Going Cyber:
The Dynamics of Cyber Proliferation and International Security

A Thesis
Submitted to the Department of
Politics and International Relations
of the University of Oxford
in partial fulfilment of the requirements
for the degree of
Doctor of Philosophy
in International Relations

By

Max W. E. Smeets

Oxford

September 18, 2017

Copyright 2017 By Max W.E. Smeets

All Rights Reserved

Going Cyber:
The Dynamics of Cyber Proliferation and International Security

Max W. E. Smeets

Thesis Advisor: Lucas Kello, D.Phil.

Abstract

For over a decade, we have heard alarming statements about the spread of cyber weapons from senior policymakers and experts. Yet, the dynamics of cyber proliferation are still understudied and under-theorized. This study offers a theoretical and empirical account of what causes the spread *and* restraint of cyber weapons and argues that the world is *not* at the brink of mass cyber proliferation. Whilst almost forty states are exploring and pursuing the development of cyber weapons, I indicate that only few have so far acquired a meaningful capability. This is due both to supply and demand factors. On the supply-side, most states have a latent capacity to develop relatively simple offensive cyber capabilities, but are unable to develop sophisticated cyber weapons. Moreover, the incentives for knowledge transfer and thus exporting offensive cyber capabilities between states are weak. On the demand-side, I show that national security considerations do not provide the best explanation of variance. Instead, domestic politics and prestige considerations are paramount. Moreover, and unlike nuclear proliferation, I argue that it is not the *possession* of cyber weapons but the *intention* of possession signalled through visible initiatives which matters. Ultimately, I note that cyber weapons can have strategic value – but only under certain conditions.

Key words: Cyber Proliferation, Cyber Weapons, Cyber Hodgepodge, Nuclear, Strategic Utility

Acknowledgements

Writing this DPhil has been an enormously enriching experience. Since my very first day starting as an MPhil student in 2012, I felt at home in Oxford. I have been given so many opportunities and will take with me many beautiful memories.

I am indebted to my supervisor Lucas Kello for shepherding me through my DPhil. Walter Mattli as advisor at St. John's College has been supportive in every way. Without the advice and support of Yuen Foong Khong I would have never been able to start the project, for which I am thankful. I was incredibly fortunate to rely on Richard Harknett's insightful criticism during my final year in Oxford, which stimulated my thinking about cyber strategy. Duncan Snidal and Jonathan Leader Maynard gave detailed comments at a critical phase of my research. Also, I thank my examiners, Kalypso Nicolaïdis and David Betz, for providing valuable suggestions and corrections to my writing.

I also have to single out the three cyber musketeers; James Shires, Jamie Collier, and Florian Egloff. I am well aware that sharing an office space with a guy who is constantly whistling is not always easy; I thank you for coping with me, providing detailed feedback on my writings, and making my research so much more enjoyable and rewarding.

Many others have read portions of the manuscript and provided written comments. Without their support this work would be in a much worse shape. Special thanks to Gjovalin Macaj, Lennart Maschmeyer, Robert Morgus, Herb Lin, and Taylor Roberts.

Much of my research and writing was conducted outside of Oxford. The months at the NATO CCD COE in Tallinn early on in my DPhil provided me an excellent environment to kick-start my research. I fell in love with Paris during my six month fellowship at Sciences Po CERI. I thank Christian Lequesne for his patience and mentorship during my time there. I also received a warm welcome from Merit E. Janow, Matthew Waxman, Jay Healey and Benjamin Dean when I spent a summer at Columbia University SIPA as a visiting fellow, for which I am thankful.

My studies could never have been completed without the financial support from the Department of Politics and International Relations, St. John's College, the Charterhouse European Bursary and the Carnegie Endowment.

Last but not least, I would like to say a heartfelt thank you to my friends and family. I cannot express how grateful I am for helping in whatever way possible and all the sacrifices that you have made on my behalf. Dankjewel voor jullie inspiratie, steun en liefde.

