22 (3): 365-404.
- Lindsay, Jon R. 2015. "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack." *Journal of Cybersecurity* 1 (1): 53-67.
<https://academic.oup.com/cybersecurity/article/1/1/53/2354517>.
- Lindsay, Jon R, and Tai Ming Cheung. 2015. "From Exploitation to Innovation: Acquisition, Absorption, and Application." In *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, edited by Jon R Lindsay, Tai Ming Cheung and Derek S Reveron, 51-86. New York: Oxford University Press.
- Lord, Kristin M, and Travis Sharp. 2011. "America's Cyber Future: Security and Prosperity in the Information Age." Edited by Kristin M Lord and Travis Sharp. Center for a New American Security. https://www.files.ethz.ch/isn/129902/CNAS_Cyber_Volume%20I_0.pdf.
- Luijckx, Eric, Kim Besseling, and Patrick de Graff. 2013. "Nineteen National Cyber Strategies." *International Journal of Critical Infrastructure Protection* 9 (1).
- Lukes, Stephen. 1974. *Power: A Radical View*. London: Palgrave Macmillan.
- Lynn, William J III. 2010. "Defending a New Domain: The Pentagon's Cyber Strategy." *Foreign Affairs*, September/October. <https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain>.
- Makridakis, Andreas, and Max Smeets. 2019. "Determinants of Cyber Readiness." *Journal of Cyber Policy* 4 (1): 72-89.
- Mansfield, Edward D, and Jon C Pevehouse. 2008. "Quantitative Methods." In *The Oxford Handbook of International Relations*, edited by Christian Reus-Smit and Duncan Snidal, 481-498. New York: Oxford University Press.
- Maoz, Zeev, and Bruce Russett. 1993. "Normative and Structural Causes of Democratic Peace, 1946-1986." *The American Political Science Review* 87 (3): 624-638.
- Maurer, Tim. 2018. *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge : Cambridge University Press.
- Maybaum, Markus, and Jens Tolle. 2016. "Arms Control in Cyberspace - Architecture for a Trust-Based Implementation Framework Based on Conventional Arms Control Methods." Edited by N Pissanidis, H Røigas and M Veenendaal. *Proceedings of the 8th International Conference on Cyber Conflict: Cyber Power* (CCD COE Publications) 159-173.
- McDonald, Geoff, Liam O Murchu, Stephen Doherty, and Eric Chien. 2013. *Stuxnet 0.5: The Missing Link*. Symantec Security Response. <https://docs.broadcom.com/doc/stuxnet-missing-link-13-en>.
- McGraw, Gary. 2013. "Cyber War is Inevitable (Unless We Build Security Back in)." *Journal of Strategic Studies* 36 (1): 109-119.
- Mearsheimer, John J. 1990. "Back to the Future: Instability in Europe After the Cold War." *International Security* 15 (1): 5-56.
- . 1984. *Conventional Deterrence*. Ithaca: Cornell University Press.

- Mearsheimer, John J. 2016. "Structural Realism." In *International Relations Theories: Discipline and Diversity*, edited by Time Dunne, Milja Kurki and Steve Smith. Oxford: Oxford University Press.
- . 2001. *The Tragedy of Great Power Politics*. New York: W. W. Norton & Company.
- Menard, Scott. 2010. "Logistic Regression." In *Encyclopedia of Research Design*, edited by Neil J Salkind, 730-735. Los Angeles: Sage.
- Merrit, Richard L, and Dina A Zinnes. 1988. "Validity of power indices." *International Interactions* 14 (2): 141-151.
- Michaelson, Greg, and J Michael Hardin. 2010. "Statistical Significance." In *Encyclopedia of Research Design*, edited by Neil J Salkind, 1361-1366. Los Angeles: Sage.
- n.d. *Ministry of Defence and Armed Forces*. Accessed 09 04, 2020. <http://www.army.cz/en/armed-forces/organisational-structure/cyb/cyber-forces-command-218593/#:~:text=Cybernetic%20and%20Information%20Warfare%20forces,land%2C%20air%20and%20special%20forces.>
- Ministry of Defence. 2016. *Cyber Primer (2nd Edition)*. Swindon: The Development, Concepts and Doctrine Centre.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160720-Cyber_Primer_ed_2_secured.pdf.
- Mitchell, Sara McLaughlin, Paul F Diehl, and James D Morrow. 2012. *Guide to the Scientific Study of International Processes*. Chichester: John Wiley & Sons.
- Morgenthau, Hans J. 1948. *Politics Among Nations: The Struggle for Power and Peace*. New York: A.A. Knopf.
- Morgus, Robert, Isabel Skierka, Mirko Hohmann, and Tim Maurer. 2015. "National CSIRTs and Their Role in Computer Security Incident Response." *New America*.
- Morgus, Robert, Max Smeets, and Trey Herr. 2018. *Countering the Proliferation of Offensive Cyber Capabilities*. Briefings from the Research Advisory Group, Global Commission on the Stability of Cyberspace.
- Most, Benjamin A, and Harvey Starr. 1989. *Inquiry, Logic, and International Politics*. Columbia: University of South Carolina Press.
- Mueller, Milton. 2017. *Will the Internet Fragment?: Sovereignty, Globalization, and Cyberspace*. Cambridge: Polity Press.
- Mulrine, Anna. 2015. "How North Korea built up a cadre of code warriors prepared for cyberwar." *Christian Science Monitor*, February 6.
<http://www.csmonitor.com/World/Passcode/2015/0206/How-North-Korea-builtup->.
- Myers, Joe. 2015. *Which country has the most engineering graduates?* World Economic Forum. Accessed September 17, 2015. <https://www.weforum.org/agenda/2015/09/which-country-most-engineering-manufacturing-and-construction-graduates/>.
- Naim, Moises. 2015. "Why Cyber War Is Dangerous for Democracies." *Carnegie Endowment for International Peace*, June 25. <https://carnegieendowment.org/2015/06/25/why-cyber-war-is-dangerous-for-democracies-pub-60500>.

- Nakashima, Ellen. 2012. "Iran blamed for cyberattacks on U.S. banks and companies." *Washington Post*, September 21. https://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html.
- Nakashima, Ellen, Greg Miller, and Julie Tate. 2012. "US, Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say." *The Washington Post*, June 19. https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html.
- National Security Office of South Korea. 2019. National Cybersecurity Strategy. https://www.krcert.or.kr/filedownload.do?attach_file_seq=2162&attach_file_id=EpF2162.pdf
- New York Cyber Task Force. 2017. *Building a Defensible Cyberspace*. New York Cyber Task Force, Columbia: School of International and Public Affairs. https://sipa.columbia.edu/sites/default/files/3668_SIPA%20Defensible%20Cyberspace-WEB.PDF.
- Nicholson, Brian, and Sundeep Sahay. 2017. "Building Iran's Software Industry: An Assessment of Plans and Prospects." *The Electronic Journal of Information Systems in Developing Countries* 13 (1): 1-19.
- Nye, Joseph S Jr. 2016/2017. "Deterrence and Dissuasion in Cyberspace." *International Security* 41 (3): 44-71.
- Nye, Joseph S Jr. 1990. "Soft Power." *Foreign Policy* (80): 153-171.
- . 2011. *The Future of Power*. New York: PublicAffairs.
- Office of the National Security Council, Republic of Croatia. "Exercise Cyber Shield 2019 was held at the Ministry of Defense". <https://www.uvns.hr/hr/aktualnosti-i-obavijesti/u-ministarstvu-obra-ne-odrzana-vjezba-kiberneticki-stit-2019>. Date accessed: 14.10.2020.
- Organski, A. F. K. 1968. *World Politics*. Alfred A. Knopf (2nd Edition).
- Organski, A. F. K, and J Kugler. 1980. *The War Ledger*. Chicago: University of Chicago Press.
- Packard, Hewlett. 2014. "Profiling an enigma: The mystery of North Korea's cyber threat landscape." HP Security Briefing Episode. <http://h30499.www3.hp.com/hpeb/attachments/hpeb/off-by-onsoftware->.
- Pape, Robert A. 2005. "International Security." *International Security* 30 (1): 7-45.
- Perloth, Nicole, and David E Sanger. 2018. "Cyberattacks Put Russian Fingers on the Switch at Power Plants, U.S. Says." *New York Times*, march 15. <https://www.nytimes.com/2018/03/15/us/politics/russia-cyberattacks.html>.
- Perloth, Nicole, and Quentin Hardy. 2012. "Bank Hacking Was the Work of Iranians Officials Say." *The New York Times*, January 8. <https://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html>.
- Peterson, Andrea. 2014. "The Sony Pictures hack, explained." *The Washington Post*, December 18. <https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/>.

- Peterson, Dale. 2013. "Offensive Cyber Weapons: Construction, Development, and Employment." *Journal of Strategic Studies* 36 (1): 120-124.
- Pollpeter, Keven. 2015. "Chinese Writings on Cyber Warfare and Coercion". In *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, edited by Jon R Lindsay, Tai Ming Cheung and Derek S Reveron, 138-162. New York: Oxford University Press.
- Pomerleau, Mark. 2019. "New Documents provide details on NSA relationship with Cyber Command." *Fifth Domain*, May 3. <https://www.fifthdomain.com/dod/2019/05/03/new-documents-provide-details-regarding-nsa-support-to-cyber-command/>.
- Potomac Institute for Policy Studies. 2015. *Cyber Readiness Index 2.0*. Arlington: Potomac Institute for Policy Studies. Accessed December 2019. <https://www.potomacinstitute.org/images/CRIndex2.0.pdf>.
- Pytlak, Allison, and George E Mitchell. 2016. "Power, rivalry and cyber conflict: An empirical analysis." In *Conflict in Cyberspace*, edited by Karsten Friis and Jens Ringsmose, 65-82. New York: Routledge.
- Quackenbush, Stephen L. 2011. "Deterrence theory: where do we stand?" *Review of International Studies* 37 (2): 741-762.
- Quester, George H. 1966. *Deterrence Before Hiroshima: The Airpower Background of Modern Strategy*. New York: Wiley.
- Radkani, Esmail. 2013. "MAHER (Iran National CERT)." International Telecommunications Union. Accessed September 7, 2020. http://www.itu.int/net/WSIS/implementation/2013/forum/agenda/session_docs/Day4/113/Panelist3-Radkani.pdf.
- Ray, James L. 2003. "Explaining Interstate Conflict and War: What Should Be Controlled for?" *Conflict Management and Peace Science* 20 (2): 1-31.
- Reed, John. 2017. "Vietnam army reveals 10,000-strong cyber warfare unit." *Financial Times*, December 26. <https://www.ft.com/content/ef924a6e-ea14-11e7-bd17-521324c81e23>.
- Relations, Council on Foreign. n.d. *Cyber Operations Tracker*. Accessed 12 2019. <https://www.cfr.org/interactive/cyber-operations>.
- Reuters. 2016. "Iran detects malware in petrochemical plants, says not linked to recent fires." August 27. <https://www.reuters.com/article/us-iran-security-cyber-idUSKCN1120E9>.
- . 2012. "Iran says detected "massive cyber attack" - TV." *Reuters*, June 21. <https://uk.reuters.com/article/uk-iran-cyber-nuclear/iran-says-detected-massive-cyber-attack-tv-idUKBRE85K1EG20120621>.
- Richardson, Lewis F. 1960. "Arms and Insecurity: A Mathematical Study of the Causes and Origins of War." Edited by Nicholas Rashevksy and Ernesto Trucco. Pittsburgh: The Boxwood Press.
- Rid, Thomas. 2012. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35 (1): 5-32.
- . 2013. *Cyber War Will Not Take Place*. London: C Hurst & Co Publishers Ltd.
- Rid, Thomas, and Ben Buchanan. 2015. "Attributing Cyber Attacks." *Journal of Strategic Studies* 38 (1-2): 4-37. <https://www.tandfonline.com/doi/abs/10.1080/01402390.2014.977382>.

- Rid, Thomas, and Peter McBurney. 2012. "Cyber Weapons." *The RUSI Journal* 157 (1): 6-13.
- Rider, Toby J, Michael G Findley, and Paul F Diehl. 2011. "Just part of the game? Arms races, rivalry, and war." *Journal of Peace Research* 48 (1): 85-100.
- Risse-Kappen, Thomas. 1991. "Public Opinion, Domestic Structure, and Foreign Policy in Liberal Democracies." *World Politics* 479-512.
- Robinson, James A. 2006. "Economic Development and Democracy." *Annual Review of Political Science* 9: 503-527.
- Romanosky, Sasha, and Zachary Goldman. 2016. "Cyber Collateral Damage." *Procedia Computer Science* 95: 10-17.
- Ross, Andrew L. 1993. "The Dynamics of Military Technology." In *Building a New Global Order: Emerging Trends in International Security*, edited by David Desitt, David Haglund and John Kirton, 106-140. Oxford: Oxford University Press.
- Rousseau, David L. 2006. *Identifying Threats and Threatening Identities: The Social Construction of Realism and Liberalism*. Stanford: Stanford University Press.
- Rueter, Nicholas. 2011. "The Cybersecurity Dilemma." Masters Thesis, Duke University. <https://hdl.handle.net/10161/3793>.
- Russett, Bruce M. 1968. "Components of an operational theory of international alliance formation." *Journal of Conflict Resolution* 285-301.
- Russett, Bruce M, and John R O'Neal. 2001. *Trignulating Peace: Democracy, Interdependence, and International Organizations*. W. W. Norton & Company.
- Ryall, Julian, and Danielle Demetriou. 2018. "US preparing 'bloody nose' cyber attacks on North Korea." *The Telegraph*, February 20. <https://www.telegraph.co.uk/news/2018/02/20/us-preparing-bloody-nose-cyber-attacks-north-korea/>.
- Ryan, Jason. 2011. "CIA Director Leon Panetta Warns of Possible Cyber-Pearl Harbor." *ABC News*, February 11. <https://abcnews.go.com/News/cia-director-leon-panetta-warns-cyber-pearl-harbor/story?id=12888905>.
- S&P Global. n.d. *S&P Capital IQ Platform*. Accessed December 2019. <https://www.spglobal.com/marketintelligence/en/solutions/sp-capital-iq-platform>.
- Sagan, Scott D. 2011. "The Causes of Nuclear Weapons Proliferation." *Annual Review of Political Science* 14: 225-244.
- Sagan, Scott D. 1996. "Why Do States Build Nuclear Weapons? Three Models in Search of a Bomb." *International Security* 21 (3): 54-86.
- Salkind, Neil J (ed). 2010. *Encyclopedia of Research Design*. Los Angeles: Sage.
- Sample, Susan G. 1998. "Military Buildups, War, and Realpolitik: A Multivariate Model." *Journal of Conflict Resolution* 42 (2): 156-75.
- Sanders, David. 2010. "Behavioural Analysis." In *Theory and Methods in Political Science*, edited by David Marsh and Gerry Stoker, 23-41. New York: Palgrave Macmillan.
- Sanger, David E. 2012. "Obama Order Sped Up Wave of Cyberattacks Against Iran." *The New York Times*, June 1. <https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html>.

- Sanger, David E, and Nicole Perlroth. 2019. "U.S. Escalates Online Attacks on Russia's Power Grid." *New York Times*, June 15. <https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html>.
- Sarkees, Meredith R, and Frank Wayman. 2010. *Resort to War: 1816 - 2007*. Washington DC: CQ Press.
- SC Media. 2015. "Russia overtaking US in cyber-warfare capabilities." *SC Magazine*, October 29. <https://www.scmagazineuk.com/russia-overtaking-us-cyber-warfare-capabilities/article/1479412>.
- Schneider, Jacquelyn. 2019. "The capability/vulnerability paradox and military revolutions: Implications for computing, cyber, and the onset of war." *Journal of Strategic Studies* 42 (6): 841-836.
- Schweller, Randall L. 2016. "The Balance of Power in World Politics." In *Oxford Research Encyclopedias*, 1-20. Oxford University Press.
- Scimago. n.d. *Scimago Journal and Country Rank*. Accessed December 2019. <https://www.scimagojr.com/>.
- Seals, Tara. 2018. "Russia, China's Cyber-Capabilities Are Catastrophic." *Info Security*, January 18. <https://www.infosecurity-magazine.com/news/russia-chinas-cybercapabilities/>.
- Senese, Paul D, and John A Vasquez. 2008. *The Steps to War: An Empirical Study*. Princeton: Princeton University Press.
- Shalal-Esa, Andrea. 2013. "Iran strengthened cyber capabilities after Stuxnet: US General." *Reuters*, January 13. Accessed December 2019. <https://www.reuters.com/article/us-iran-usa-cyber/iran-strengthened-cyber-capabilities-after-stuxnet-u-s-general-idUSBRE90G1C420130118>.
- Shimshoni, J. 1988. *Israel and conventional deterrence: Border warfare from 1953 to 1970*. Ithaca: Cornell University Press.
- Shiping, Tang. 2010. "Offence-defence Theory: A Definitive Understanding." *The Chinese Journal of International Politics* 3: 213-260.
- Singer, J David. 1988. "Reconstructing the Correlates of War Dataset on Material Capabilities of States, 1816-1985." *International Interactions* 14 (2): 115-132.
- Singer, J David, Stuart Bremer, and John Stuckey. 1972. "Capability Distribution, Uncertainty and Major Power War, 1820-1965." In *Peace, War, and Number*, edited by Bruce Russett, 19-48. Beverly Hills: Sage.
- Singer, P W, and Emerson T Brooking. 2018. *LikeWar: The Weaponization of Social Media*. New York : Houghton Mifflin Harcourt Publishing Company .
- Singer, P. W, and Allan Friedman. 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press.
- Singh, Sonali, and Christopher Way. 2004. "The Correlates of Nuclear Proliferation." *Journal of Conflict Resolution* 48 (6): 859-885.
- Siverson, Randolph M, and Harvey Starr. 1990. "Opportunity, Willingness, and the Diffusion of War." *American Political Science Review* 84 (1): 47-67.

- Skolnikoff, Eugene B. 1993. *The Elusive Transformation: Science, Technology, and the Evolution of International Politics*. Princeton: Princeton University Press.
- Slayton, Rebecca. 2017. "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment." *International Security* 41 (3): 72-109.
- Small Media. 2017. "Filterwatch: Iranian Internet Infrastructure and Policy Report." Accessed December 2019. <https://smallmedia.org.uk/news/filterwatch-october-2017>.
- Small Media. 2015. "Iranian Infrastructure and Policy Report." Accessed 2016. [http://smallmedia.org.uk/sites/default/files/u8/200215_InternetInfrastructure%20\(1\).pdf](http://smallmedia.org.uk/sites/default/files/u8/200215_InternetInfrastructure%20(1).pdf).
- . 2014. "Iranian Internet Infrastructure and Policy Report." February. Accessed September 8, 2020. https://smallmedia.org.uk/sites/default/files/u8/IIIP_Feb2014.pdf.
- Smeets, Max. 2018. "A matter of time: On the transitory nature of cyberweapons." *The Journal of Strategic Studies* 41 (1-2): 6-32. <https://www.tandfonline.com/doi/pdf/10.1080/01402390.2017.1288107?needAccess=true>.
- Smeets, Max. 2018. "The Strategic Promise of Offensive Cyber Operations." *Strategic Studies Quarterly* (Sr) 90-113.
- Software Engineering Institute. n.d. *The CERT Division*. Accessed December 2019. <https://www.sei.cmu.edu/about/divisions/cert/index.cfm#history>.
- Solon, Olivia. 2016. "Hacking group auctions 'cyber weapons' stolen from NSA." *The Guardian*, August 16. <https://www.theguardian.com/technology/2016/aug/16/shadow-brokers-hack-auction-nsa-malware-equation-group>.
- Sprout, H, and Sprout M. 1965. *The Ecological Perspective on Human Affairs, with Special Reference to International Politics*. Princeton: Princeton University Press.
- Sprout, Harold, and Margaret Sprout. 1969. "Environmental Factors in the Study of International Politics." In *International Politics and Foreign Policy*, edited by J D Rosenau. New York: Free Press.
- Starr, Harvey. 1978. "'Opportunity' and 'willingness' as ordering concepts in the study of war." *International Interactions* 4 (4): 363-387.
- Sterling, Bruce. 2019. "Iranian National Cyberspace." *Wired*, November 18. <https://www.wired.com/beyond-the-beyond/2019/11/iranian-national-cyberspace/>.
- Stevens, Tim. 2012. "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace." *Contemporary Security Studies* 33: 148-170.
- . 2016. *Cyber Security and the Politics of Time*. Cambridge: Cambridge University Press.
- Stevens, Tim. 2017. "Cyberweapons: an emerging global governance architecture." *Palgrave Communications* 1-6. <https://www.nature.com/articles/palcomms2016102.pdf>.
- Stevens, Tim. 2017. "Cyberweapons: Power and the Governance of the Invisible." *International Politics* 55: 482-502.
- Stevens, Tim. 2019. "Strategic cyberterrorism: problems of ends, ways and means." In *Handbook of Terrorism and Counter Proliferation Post 9/11*, edited by David Martin Jones, Paul Schulte, Carl Ungerer and Smith M L R, 42-52. Cheltenham: Edward Elgar Publishing Limited.