Table of Contents

Acknowledgements 4
Table of Contents 5
Figures Index 8
Tables index 9
Abbreviations 10
Chapter 1: Introduction 12
1.1 The Puzzle and Research Question(s) 12
1.2 Argument 13
1.4. Bridging Fields of Research 18
1.5. Data Analysis 20
1.5.1 The Data Paradox 20
1.5.2 Making Sense of the 'Cyber Hodgepodge' 22
1.5.4 Cyber Threat Actors Dataset 25
1.5.5 Cyber Exploration and Pursuit Dataset 27
1.6 Structure of the Thesis 28
Chapter 2: The Concept of 'Cyber Weapon' 30
2.1 Current Conceptual Problems 30
2.2 Conceptualizing Cyber Weapons as a Multilevel Concept 33
2.2.1 The Base Level: Weapons 35
2.2.2 The Qualificatory Level: the Prefix "Cyber-" 38
2.2.3 The Secondary level: the Necessary and Sufficient Features of Cyber Weapons 46
2.2.4 The Indicator Level 49
2.3 Conclusion 55
Chapter 3: A Survey of the Cyber Proliferation Landscape: The Past and Present 57
3.1 Introduction 57
3.2 Exploration, Pursuit and Acquisition of Cyber Weapons 59
3.3 Variations of Cyber Proliferation 63
3.3.1 Sophistication 64
3.3.2 Proxy Actors 71
3.3.3 Organizational Structure and Budgets 77
3.4 'Order of Entry' Effects in Cyber Weapon Development: First Mover and Latecomer Advantages ... 78
3.4.1 Early Mover Advantages 79

3.4.2 Late Mover Advantages 81
3.4 Conclusion 83
Chapter 4: Supply-Side: What it Takes to Develop Cyber Weapons 84
4.1 Introduction 84
4.2 Identifying Cyber Weapons: Looking for a Needle in a Haystack 86
4.3 Case Studies of Cyber Weapons' Development Costs 91
4.3.1 DDoS Attacks: Cyber Weapon on the Cheap 91
4.3.2 Data Removals: Getting the most Bang for your Buck 93
4.3.3 Physical Destruction: Crossing the Rubicon 97
4.3.4 Knitting the Pieces Together: an Overview of the Main Obstacles 100
4.4 Drivers of Cost Reduction 103
4.5 The Incentives for the Transfer of Cyber Weapon Technology 106
4.6 Conclusion 112
Chapter 5: Demand-Side Predictors: Assessing Three Proliferation Frameworks 115
5.1 Introduction 115
5.2 The National Security Imperative 117
5.2.1 Theoretical Framework 117
5.2.2 Evidence 119
5.3 The Domestic Politics Imperative 126
5.3.1 Theoretical Framework 126
5.3.2 Evidence 128
5.4 The Normative Imperative: Cyber Symbolism 136
5.4.1 Theoretical Framework 136
5.4.2 Evidence 138
5.5 Conclusion 144
Chapter 6: A Strategic Utility Analysis of Cyber Weapons 146
6.1 Introduction 146
6.2 From Destructive Effect to Strategic Utility 146
6.3 Cyber Bargaining: Strategic Utility in (Potential) Possession 151
6.4 The Strategic Value of using Cyber Weapons 163
6.4.1 Distinguishing between Counterforce and Countervalue Capabilities 164
6.4.2 Strategic Utility of Using Counterforce and Countervalue Cyber Weapons 168
6.5 Conclusion 177
Chapter 7: Conclusion 179
7.1 Summary of Findings 179

7.2 Implications for Theory and Practice 182
7.3 Limitations and Future Research 184
Appendix 1: The Offensive Cyber Operations Dataset: Codebook 191
1.1 Overview 191
1.2 Description 191
1.3 Variables 193
1.4 Limitations 194
Appendix 2: The Cyber Threat Actor Dataset: Codebook 196
2.1 Overview 196
2.2 Description 196
2.3 Variables 201
2.4 Limitations 203
Appendix 3: The Cyber Exploration and Pursuit Dataset: Codebook 205
3.1 Overview 205
3.2 Description 205
3.3 Variables 206
3.4 Limitations 207
References 210

Figures Index

Figure 1.1: *Overview of Labels used for Threat Actor 'SoFacy'*…….. 23

Figure 1.2: *General Overview of Datasets*…… 24

Figure 1.3: *Overview of UPS' Reported Offensive Cyber Operations*…… 26

Figure 2.1: *Summary Conceptual Analysis of a Cyber Weapon*…… 35

Figure 3.1: *States' Exploration, Pursuit and Acquisition of Cyber Weapons, over time*…… 60