- Stone, John. 2013. "Cyber War Will Take Place!" *Journal of Strategic Studies* 36 (1): 101-108.
- Strickland, Lawrence, and Jonah Force Hill. 2017. "Multi-stakeholder internet governance: successes and opportunities." *Journal of Cyber Policy* 2 (3): 296-317.
<https://www.tandfonline.com/doi/pdf/10.1080/23738871.2017.1404619?needAccess=true>.
- Sui Ngan Ng, Sharon, and Nirmala Rao. 2010. "Chinese Number Words, Culture, and Mathematics Learning." *Review of Educational Research* 80 (2): 180-206.
<https://www.jstor.org/stable/40658461>.
- Sulek, David, and Ned Moran. 2009. "What Analogies Can Tell Us About the Future of Cybersecurity." In *The Virtual Battlefield: Perspectives on Cyber Warfare*, edited by Christian Czosseck and Kenneth Geers, 118-131. IOS Press.
- Tabansky, Lior, and Isaac Ben Israel. 2015. *Cybersecurity in Israel*. New York: Springer.
- Tankard, Colin. 2011. "Advanced Persistent threats and how to monitor and detect them." *Network Security* 2011 (8): 16-19.
- The Economist*. 2010. "War in the Fifth Domain - Are the mouse and keyboard the new weapons of conflict?" July 1. <https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain>.
- The Irish Times. 2012. "Obama 'sped up' Iran cyberattacks." *The Irish Times*, June 1.
<https://www.irishtimes.com/news/obama-sped-up-iran-cyberattacks-1.717795>.
- The United States Army. 2010. *Cyberspace Operations Concept Capability Plan 2016-2028*. February 22. <https://fas.org/irp/doddir/army/pam525-7-8.pdf>.
- The World Bank. n.d. *World Development Indicators*. Accessed December 2019.
<http://datatopics.worldbank.org/world-development-indicators/>.
- Tofangsazi, Bashir. 2020. "From the Islamic Republic to the Green Movement: Social Movements in Contemporary Iran." *Sociological Compass* 14 (1): 1-16.
<https://onlinelibrary.wiley.com/doi/epdf/10.1111/soc4.12746>.
- UNIDIR. 2013. *The Cyber Index: International Security Trends and Realities*. Geneva: United Nations Institute for Disarmament Research.
- UNIDIR. 2013. *The Cyber Index: International Security Trends and Realities*. United Nations Institute for Disarmament Research. <https://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf>.
- United Nations. 2015. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." <https://dig.watch/un-gge-report-2015-a70174>.
- United Nations. 2014. "World Economic Situation and Prospects." Accessed December 2019.
https://www.un.org/en/development/desa/policy/wesp/wesp_current/2014wesp_country_classification.pdf.
- Usborne, David. 2012. "Cyber attack on US 'could be as damaging as 9/11'." *The Independent*, October 13. <https://www.independent.co.uk/news/world/americas/cyber-attack-us-could-be-damaging-9-11-8209821.html>.
- Valeriano, Brandon. 2013. *Becoming Rivals: The Process of Interstate Rivalry Development*. New York: Routledge.

- Valeriano, Brandon, and Ben Jensen. 2019. "How cyber operations can help manage crisis escalation with Iran." *Washington Post*, June 25.
<https://www.washingtonpost.com/politics/2019/06/25/how-cyber-operations-can-help-manage-crisis-escalation-with-iran/>.
- Valeriano, Brandon, and Ryan C Maness. 2015. *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*. New York: Oxford University Press.
- Valeriano, Brandon, and Ryan C Maness. 2014. "The dynamics of cyber conflict between rival antagonists 2000-2011." *Journal of Peace Research* 51 (3): 347-360.
- Valeriano, Brandon, and Ryan Maness. 2018. "How We Stopped Worrying about Cyber Doom and Started Collecting Data." *Politics and Governance* 6 (2).
<https://www.cogitatiopress.com/politicsandgovernance/article/view/1368>.
- Valeriano, Brandon, Benjamin Jensen, and Ryan C Maness. 2018. *Cyber Strategy: The Evolving Character of Power and Coercion*. New York: Oxford University Press.
- Van Evera, Stephen. 2001. *Causes of War: Power and the Roots of Conflict*. Cornell University Press.
- Van Evera, Stephen. 1998. "Offense, Defense, and the Causes of War." *International Security* 22 (4): 5-43.
- Vasquez, John A. 2004. *The Power of Power Politics*. Cambridge: Cambridge University Press.
- . 2009. *The War Puzzle Revisited*. Cambridge: Cambridge University Press.
- Voo, Julia, Irfan Hemani, Simon Jones, Winona DeSombre, Daniel Cassidy, and Anina Schwarzenbach. 2020. *National Cyber Power Index 2020: Methodological and Analytical Considerations*. Belfer Center for Science and International Affairs, Harvard Kennedy School. https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf.
- Wakefield, Jane. 2019. "Russia 'successfully tests' its unplugged internet." *BBC News*, December 24. <https://www.bbc.co.uk/news/technology-50902496>.
- Wallace, Michael M D. 1979. "Arms Races and Escalation: Some New Evidence." *Journal of Conflict Resolution* 23 (1): 3-16.
- Walt, Stephen M. 2010. "Is the Cyber Threa Overblown." *Foreign Policy*, March 30.
- Waltz, Kenneth N. 1990. "Nuclear Myths and Political Realities." *American Political Science Review* 84 (3): 731-745.
- . 1979. *Theory of International Politics*. London: Addison-Wesley.
- Wehrey, Frederic, Theodore W Karasik, Alireza Nader, Jeremy Ghez, Lydia Hansell, and Robert A Guffey. 2009. *Saudi_Iranian Relations Since the Fall of Saddam: Rivarly, Cooperation, and Implications for U.S. Policy*. RAND National Security Research Division.
- West-Brown, Moira. 2003. "Handbook for Computer Security Incident Response Teams (CSIRTs)." Carnegie Mellon Software Engineering Insitute, Pittsburgh.
https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf.
- Whyte, Chris, and Brian Mazanec. 2019. *Understanding Cyber Warfare: Politics, Policy, Strategy*. London: Routledge.

- Williams, Greg. 2017. "From the Editor: how Russia hacked the internet." *Wired*. May 4, 2017. <https://www.wired.co.uk/article/from-the-editor-june-2017>
- Wilner, Alex S. 2015. *Deterring Rational Fanatics*. Philadelphia: University of Pennsylvania.
- Wohlforth, William C. 2008. "Realism." In *The Oxford Handbook of International Relations*, edited by Christian Reus-Smit and Duncan Snidal. Oxford: Oxford University Press.
- Wohlforth, William C. 1999. "The Stability of a Unipolar World." *International Security* 24 (1): 5-41.
- Wright, Morgan. 2018. "North Korea's nuclear threat is nothing compared to its cyber warfare capabilities." *The Hill*, June 6. <https://thehill.com/opinion/cybersecurity/390601-north-koreas-nuclear-threat-is-nothing-compared-to-its-cyber-warfare>.
- Wright, Quincy. 1964. *A Study of War*. revised edition. Chicago: University of Chicago Press.
- Xinhua News. 2018. "Czech military to build cyber forces headquarters." *Xinhua News*, July 17. http://www.xinhuanet.com/english/europe/2018-07/17/c_137329274.htm.
- Zetter, Kim. 2014. *Countdown to Zero: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown Publishers.
- . 2012. "Meet 'Flame,' The Massive Spy Malware Infiltrating Iranian Computers." *Wired*, May 28. <https://www.wired.com/2012/05/flame/>.
- Zisser, Eyal. 2011. "Iranian Involvement in Lebanon." *Military and Strategic Affairs* 3 (1): 3-16. [https://www.inss.org.il/wp-content/uploads/sites/2/systemfiles/\(FILE\)1308129458.pdf](https://www.inss.org.il/wp-content/uploads/sites/2/systemfiles/(FILE)1308129458.pdf).

Appendix: Active cyber capability and strategy data

National Computer Security Incident Response Teams (CSIRTs) (2000-2017)				
<i>Id</i>	<i>CSIRT name</i>	<i>Country</i>	<i>Year established</i>	<i>Sources</i>
1	AFCERT	Afghanistan	2009	http://mcit.gov.af/Content/files/National%20Cybersecurity%20Strategy%20of%20Afghanistan%20(November2014).pdf ; https://unidir.org/cpp/en/states/afghanistan
2	ALCIRT	Albania	2011	http://cyberalbania.al/?page_id=971 ; https://cesk.gov.al/publicAnglisht_html/rreth-nesh/organizimi/index.html
3	ArCERT	Argentina	1999	http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/61122/norma.htm ; http://www.internationalcybercenter.org/certicc/certoas
4	ICIC-CERT	Argentina	2011	https://www.first.org/members/teams/icic-cert ; https://www.cybersecurityintelligence.com/critical-infrastructures-for-information-and-cybersecurity-icic--2741.html
5	CERT-AM	Armenia	2007	https://www.trusted-introducer.org/directory/teams/cert-am.html ; https://www.cert.am/
6	GovCERT.au	Australia	2005	http://itlaw.wikia.com/wiki/GovCERT.au ; https://www.auscert.org.au/
7	CERT Australia	Australia	2010	https://www.cyber.gov.au/acsc/view-all-content/glossary/cert-australia ; https://www.zdnet.com/article/cert-aus-opens-has-beers-with-auscert/
8	GovCERT.at	Austria	2008	http://www.govcert.gv.at/ ; https://www.cybersecurityintelligence.com/govcert-austria-4610.html
9	CERT.GOV.AZ	Azerbaijan	2008	https://cert.gov.az/az/pages/2 ; https://www.first.org/members/teams/cert-gov-az
10	CERT.AZ	Azerbaijan	2013	https://www.cert.az/s/u/document/rfc_2350.pdf ; https://www.first.org/members/teams/cert-az
11	BGD E-GOV CIRT	Bangladesh	2016	https://www.cirt.gov.bd/about-us/ ; https://www.trusted-introducer.org/directory/teams/bgd-e-gov-cirt.html
12	CERT.BY	Belarus	2012	https://cert.by/?lang=en ; https://www.first.org/members/teams/cert-by
13	CERT.Be	Belgium	2009	https://www.trusted-introducer.org/directory/teams/certbe.html ; https://www.cert.be/language_selection?destination=%3Cfront%3E
14	bjCSIRT	Benin	2017	https://csirt.gouv.bj/ ; https://www.africert.org/african-csirts/
15	btCSIRT	Bhutan	2017	https://www.btcert.bt/ ; http://www.ft.lk/article/591951/Sri-Lanka-CERT%7CCC-trains-Bhutan-Computer-Incident-Response-Team
16	CSIRT-BO	Bolivia	2015	https://cgii.gob.bo/es/acerca-del-cgii ; https://unidir.org/cpp/en/states/bolivia

17	CERT RS	Bosnia and Herzegovina	2017	https://oib.aidrs.org/ ; http://www.msb.gov.ba/dokumenti/strateski/default.aspx?id=6248&langTag=bs-BA
18	CERT.BR	Brazil	1997	https://www.cert.br/sobre/ ; https://www.first.org/members/teams/cert-br
19	CTIR Gov	Brazil	2004	https://www.ctir.gov.br/ ; https://igarape.org.br/wp-content/uploads/2019/01/A-Strategy-for-Cybersecurity-Governance-in-Brazil.pdf
20	BruCERT	Brunei	2004	https://www.first.org/members/teams/brucert ; https://www.cybersecurityintelligence.com/brucert-1920.html
21	CERT Bulgaria	Bulgaria	2008	https://www.trusted-introducer.org/directory/teams/cert-bulgaria.html ; https://www.govcert.bg/EN/Pages/default.aspx
22	CIRT.Bf	Burkina Faso	2012	http://www.cirt.bf/index.php/a-propos/ ; https://www.sei.cmu.edu/education-outreach/computer-security-incident-response-teams/national-csirts/
23	CamCERT	Cambodia	2010	https://www.camcert.gov.kh/en/who-we-are/ ; https://www.jica.go.jp/project/cambodia/0609376/04/pdf/03_gisms_v1_e4.pdf
24	CIRT/ANTIC	Cameroon	2012	https://www.coe.int/en/web/octopus-old2019/country-wiki1/-/asset_publisher/hFPA5fbKjyCJ/content/cameroon?inheritRedirect=false ; https://www.itu.int/en/ITU-D/Capacity-Building/Documents/IG_workshop_August2018/Presentations/Session5_SergeZongorev.pdf
25	CCIRC	Canada	2003	https://www.first.org/members/teams/ccirc ; https://www.publicsafety.gc.ca/cnt/trnsprnc/ccss-nfrmtn-prvc/prvc-mpct-sssmnt/cndn-cbr-ncdnt-en.aspx
26	CSIRT-CL	Chile	2004	https://www.csirt.gob.cl/ ; https://www.coe.int/bg/web/octopus-old2019/country-wiki1/-/asset_publisher/hFPA5fbKjyCJ/content/chile?_101_INSTANCE_hFPA5fbKjyCJ_viewMode=view/
27	CNCERT/CC	China	2002	http://www.cert.org.cn/publish/english/index.html ; https://www.first.org/members/teams/cncert-cc
28	ColCERT	Colombia	2012	http://www.colcert.gov.co/?q=acerca-de ; https://www.cybersecurityintelligence.com/colcert-2735.html
29	CSIRT-CR	Costa Rica	2012	https://publications.iadb.org/handle/11319/7449 ; https://www.micit.go.cr/tags/ciberseguridad
30	CI CERT	Cote d'Ivoire	2009	http://www.cicert.ci/qui-sommes-nous/ ; https://www.cybersecurityintelligence.com/ci-cert-4898.html
31	CERT ZSIS	Croatia	2007	https://www.first.org/members/teams/cert_zsis ; https://www.zsis.hr/default.aspx?id=114
32	CERT HR	Croatia	2009	https://www.first.org/members/teams/cert-hr ; https://www.cert.hr/
33	CSIRT-CY	Cyprus	2016	https://csirt.cy/ ; https://www.trusted-introducer.org/directory/teams/csirt-cy.html
34	CSIRT.CZ	Czech Republic	2008	https://www.csirt.cz ; https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map#country=Czech%20Republic
35	GOVCERT.CZ	Czech Republic	2012	https://www.govcert.cz/en/government-cert/govcert-cz/ ; https://www.first.org/members/teams/govcert-cz
36	Danish GovCERT	Denmark	2009	https://www.trusted-introducer.org/directory/teams/cfcs.html ; https://www.cybersecurityintelligence.com/danish-govcert-1962.html

37	EcuCERT	Ecuador	2013	https://www.first.org/members/teams/ecucert ; https://www.ecucert.gob.ec/
38	EG-CERT	Egypt	2009	http://www.egcert.eg/about-us ; http://www.mcit.gov.eg/
39	CERT-EE	Estonia	2006	https://www.ria.ee/en/cert-estonia.html ; https://www.first.org/members/teams/cert-ee
40	Ethio-CERT	Ethiopia	2012	https://www.first.org/members/teams/ethio-cert ; http://ethiocert.insa.gov.et/
41	CERT-FI	Finland	2002	https://www.viestintavirasto.fi/en/cybersecurity/cert-fi.html ; https://www.kyberturvallisuuskeskus.fi/en/our-activities/cert
42	CERT-FR	France	1999	https://www.ssi.gouv.fr/actualite/creation-du-cert-fr/ ; https://www.trusted-introducer.org/directory/teams/cert-fr.html
43	CERT-GOV-GE	Georgia	2011	http://www.cert.gov.ge/ ; https://www.trusted-introducer.org/directory/teams/cert-gov-ge.html
44	CERT-Bund	Germany	2001	https://www.bsi.bund.de/EN/Topics/IT-Crisis-Management/CERT-Bund/cert-bund_node.html ; https://www.first.org/members/teams/cert-bund
45	CERT-GH	Ghana	2014	https://www.cert-gh.org/about/constituency/ ; https://www.cybersecurityintelligence.com/cert-gh-4904.html
46	NCERT-GR	Greece	2009	https://www.trusted-introducer.org/directory/teams/ncert-gr.html ; http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_greece.pdf
47	CERT.gy	Guyana	2013	https://cirt.gy/cirt.gy/about.html ; https://ndma.gov.gy/pillars/cybersecurity/
48	GovCERT-Hungary	Hungary	2013	http://www.cert-hungary.hu/ ; https://www.first.org/members/teams/cert-hungary
49	CERT-IS	Iceland	2013	https://www.cert.is/en/node/2.html ; https://www.trusted-introducer.org/directory/teams/cert-is.html
50	CERT-In	India	2004	https://cert-in.org.in/ ; https://www.financialexpress.com/opinion/getting-cyber-defences-ready-india-needs-a-robust-cybersecurity-policy/2077314/
51	ID-SIRT/CC	Indonesia	2007	https://www.first.org/members/teams/id-sirtii-cc ; https://www.itu.int/ITU-D/finance/work-cost-tariffs/events/tariff-seminars/vietnam09-tas/pdf/Gunawan_SIRT.pdf
52	Gov-CSIRT	Indonesia	2012	https://govcsirt.bssn.go.id/ ; https://www.kominfo.go.id/content/detail/3263/gov-csirt-government-computer-security-incident-response-team/0/kemanan_informasi
53	CERT MAHER	Iran	2008	https://www.certcc.ir/index ; http://www.itu.int/net/wsis/implementation/2013/forum/agenda/session_docs/Day4/113/Panelist3-Radkani.pdf
54	CSIRT-IE	Ireland	2011	https://www.ncsc.gov.ie/CSIRT/ ; https://www.cybersecurityintelligence.com/csirt-ie-4617.html
55	CERTGOVIL	Israel	2006	https://www.first.org/members/teams/certgovil ; https://www.trusted-introducer.org/directory/teams/certgovil.html
56	CERT-IL	Israel	2014	https://www.first.org/members/teams/cert-il ; https://il-cert.org.il/

57	CERT IT	Italy	2014	https://www.certnazionale.it/chi-siamo/ ; https://www.cyberwiser.eu/italy-it
58	CERT-PA	Italy	2014	https://www.dataguidance.com/news/italy-security-information-system-announces-csirt-beginning-activities ; https://www.agid.gov.it/en/security/cert-pa
59	JPCERT/CC	Japan	1996	https://www.jpccert.or.jp/english/about/index.html ; https://www.cybersecurityintelligence.com/jpccert-cc-2721.html
60	KZ-CERT	Kazakhstan	2011	https://www.first.org/members/teams/kz-cert ; https://www.cybersecurityintelligence.com/kz-cert-2759.html
61	KE-CIRT/CC	Kenya	2012	http://www.ke-cirt.go.ke/index.php/about-us/ ; https://www.cybersecurityintelligence.com/ke-cirt-cc-2760.html
62	LaoCERT	Laos	2012	https://www.laocert.gov.la/en/Page-1- ; https://www.cybersecurityintelligence.com/laocert-4900.html
63	CERT.LV	Latvia	2006	https://cert.lv/en/about-us
64	CERTLibya	Libya	2013	https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Libya.pdf ; https://www.africert.org/libya/
65	CERT-LT	Lithuania	2006	https://www.trusted-introducer.org/directory/teams/nksc/cert-lt.html ; https://www.nksc.lt/pranesti.html
66	GOVCERT.LU	Luxembourg	2011	https://www.govcert.lu/en/
67	MKD CIRT	Macedonia	2016	https://mkd-cirt.mk/about-mkd-cirt/rfc2350/constituents/?lang=en ; https://www.trusted-introducer.org/directory/teams/mkd-cirt.html
68	MyCERT	Malaysia	1997	https://www.mycert.org.my/en/about/about_us/main/detail/344/index.html
69	MT CSIRT	Malta	2002	https://www.trusted-introducer.org/directory/teams/mt-csirt.html ; https://www.first.org/members/teams/mt-csirt
70	CERT-MU	Mauritius	2008	https://www.first.org/members/teams/cert-mu ; https://itlaw.wikia.org/wiki/CERT-MU
71	CERT-MX	Mexico	2010	https://www.first.org/members/teams/cert-mx ; https://www.cert.org.mx/
72	CERT-GOV-MD	Moldova	2010	https://stisc-cert.gov.md/?lang=en ; https://www.cybersecurityintelligence.com/cert-gov-md-2763.html
73	CERT-MC	Monaco	2015	https://www.trusted-introducer.org/directory/teams/cert-mc.html ; https://www.first.org/members/teams/cert-mc
74	CIRT.ME	Montenegro	2012	https://www.trusted-introducer.org/directory/teams/cirtme.html ; http://cirt.me/cirt
75	MaCERT	Morocco	2011	https://www.dgssi.gov.ma/presentation/dgssi/organisation.html ; https://www.first.org/members/teams/macert
76	mmCERT	Myanmar	2004	https://www.mmcert.org.mm/index.php/about-us.html

77	CERT-RO/GOVCERT.NL	Netherlands	2002	https://www.ncsc.nl/ ; https://www.trusted-introducer.org/directory/teams/ncsc-nl.html
78	CERT.NZ	New Zealand	2017	https://www.cert.govt.nz/about/about-us/
79	ngCERT	Nigeria	2015	https://www.cert.gov.ng/ ; https://www.first.org/members/teams/ngcert
80	NorCERT	Norway	2004	https://nsm.stat.no/norcet/
81	OCERT	Oman	2010	http://www.cert.gov.om/about.aspx#.XA6G02j7TIU
82	CSIRT Panama	Panama	2011	https://cert.pa/ ; https://www.coe.int/hy/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/content/panama/pop_up?_101_INSTANCE_hFPA5fbKjyCJ_viewMode=print&_101_INSTANCE_hFPA5fbKjyCJ_languageId=hy_AM
83	CERT.Py	Paraguay	2012	https://www.cert.gov.py/index.php/certpy
84	PeCERT	Peru	2009	https://www.peru.gob.pe/pecert/
85	NCERT	Philippines	2017	https://ncert.gov.ph/
86	CERT Polska	Poland	1996	https://www.cert.pl/ ; https://www.trusted-introducer.org/directory/teams/cert-polska.html
87	CERT.GOV.PL	Poland	2008	https://www.cert.gov.pl
88	CERT.PT	Portugal	2015	https://www.cncs.gov.pt/certpt/
89	QCERT	Qatar	2005	http://www.qcert.org/
90	CERT-RO	Romania	2011	https://cert.ro/ ; https://www.first.org/members/teams/cert-ro
91	RU-CERT	Russia	1998	https://www.cert.ru/en/about.shtml
92	CERT-GOV.RU	Russia	2012	http://www.gov-cert.ru/
93	RwCERT	Rwanda	2014	http://rw-csirt.rw/eng/about-us/history.php
94	CERT SA	Saudi Arabia	2006	http://www.cert.gov.sa/index.php?option=com_content&task=view&id=69&Itemid=116
95	SingCERT	Singapore	1997	https://www.csa.gov.sg/singcert/about-us
96	SG-GITSIR	Singapore	2016	https://www.tech.gov.sg/products-and-services/gitsir/ ; https://www.first.org/members/teams/sg-gitsir
97	CSIRT. SK	Slovakia	2009	https://www.csirt.gov.sk/

98	SK-CERT	Slovakia	2016	https://www.sk-cert.sk/sk/o-nas/index.html ; https://www.trusted-introducer.org/directory/teams/sk-cert.html
99	SI CERT	Slovenia	1994	https://www.cert.si/en/ ; https://www.trusted-introducer.org/directory/teams/si-cert.html
100	ECS-CSIRT	South Africa	2003	www.ssa.gov.za/CSIRT.aspx
101	KN-CERT	South Korea	2004	https://www.first.org/members/teams/kn-cert ; https://unidir.org/cpp/en/states/republicofkorea
102	KrCERT.CC	South Korea	2010	https://www.krcert.or.kr/krcert/intro.do ; https://unidir.org/cpp/en/states/republicofkorea
103	CNN-CERT	Spain	2006	https://www.ccn-cert.cni.es/ ; https://www.trusted-introducer.org/directory/teams/ccn-cert.html
104	CERT-Seguridad Industria	Spain	2012	https://www.certs.es/sobre-certs/que-es-certs
105	Sri Lanka CERT/CC	Sri Lanka	2006	http://www.slcert.gov.lk/aboutUs.php
106	Sudan-CERT	Sudan	2010	http://www.cert.sd/
107	CERT-SE	Sweden	2003	https://www.cert.se/om-cert-se
108	GovCERT.ch	Switzerland	2008	https://www.govcert.admin.ch/
109	CERT Syria	Syria	2009	https://www.cybersecurityintelligence.com/cert-syria-2774.html ; https://www.nans.gov.sy/en/
110	TWCERT/CC	Taiwan	1998	https://www.twcert.org.tw/tw/mp-1.html ; https://www.first.org/members/teams/twcert-cc
111	TWNCERT	Taiwan	2003	https://www.twncert.org.tw/ ; https://www.twncert.org.tw/About?lang=en
112	TZ-CERT	Tanzania	2010	https://www.tzcert.go.tz/about-us/
113	ThaiCERT	Thailand	2000	https://www.first.org/members/teams/thaicert ; https://www.thaicert.or.th/about-en.html
114	CERT Tonga	Tonga	2016	https://www.cert.gov.to/
115	TunCERT	Tunisia	2004	https://www.first.org/members/teams/tuncert ; https://www.ansi.tn/tuncert/presentation
116	TR-CERT	Turkey	2007	https://www.trusted-introducer.org/directory/teams/tr-cert.html ; https://www.first.org/members/teams/tr-cert
117	UgCERT	Uganda	2013	http://www.ug-cert.ug/data/smenu/17/Roles-and-Functions.html
118	CERT-UA	Ukraine	2007	https://www.cert.gov.ua/

119	CERTae	United Arab Emirates	2008	https://www.tra.gov.ae/aecert/ar/about-us/vision-mission-goals.aspx
120	GovCERT UK	United Kingdom	2007	https://www.trusted-introducer.org/directory/teams/ncsc-(uk).html ; https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf
121	CERT-UK	United Kingdom	2014	https://www.gov.uk/government/news/uk-launches-first-national-cert ; https://wiki.openrightsgroup.org/wiki/CERT-UK
122	FedCERT	United States	2000	http://itlaw.wikia.com/wiki/Federal_Computer_Incident_Response_Center ; https://www.rand.org/content/dam/rand/pubs/monograph_reports/2007/MR976.pdf
123	CERT-US	United States	2003	https://www.us-cert.gov/about-us
124	CERTuy	Uruguay	2008	https://www.first.org/members/teams/certuy ; https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/
125	UZ-CERT	Uzbekistan	2005	https://uzcert.uz/ ; https://freedomhouse.org/report/freedom-net/2017/uzbekistan
126	VenCERT	Venezuela	2008	http://www.suscerte.gob.ve/?page_id=1736 ; http://www.vencert.gob.ve/es-ve/
127	VNCERT	Vietnam	2005	http://www.vncert.gov.vn/gioi-thieu.php
128	SRB-CERT	Serbia	2017	https://www.cert.rs/stranica/57-O+Nacionalnom+CERT-u.html
129	ZmCIRT	Zambia	2012	https://www.first.org/members/teams/zmcirt ; http://www.daily-mail.co.zm/zambia-hosts-first-cyber-security-drill/ ; http://www.cirt.zm/

National Cyber Security Strategy (NCSS) documents (2000-2017)

<i>Id</i>	<i>NCSS name</i>	<i>Country</i>	<i>Year published</i>	<i>Sources</i>
1	National Cyber Security Strategy of Afghanistan	Afghanistan	2014	http://nic.af/Content/files/National%20Cybersecurity%20Strategy%20of%20Afghanistan%20(November2014).pdf
2	Cyber Security Policy Paper 2015-2017	Albania	2015	http://ncsi.ega.ee/app/uploads/2016/05/Policy-Paper-on-Cyber-Security-2015-2017-Eng.doc
3	Cyber Security Strategy	Australia	2009	http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf
4	Australia's Cyber Security Strategy	Australia	2016	https://www.homeaffairs.gov.au/cyber-security-subsite/files/PMC-Cyber-Strategy.pdf
5	Austrian Cyber Security Strategy	Austria	2013	https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AT_NCSS.pdf

6	National Cyber Security Strategy	Bangladesh	2014	http://www.dpp.gov.bd/upload_file/gazettes/10041_41196.pdf
7	Cyber Security Strategy	Belgium	2012	https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/belgian-cyber-security-strategy/view
8	Security Strategy of Information and Communications and Cybersecurity of the Public Federal Administration	Brazil	2015	https://www.article19.org/resources/brazil-cyber-security-strategy/
9	National Cyber Strategy "Cyber sustainable 2020"	Bulgaria	2016	https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-6/view
10	National Cybersecurity Plan	Burkina Faso	2010	https://unidir.org/cpp/en/state-pdf-export/eyJjb3VudHJ5X2dyb3VwX2lkIjoiNSJ9
11	Canada's Cyber Security Strategy	Canada	2010	https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/archive-cbr-scrt-strtyg/archive-index-en.aspx
12	National Cybersecurity Policy	Chile	2017	https://www.unodc.org/e4j/data/_university_uni_/chiles_national_cybersecurity_policy_2017-2022.html?lng=en
13	National Cyberspace Strategy	China	2016	https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/
14	National Digital Security Policy	Colombia	2016	https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf
15	Policy Guidelines on Cybersecurity and Cyberdefence	Colombia	2011	https://www.sites.oas.org/cyber/Documents/Colombia%20-%20National%20Cybersecurity%20and%20Cyberdefense%20Policy.pdf
16	The National Cyber Security Strategy of The Republic of Croatia	Croatia	2015	https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/croatian-cyber-security-strategy
17	Cybersecurity Strategy of the Republic of Cyprus	Cyprus	2012	https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CybersecurityStrategyoftheRepublicofCyprusv10_English.pdf/view
18	Cyber Security Strategy of the Czech Republic for the 2011-2015 period	Czech Republic	2011	https://www.enisa.europa.eu/media/news-items/CZ_Cyber_Security_Strategy_20112015.PDF
19	National Cyber Security Strategy of the Czech Republic	Czech Republic	2015	https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-of-czech-republic-2011-2015

20	The Danish Cyber and Information Security Strategy	Denmark	2015	https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-strategy-for-cyber-and-information-security
21	National Cybersecurity Strategy	Egypt	2017	https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/EgyptNational%20Cybersecurity%20Strategy-English%20version-18%20Nov%202018.pdf
22	Cyber Security Strategy	Estonia	2008	https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy/@_@download_version/993354831bfc4d689c20492459f8a086/file_en
23	Cyber Security Strategy	Estonia	2014	https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf
24	National Information Security Policy of the Federal Democratic Republic of Ethiopia	Ethiopia	2011	https://www.insa.gov.et/documents/20124/0/National+Informattion+Security+Policy.pdf/45e78efa-d671-4fbc-16c7-38eb1c70e35d?t=1600929143177&download=true
25	Finland's Cyber security Strategy	Finland	2013	https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf
26	Information systems defence and security	France	2011	https://www.enisa.europa.eu/media/news-items/Information_system_security_France_strategy.pdf/at_download/file
27	National Digital Security Strategy	France	2015	https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/information-systems-defence-and-security-frances-strategy/@_@download_version/c7d0d0671bbc4756afd87513675d58eb/file_en
28	The Gambia National Cybersecurity Strategy	Gambia	2016	http://www.moici.gov.gm/gambia-national-cyber-security-strategy
29	Cyber Security Strategy of Georgia	Georgia	2012	https://sherloc.unodc.org/cld/lessons-learned/geo/cyber_security_strategy_of_georgia_2012-2015.html?
30	Cyber Security Strategy	Georgia	2017	https://matsne.gov.ge/ka/document/view/1923932
31	Cyber Security Strategy for Germany	Germany	2011	https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile
32	Cyber Security Strategy for Germany	Germany	2016	https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany/@_@download_version/5f3c65fe954c4d33ad6a9242cd5bb448/file_en
33	Ghana National Cyber Security Policy and Strategy	Ghana	2015	https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/National-Cyber-Security-Policy-Strategy-Revised_23_07_15.pdf
34	National Cyber Security Strategy	Greece	2017	https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-greece/@_@download_version/50cded9109d442e7839649f42055da60/file_en

35	National Cyber Security Strategy of Hungary	Hungary	2013	http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/HU_NCSS.pdf
36	Icelandic National Cyber Security Strategy 2015-2026	Iceland	2015	https://www.stjornarradid.is/media/innanrikisraduneyti-media/media/frettir-2015/Icelandic_National_Cyber_Security_Summary_loka.pdf
37	National Cyber Security Policy	India	2013	http://meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf
38	National Cyber Security Strategy	Indonesia	2017	https://bssn.go.id/strategi-keamanan-siber-nasional/
39	National Cyber Security Strategy 2015-2017	Ireland	2015	http://www.dccae.gov.ie/communications/SiteCollectionDocuments/Internet-Policy/NationalCyberSecurityStrategy20152017.pdf
40	Israel National Cyber Security Strategy	Israel	2017	https://cyber.haifa.ac.il/images/pdf/cyber_english_A5_final.pdf
41	National Strategic Framework For Cyberspace Security	Italy	2013	http://www.sicurezza nazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf
42	National Cyber Security Strategy	Jamaica	2015	http://mstem.gov.jm/sites/default/files/Jamaica%20National%20Cyber%20Security%20Strategy.pdf
43	The First National Strategy on Information Security	Japan	2006	https://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf
44	The Second National Strategy on Information Security	Japan	2009	https://www.nisc.go.jp/eng/pdf/national_strategy_002_eng.pdf
45	Information Security Strategy for Protecting the Nation	Japan	2010	https://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf
46	Cybersecurity Strategy: Towards a world-leading, resilient and vigorous cyberspace	Japan	2013	https://www.nisc.go.jp/eng/pdf/cybersecuritystrategy-en.pdf
47	Cybersecurity Strategy	Japan	2015	https://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf
48	National Information Assurance and Cyber Security Strategy	Jordan	2012	http://nitc.gov.jo/PDF/NIACSS.pdf

49	Cybersecurity Concept	Kazakhstan	2017	https://legalacts.egov.kz/npa/view?id=1714716 ; https://www.zakon.kz/4886464-utverzhdn-plan-meropriyatiy-po.html decree for approval of cyber shield https://online.zakon.kz/Document/?doc_id=37154346
50	National Cybersecurity Strategy	Kenya	2014	http://icta.go.ke/pdf/NATIONAL%20CYBERSECURITY%20STRATEGY.pdf
51	National Cyber Security Strategy for the State of Kuwait	Kuwait	2017	https://citra.gov.kw/sites/en/LegalReferences/English%20Cyber%20Security%20Strategy.pdf
52	Cyber Security Strategy of Latvia	Latvia	2014	http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/lv-ncss
53	National Cyber Security Policy Guidelines	Lebanon	2015	http://www.omsar.gov.lb/Cultures/en-US/ResourcesSupport/SupportAdministration/Documents/Lebanese%20National%20Cyber%20Security%20Policy%20Guidelines%20v1.7.pdf
54	Electronic information security (cyber security) Development 2011-2019 META PROGRAM	Lithuania	2011	http://www.ird.lt/doc/teises_aktai_en/EIS(KS)PP_796_2011-06-29_EN_PATAIS.pdf
55	National Strategy of Cyber Security	Luxembourg	2011	https://cybersecurite.public.lu/dam-assets/fr/scs-1-2011.pdf
56	National Cybersecurity Strategy II	Luxembourg	2015	https://securitymadein.lu/wp-content/uploads/2015/08/LU_NCSSL_2_EN_booklet.pdf
57	National Cybersecurity Strategy	Malawi	2017	https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/00019_07_Malawi%20national-cybersecurity-strategy.pdf
58	National Cyber Security	Malaysia	2006	https://www.nacsa.gov.my/ncsp.php
59	National Cyber Security	Malaysia	2009	https://www.itu.int/ITU-D/cyb/events/2009/hyderabad/docs/hashim-national-policy-malaysia-sept-09.pdf
60	Public Sector National Cyber Security Strategy	Malaysia	2016	https://www.nacsa.gov.my/doc/RAKKSSA-VERSI-1-APRIL-2016-BM.pdf
61	Malta Cyber Security Strategy	Malta	2016	https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Mita%20_Malta%20Cyber%20Security%20Strategy%20-%20Book.pdf
62	National Cyber security Strategy	Mauritius	2014	http://mtci.govmu.org/English/Documents/Final%20National%20Cyber%20Security%20Strategy%20November%202014.pdf
63	National Cybersecurity Strategy	Mexico	2017	https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

64	National Cyber Security Programme	Moldova	2015	http://old.mtic.gov.md/en/projects/cyber-security-programme
65	National Strategy for Digital Security	Monaco	2017	https://amsn.gouv.mc/var/amsn/storage/original/application/822de9d606448af4e900f566abd3e00c.pdf
66	National program on information security 2010-2015	Mongolia	2010	https://crc.gov.mn/en/k/1g/g
67	National Cyber Security Strategy for Montenegro	Montenegro	2013	http://www.mid.gov.me/ResourceManager/FileDownload.aspx%3Frid%3D165416%26rType%3D2%26file%3DCyber%2BSecurity%2BStrategy%2Bfor%2BMontenegro.pdf NATIONAL
68	Cyber Security Strategy of Montenegro	Montenegro	2017	http://www.ti.gov.me/ResourceManager/FileDownload.aspx?rid=305198&rType=2&file=Cyber%20Security%20Strategy%20of%20Montenegro%202018-2021%20eng.pdf
69	National Strategy in the matter of cybersecurity	Morocco	2012	https://www.dgssi.gov.ma/sites/default/files/attached_files/strategie_nationale.pdf
70	Mozambique's National Cybersecurity Strategy	Mozambique	2016	http://www.oam.org.mz/wp-content/uploads/2017/06/Draft_National_Cyber_Security_Strategy_Mozambique_PT_GT_24052017FINAL.pdf
71	National Cybersecurity Policy	Nepal	2016	https://nta.gov.np/wp-content/uploads/2018/05/Nepal-Cybersecurity-Policy-Draft.pdf
72	The National Cyber Security Strategy: Strength through cooperation	Netherlands	2011	https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Netherlands_Cyber_Security_strategy.pdf/
73	National Cyber Security Strategy 2: From awareness to capability	Netherlands	2014	https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf
74	New Zealand's Cyber Security Strategy	New Zealand	2011	http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/nzcybersecuritystrategyjune2011_0.pdf
75	New Zealand's Cyber Security Strategy	New Zealand	2015	http://www.dPMC.govt.nz/sites/all/files/publications/nz-cyber-security-strategy-december-2015.pdf
76	National Cybersecurity Strategy	Nigeria	2014	https://cert.gov.ng/images/uploads/NATIONAL_CYBESECURITY_STRATEGY.pdf
77	Cyber Security Strategy for Norway	Norway	2012	https://www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/cyber_security_strategy_norway.pdf
78	National Cyber Security Act	Pakistan	2014	http://www.senate.gov.pk/uploads/documents/1397624997_197.pdf

79	National Strategy for Cyber Security and Protection of Critical infrastructure	Panama	2013	https://www.unodc.org/res/cld/lessons-learned/pan/estrategia_nacional_de_seguridad_cibernetica_y_proteccion_de_infraestructuras_criticas_html/Estrategia_Nacional_de_Seguridad_Cibernetica_y_Proteccion_de_Infraestructuras_Criticas.pdf
80	National Plan for Cybersecurity	Paraguay	2017	http://gestordocumental.senatics.gov.py/share/s/zkKW1CkKScSvapqlB7UhNg
81	Philippine National Cyber Security Plan	Philippines	2005	https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Philippine_2005_National%20Cyber%20Security%20Plan%202005.pdf
82	National Cybersecurity Plan 2022	Philippines	2017	http://www.dict.gov.ph/wp-content/uploads/2017/04/FINAL_NationalCyberSecurityPlan2022.pdf
83	Cyberspace Protection Policy of the Republic of Poland	Poland	2013	http://www.cert.gov.pl/download/3/162/PolitykaOchronyCyberprzestrzeniRP148x210wersjaang.pdf
84	Cybersecurity Doctrine of the Polish Republic	Poland	2015	http://en.bbn.gov.pl/en/news/400,Cybersecurity-Doctrine-of-the-Republic-of-Poland.html
85	Cybersecurity Doctrine of the Republic of Poland	Poland	2017	https://en.bbn.gov.pl/en/news/400,Cybersecurity-Doctrine-of-the-Republic-of-Poland.html
86	Strategy of information and cyberspace security	Portugal	2013	https://comum.rcaap.pt/bitstream/10400.26/7757/1/idncaderno_12.pdf
87	National Cyberspace Security Strategy	Portugal	2015	https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/portuguese-ncss/@@download_version/a230c84ceaac4f5f8ba9da76a561b43d/file_en
88	Qatar National Cyber Security Strategy	Qatar	2014	http://www.ictqatar.qa/en/cyber-security/national-cyber-security-strategy
89	Cyber security strategy of Romania	Romania	2013	https://cert.ro/vezi/document/strategia-de-securitate-cibernetica
90	Information Security Doctrine of the Russian Federation	Russia	2000	https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf
91	Basic Principles for State Policy of the Russian Federation in the field of International Information Security to 2020	Russia	2013	https://www.cncs.gov.pt/content/files/ru_state-policy_information_security.pdf
92	Concept of a Cyber Security Strategy	Russia	2014	http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf

93	Information Security Doctrine of the Russian Federation (update)	Russia	2016	https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptlCk6BZ29/content/id/2563163
94	National Cyber Security Policy	Rwanda	2015	https://www.minict.gov.rw/fileadmin/Documents/National_Cyber_Security_Policy/Rwanda_Cyber_Security_Policy_01.pdf
95	Samoa National Cybersecurity Strategy	Samoa	2016	http://www.samoagovt.ws/wp-content/uploads/2017/02/MCIT-Samoa-National-Cybersecurity-Strategy-2016-2021.pdf
96	Developing National Information Security Strategy for the Kingdom of Saudi Arabia	Saudi Arabia	2013	https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/SaudiArabia_NISS_Draft_7_EN.pdf
97	Senegalese National Cybersecurity Strategy	Senegal	2017	https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/SNC2022-Senegal-NCS-Jan-2018_eng.pdf
98	Information Security Development Strategy	Serbia	2017	http://www.pravno-informacioni-sistem.rs/SIGlasnikPortal/eli/rep/sgrs/vlada/strategija/2017/53/1/reg
99	National Cyber Security and Data Protection Strategy	Sierra Leone	2017	https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/00090_03_Sierra%20Leone%20national-cyber-security-strategy-2017-final-draft.pdf
100	Infocomm Security Masterplan	Singapore	2005	https://www.imda.gov.sg/news-and-events/Media%20Room/archived/ida/Media%20Releases/2005/20050712110643
101	Infocomm Security Masterplan 2	Singapore	2008	https://www.qcert.org/sites/default/files/public/documents/SG-PL-Infocomm%20Security%20Masterplan%202-Eng-2008.pdf
102	National Cyber Security Masterplan	Singapore	2013	https://www.imda.gov.sg/-/media/Imda/Files/Inner/About-Us/Newsroom/Media-Releases/2013/0724_ncsm/AnnexA.pdf?la=en
103	Singapore's Cybersecurity Strategy	Singapore	2016	https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy/~/_media/0ecd8f671af2447890ec046409a62bc7.ashx
104	National Strategy for Information Security in the Slovak Republic	Slovakia	2008	https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Slovakia_National_Strategy_for_ISEC.pdf
105	Cyber Security Concept of the Slovak Republic	Slovakia	2015	http://www.rokovania.sk/File.aspx/ViewDocumentHtml/Mater-Dokum-187874
106	Cyber Security Strategy	Slovenia	2016	https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/si-ncss
107	Cyber Security Policy of South Africa	South Africa	2010	https://static.pmg.org.za/docs/100219cybersecurity.pdf
108	The National Cybersecurity Policy Framework	South Africa	2015	https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf

109	National Cyber Security Masterplan (summary)	South Korea	2011	http://www.sicurezzaibernetica.it/db/%5BSouth%20Korea%5D%20National%20Cyber%20Security%20Strategy%20-%202011%20-%20EN.pdf
110	National Cyber Security Strategy	Spain	2013	http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf
111	Strategy to improve Internet security in Sweden	Sweden	2006	https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Sweden_2006_Strategy_Internet_security_2006_12_July_2006.pdf
112	Strategy for information security in Sweden	Sweden	2010	https://www.msb.se/siteassets/dokument/publikationer/english-publications/strategy-for-information-security-in-sweden.pdf
113	A national cyber security strategy	Sweden	2017	https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/swedish-national-cyber-security-strategy/@_download_version/d8934f793fe048d09804a9f17c41d13b/file_en
114	National strategy for the protection of Switzerland against cyber risks	Switzerland	2012	https://www.isb.admin.ch/dam/isb/en/dokumente/ikt-vorgaben/strategien/ncs/Nationale_Strategie_Schutz_Schweiz_vor_Cyber-Risiken_NCS_2018-22_EN.pdf.download.pdf/Nationale_Strategie_Schutz_Schweiz_vor_Cyber-Risiken_NCS_2018-22_EN.pdf
115	National Information Security Policy	Syria	2014	http://www.nans.gov.sy/ar/file/5a399d259b914
116	National Strategy for Cybersecurity Development Program	Taiwan	2013	https://nicst ey.gov.tw/en/FD815304EBFFE6FC/2f7c6553-43d2-4bb8-b206-bb9e2e16a27f
117	National Cyber Security Program of Taiwan	Taiwan	2017	https://nicst ey.gov.tw/File/3BF304D39EA91236
118	National Cybersecurity Strategy	Thailand	2017	http://www.nsc.go.th
119	National Cyber Security Strategy	Trinidad and Tobago	2012	https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/trinidad-and-tobago-cyber-security-strategy/@_download_version/913cdd2b2a3e4a1bbf07e74c8381e418/file_en
120	National Cyber Security Strategy and 2013-2014 action plan	Turkey	2013	https://www.uab.gov.tr/uploads/pages/siber-guvenlik/ulusalsibereng.pdf
121	National Cyber Security Strategy	Turkey	2016	http://www.udhb.gov.tr/doc/siberg/UlusalSibereng.pdf
122	National Information Security Policy	Uganda	2014	http://www.nita.go.ug/sites/default/files/publications/National%20Information%20Security%20Policy%20v1.0_0.pdf
123	Cyber Security Strategy of Ukraine	Ukraine	2016	http://zakon2.rada.gov.ua/laws/show/96/2016
124	National Cyber Security Strategy 2016-2021	United Kingdom	2016	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/564268/national_cyber_security_strategy.pdf

125	Cyber Security Strategy of the United Kingdom	United Kingdom	2009	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf
126	The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world	United Kingdom	2011	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf
127	The National Strategy to Secure Cyberspace	United States	2003	https://www.hsdl.org/?view&did=1040
128	Cybersecurity National Action Plan	United States	2016	https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan
129	Information Security Policy for Public Administration	Uruguay	2014	https://www.impo.com.uy/bases/decretos/452-2009
130	National Cybersecurity Policy	Vanuatu	2013	https://ogcio.gov.vu/images/Cybersecurity-Policy-EN-FR-BI.pdf
131	Vietnam's Cyber Security Strategy	Vietnam	2016	https://mic.gov.vn/Upload_Moi/2018/QD-898Eng1--7-.docx

Military cyber operations units (2000-2017)

<i>Id</i>	<i>Unit name</i>	<i>Country</i>	<i>Year established</i>	<i>Sources</i>
1	Cyber Coordination Unit	Argentina	2013	http://www.fuerzas-armadas.mil.ar/ComandoConjuntoDeCiberdefensa/ResenaHistorica.aspx
2	Joint Cyber Defence Command	Argentina	2014	http://www.fuerzas-armadas.mil.ar/ComandoConjuntoDeCiberdefensa/ResenaHistorica.aspx
3	Defence Network Operations Centre	Australia	2003	http://www.aphref.aph.gov.au_house_committee_pwc_hmas_submissions_sub1.pdf ; http://press-files.anu.edu.au/downloads/press/p125391/mobile/ch06s10.html
4	Cyber Security Operations Centre	Australia	2010	https://informationsecurity.report/Resources/Whitepapers/f70456d6-9a09-408f-9fcd-9da1cc575087_csoc_brochure.pdf ; http://repository.jeffmalone.org/files/cyber/csoc_brochure.pdf
5	Information Warfare Division	Australia	2017	https://theconversation.com/cyber-revolution-in-australian-defence-force-demands-rethink-of-staff-training-and-policy-80317 ; https://www.defence.gov.au/jcg/iwd.asp
6	Command Leadership Support and Cyber Defence	Austria	2017	http://www.bundesheer.at/organisation/beitraege/fueuz/index.shtml
7	Cyber Security Operations Centre	Belgium	2016	https://english.n-va.be/news/wanted-200-computer-experts-for-cyber-army ; https://www.mil.be/nl/evolutie-van-defensie/beschermen-verdedigen-en-vechten-in-cyberspace/

8	CDCiber	Brazil	2011	Military Balance 2012; http://www.lexeditora.com.br/legis_23976242_PORTARIA_N_3028_DE_14_DE_NOVEMBRO_DE_2012.aspx
9	ComDCiber	Brazil	2016	http://eblog.eb.mil.br/index.php/exercito-no-brazil-cyber-defence-entrevista-com-general-okamura-comandante-de-defesa-cibernetica.html ; https://dialogo-americas.com/en/articles/brazilian-armed-forces-strengthen-nations-cyber-defense ; http://www.janes.com/article/66601/brazil-announces-establishment-of-new-cyber-defence-command
10	Canadian Forces Network Operations Centre	Canada	2004	http://cradpdf.drdc-rddc.gc.ca/PDFS/unc198/p800329_A1b.pdf ; https://reg.gg.ca/heraldry/pub-reg/project.asp?ProjectID=2019&lang=e
11	Canadian Forces Cyber Task Force	Canada	2010	Andrew Jones and Gerald L. Kovacich. 2016. "Global Information Warfare", 2nd edition. London: Taylor and Francis; https://www.youtube.com/watch?v=vYtfxID7E4 ; Jones, Kovacich (2016)
15	Elite corps	China	1997	Waters et al. 2008. "Australia and Cyber-Warfare". Canberra: ANU E Press; Ball, Desmond. 2011. China's Cyber Warfare Capabilities. Security Challenges, 7(2):81-103.
16	Net Force	China	2000	Waters et al. 2008. "Australia and Cyber-Warfare". Canberra: ANU E Press; Ball, Desmond. 2011. China's Cyber Warfare Capabilities. Security Challenges, 7(2):81-103.
12	Unit 61398	China	2006	https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf ; https://www.cfr.org/cyber-operations/pla-unit-61398
13	Unit 61486	China	2007	https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016_FINAL.pdf ; https://www.crowdstrike.com/blog/hat-tribution-pla-unit-61486/
14	Information Safeguards Base	China	2010	Nigel Inkster. 2012. China in Cyberspace, in "Cyberspace and National Security" (Ed. Derek S. Reveron). Washington DC: Georgetown University Press; Ball, Desmond. 2011. China's Cyber Warfare Capabilities. Security Challenges, 7(2):81-103.
17	Blue Army Division	China	2011	https://www.theaustralian.com.au/business/technology/chinas-blue-army-could-conduct-cyber-warfare-on-foreign-powers/news-story/5ebbec95bc758f8f214328d71a42ee5b ; http://world.time.com/2011/05/27/meet-chinas-newest-soldiers-an-online-blue-army/
18	Strategic Support Force	China	2016	Kevin Pollpeter et al. 2017 The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations. RAND; https://jamestown.org/program/strategic-support-force-update-overview/
19	Joint Cyber Command	Colombia	2012	https://www.sites.oas.org/cyber/Documents/Colombia%20-%20National%20Cybersecurity%20and%20Cyberdefense%20Policy.pdf ; https://www.cybersecurityintelligence.com/joint-cyber-command-ccoc-4823.html .
20	Cyber Defence Unit	Estonia	2011	https://ccdcoe.org/sites/default/files/multimedia/pdf/CDU_Analysis.pdf ; https://www.postimees.ee/249260/kaitseliit-pani-aluse-kuberalluksusele ; https://www.npr.org/2011/01/04/132634099/in-estonia-volunteer-cyber-army-defends-nation?t=1600421437816
21	Cyber Division	Finland	2014	https://puolustusvoimat.fi/en/about-us/c5-agency

22	CALID Cyber Defence and Analysis Centre	France	2006	https://www.defense.gouv.fr/portail/enjeux2/la-cyberdefense/la-cyberdefense/presentation ; https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports_National_Cybersecurity_and_Cyberdefense_Policy_Snapshots_Collection_1.pdf
23	Cyber Command	France	2016	https://www.defense.gouv.fr/actualites/articles/14-juillet-le-commandement-de-la-cyberdefense-va-defiler-sur-les-champs-elysees ; https://www.diplomatie.gouv.fr/en/french-foreign-policy/defence-security/cyber-security/
24	Cyber Security Bureau	Georgia	2014	http://csbd.gov.ge/mission.php?lang=en ; https://mod.gov.ge/en/page/59/cyber-security-bureau
25	Department of Information and Computer Network Operations	Germany	2009	http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf ; Military Balance 2016.
26	Cyber and Information Space Command	Germany	2017	http://cir.bundeswehr.de/portal/a/cir/start/kdocir/ueberuns!/ut/p/z1/04_Sj9CPykssy0xPLMnMz0vMAfIjo8zi zSxNPN2Ngg18DZyNTA0cncz8LYxMDA0Ngo31wwkpiAJKG-AAjgb6wSmp-pFAM8xxmmFkph-sH6UflZVYllihV5BfVJKTWqKXmAxyoX5kRmJeSk5qQH6yI0SgIDei3KDcUREAO8xWww!/dz/d5/L2dBISEvZ0FBIS9nQSEh/#Z7_694IG2S0M0C250AB6O82411026 ; https://www.dw.com/en/german-army-launches-new-cyber-command/a-38246517
27	Directorate of Cyber Defence	Greece	2011	http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf ; https://www.secnews.gr/68869/
28	Defence Information Warfare Agency	India	2003	https://idsa.in/jds/2_2_2008_IntegratingtheIndianMilitary_Vanand ; https://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf
29	Cyber Security Establishment	India	2005	http://www.potomac institute.org/images/CRI/CRI_India_Profile.pdf ; https://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf
30	Cyber Defence Operations Centre	Indonesia	2017	https://www.nst.com.my/news/2017/01/204974/countrys-cyber-defence-operations-centre-sept-says-hishammuddin ; https://kominfo.go.id/content/detail/10997/tni-bentuk-satsiber/0/sorotan_media ; https://www.airforce-technology.com/news/indonesian-air-force-establishes-cyber-unit-to-address-cyberattacks/#:~:text=The%20unit%20at%20the%20airforce,of%20the%20military%20from%20theft.
31	Cyber defence command	Iran	2010	https://nligf.nl/v1/upload/pdf/Structure_of_Irans_Cyber_Operations.pdf ; Military Balance 2016
32	C4 Computer Services Directorate	Israel	2003	https://www.idf.il/en/minisites/c4i-and-cyber-defense-directorate/ ; https://en.wikipedia.org/wiki/Computer_Service_Directorate
33	C4i and Cyber Defence Directorate	Israel	2017	https://www.idf.il/en/minisites/c4i-and-cyber-defense-directorate/ ; https://www.israelhayom.com/2020/06/11/ids-c4i-directorate-thwarts-iranian-cyberattack-on-armys-supply-chain/
34	Joint Cybernetic Operations Command	Italy	2017	https://www.difesa.it/InformazioniDellaDifesa/periodico/Periodico_2017/Documents/Numero3/ID-3_2017_ridotto.pdf#search=cyber ; https://www.ispionline.it/it/pubblicazione/italian-cyber-defence-build-20380

35	Joint-JSDF Command, Control, Communications, and Computer Systems Command	Japan	2008	Military Balance 2016; Jason Healey (ed). 2013. "A Fierce Domain: Conflict in cyberspace 1986-2012 ". Cyber Conflict Studies Association.
36	Cyber Defence Unit	Japan	2014	http://www.potomacinstitute.org/images/CRI/CRI_Japan_Profile_PIPS.pdf ; https://www.tandfonline.com/doi/pdf/10.1080/03071847.2014.895264 ; https://www.mod.go.jp/j/publication/shiritai/cyber/index.html
37	Cyber Defence Unit	Latvia	2014	http://www.mod.gov.lv/~media/AM/Par_aizsardzibas_nozari/Plani,%20konceptijas/cyberzs_April_2013_EN_final.ashx ; https://www.zs.mil.lv/en/node/365
38	Malaysian Armed Forces Cyber Defence Operations Centre	Malaysia	2017	https://thediplomat.com/2017/01/whats-next-for-malaysias-cyber-war/ ; https://www.thestar.com.my/news/nation/2017/01/18/military-sets-up-new-cyber-defence-ops-centre
39	Defence Services Computer Directorate	Myanmar	2004	Bitzinger and Vlavianos. 2016. "Emerging critical technologies and security in the asia-pacific". London: Palgrave; https://foreignpolicy.com/2016/04/01/the-perils-of-burmas-internet-craze/
40	Defence Cyber Command	Netherlands	2014	https://english.defensie.nl/topics/cyber-security/cyber-command ; https://www.tandfonline.com/doi/full/10.1080/23800992.2018.1484235
41	Joint Sigint Cyber Unit	Netherlands	2014	https://www.defensie.nl/actueel/nieuws/2014/07/03/aivd-en-mivd-slaan-handen-ineen-tegen-cyberdreiging ; https://www.tandfonline.com/doi/full/10.1080/23800992.2018.1484235
42	Unit 121	North Korea	1998	Tobias Feakin. 2013. "Playing Blind-Man's Buff: Estimating North Korea's Cyber Capabilities". International Journal of Korean Unification Studies; https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf
43	Cyber Defence Force	Norway	2012	https://forsvaret.no/en/organisation/other-departments
44	8th Division of Information Operations	Peru	2008	http://www.sadefensejournal.com/wp/?p=1022 ; https://ncsi.ega.ee/country/pe/ ; http://www.ccffaa.mil.pe/menuORG/AutoridadesCCFFAA/ACFFAA_JDIEMCFFAA.htm ; https://dialogo-americas.com/articles/peru-us-exchange-knowledge-on-information-operations/ ; http://www.sadefensejournal.com/wp/?p=1022
45	National Cryptology Centre	Poland	2013	https://ccdcoe.org/sites/default/files/multimedia/pdf/NCSO_Poland_2017.pdf ; https://www.gov.pl/web/national-defence/the-national-defence-ministry-creates-the-cyberspace-defence-forces
46	Cybernetic Operations Centre	Poland	2015	https://www.cyber.mil.pl/articles/o-nas-f/2018-10-23c-centrum-operacji-cybernetycznych/
47	Directorate of Communications and Information Systems	Portugal	2014	https://www.emgfa.pt/pt/organizacao/dircsi/missaoatribuicoesdircsi ; https://www.defesa.gov.pt/pt/pdefesa/ciberdefesa/centro/Paginas/default.aspx
48	Information Security Centre (Military Unit 64829)	Russia	2002	Jeffrey Carr. 2012. "Inside Cyber Warfare". 2nd edition. Cambridge: O'Reilly; https://www.forbes.com/sites/zakoffman/2020/03/21/putins-secret-intelligence-agency-hacked-dangerous-new-cyber-weapons-target-your-devices/

49	Centre for Electronic Surveillance of Communications (Military Unit 71330)	Russia	2003	https://www.securityartwork.es/2016/12/20/the-russian-icc-v-fsb/ ; Jeffrey Carr. 2012. "Inside Cyber Warfare". 2nd edition. Cambridge: O'Reilly.
50	Cyber Defence Operations Hub	Singapore	2013	https://www.zdnet.com/article/singapore-creates-operations-hub-to-beef-up-cyberdefense/ ; https://www.mindef.gov.sg/web/portal/mindef/about-us/organisation/organisation-profile/defence-cyber-organisation
51	Cyber Defence Organisation	Singapore	2017	https://www.opengovasia.com/articles/7770-singapore-armed-forces-setting-up-new-command-integrating-c4-and-cyber-defence-operations ; https://www.mindef.gov.sg/web/portal/mindef/about-us/organisation/organisation-profile/defence-cyber-organisation
52	Cyber Command	South Korea	2010	https://nakedsecurity.sophos.com/2010/01/11/south-korea-launches-cyberwarfare-command-centre/ ; Military Balance 2016.
53	Joint Cyber Defence Command	Spain	2013	http://www.emad.mde.es/CIBERDEFENSA/ ; https://www.cyberwiser.eu/content/spanish-joint-cyber-defence-command-selects-indra-cyber-range-platform
54	Armed Forces Command Support Organisation	Switzerland	2016	https://www.vtg.admin.ch/en/organisation/afcso.html
55	Information, Communication, and Electronic Force Command	Taiwan	2017	https://taiwantoday.tw/news.php?unit=2,6,10,15,18&post=117794 ; http://focustaiwan.tw/news/aip/201706290027.aspx
56	Cyber Warfare Unit	Thailand	2015	https://thediplomat.com/2015/10/thailands-military-to-set-up-new-cyberwar-unit/ ; https://prachatai.com/english/node/4767
57	General Staff Warfare and Cyber Defence Command	Turkey	2012	https://www.aa.com.tr/en/turkey/turkish-armys-new-cyber-defense-unit/283399 ; http://edam.org.tr/document/CyberNuclear/edam_cyber_security_ch2.pdf
58	Defence Cyber Operations Group/Joint Forces Cyber Group	United Kingdom	2011	https://www.zdnet.com/article/mod-recruits-hundreds-of-cyber-experts/ ; https://www.secret-bases.co.uk/wiki/Joint_Forces_Command ; https://www.gov.uk/government/organisations/joint-forces-command/about/recruitment
59	Cyber Security Operations Centre	United Kingdom	2016	https://www.gov.uk/government/news/defence-secretary-announces-40m-cyber-security-operations-centre ; https://wiki.openrightsgroup.org/wiki/Cyber_Security_Operations_Centre
60	JTF-CND	United States	1998	Jason Healey (ed). 2013. "A Fierce Domain: Conflict in cyberspace 1986-2012 ". Cyber Conflict Studies Association; https://nsarchive.gwu.edu/briefing-book/cyber-vault/2019-06-29/joint-task-force-computer-network-defense-20-years-later
61	JTF-CNO	United States	2000	Jason Healey (ed). 2013. "A Fierce Domain: Conflict in cyberspace 1986-2012 ". Cyber Conflict Studies Association; https://nsarchive.gwu.edu/briefing-book/cyber-vault/2019-06-29/joint-task-force-computer-network-defense-20-years-later

62	JTF-GNO	United States	2004	Jason Healey (ed). 2013. "A Fierce Domain: Conflict in cyberspace 1986-2012 ". Cyber Conflict Studies Association; https://ctovision.com/jtf-cnd-to-jtf-cno-to-jtf-gno-to-cybercom/ ; https://nsarchive.gwu.edu/briefing-book/cyber-vault/2019-06-29/joint-task-force-computer-network-defense-20-years-later
63	Cyber Command	United States	2010	https://www.cybercom.mil/About/ ; https://warontherocks.com/2019/04/cyber-command-the-nsa-and-operating-in-cyberspace-time-to-end-the-dual-hat/