Figure 3.2: *Offensive Cyber Actors Landscape*…….. …… 65

Figure 3.3: *Reported Cyber Threat Actors based in the U.S*…….. ……..... 68

Figure 3.4: *Reported Cyber Threat Actors based in China*…….. …….. 69

Figure 3.5: *Reported Cyber Threat Actors based in Russia*…….. ……. 70

Figure 3.6: *Offensive Cyber Actors in the U.S. and Attribution Certainty*…….. …….. 74

Figure 3.7: *Offensive Cyber Actors in China and Attribution Certainty*…….. …….. 75

Figure 3.8: *Offensive Cyber Actors in Russia and Attribution Certainty* …….. ……. 76

Figure 4.1: *Reported Offensive Cyber Operations, over time (2010-2016)* …….. …… 88

Figure 4.2: *Reported Offensive Cyber Operations, over time (2001-2010)* ……..…….. ……. 89

Figure 4.3: *Reported Offensive Cyber Operations, over time (1986-2002)* …….. …… 90

Figure 4.2: *Connections between Shamoon, Jokra and Destover*…….……..…… 96

Figure 7.1: *Cost-Security relationship: Vertical Nuclear Proliferation*……..……... 188

Figure 7.2: *Cost-Security relationship: Vertical Cyber Proliferation*……..... 188

Figure A.2.1: *Overview 'Offensive Cyber Capability'*…… 200

Tables index

Table 4.1: *Cyber Weapon cases based on Level of Sophistication*……. 91
Table 4.2: *Main Obstacles to Cyber Weapon Development*…… 101
Table 4.3: *Actors' Capability and Willingness to Transfer Cyber Weapon Technology*…….……... 108
Table 6.1: *Countervalue and Counterforce Dimensions of Cyber Weapons*……..…..... 166
Table A2.1: *Data Collection and Analysis Cyber Exploitation and Pursuit*…….. 199
Table A2.2: *Spectrum of State Responsibility Conducting Offensive Cyber Operations*…… 199

Abbreviations

AI	Artificial Intelligence
APRANET	Advanced Research Projects Agency Network
APT	Advanced Persistent Threat
ASEAN	Association of Southeast Asian Nations
B.C.	Before Christ
CCD COE	Cooperative Cyber Defence Centre of Excellence
CFCW	Counterforce Cyber Weapons
CIA	Central Intelligence Agency
CNA	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Exploitation
CSoJ	Cutting Sword of Justice
CVCW	Countervalue Cyber Weapons
DDoS	Distributed-Denial-of-Service
DGSE	General Directorate of External Security
DHS	Department of Homeland Security
DNS	Domain Name System
DoS	Denial-of-Service
ENISA	European Network and Information Security Agency
ENR	Enrichment and Reprocessing
EU	European Union
FBI	Federal Bureau of Investigation
FEP	Fuel Enrichment Plant
GCCS	Global Conference on Cyberspace
GCHQ	United Kingdom's Government Communications Headquarters
GDP	Gross Domestic Product
GGE	Government Group of Experts
HMI	Human Machine Interface
IC	Integrated Circuit
ICS	Industrial control system
IP	Internet Protocol
IPSec	Internet Protocol Security
IR	International Relations
ISS	Internet Security Systems
IT	Information Technology
ITU	International Telecommunications Union
JSF	Joint Strike Fighter
MALE UAV	Medium-altitude Long-endurance Unmanned Aerial Vehicle
MILNET	Military Network
MMCA	Monte Melkonian Cyber Army
NAS	National Academy of Sciences
NATO	North Atlantic Treaty Organization
NCSS	National Cyber Security Strategies
NPT	Nuclear Proliferation Treaty
NSA	National Security Agency
OIOCC	Organizational Integration of Offensive Cyber Capabilities
OS	Operation System
OSCE	Organization for Security and Co-operation in Europe
PCA	Pakistan Cyber Army
PCCIP	President's Commission on Critical Infrastructure Protection
PDD-63	Presidential Decision Directive 63

PLA	People's Liberation Army
PLC	Programmable Logic Controller
RMA	Revolution in Military Affairs
SCADA	Supervisory Control And Data Acquisition
SIS	Safety Instrumented Systems
SLOC	Source lines of code
SQL	Structured Query Language
START	Strategic Arms Reduction Treaty
TAO	Tailored Access Operations
TCP	Transmission Control Protocol
UK	United Kingdom
UN	United Nations
UNIDIR	United Nations Institute for Disarmament Research
URL	Uniform Resource Locator
US	United States
VPN	Virtual Private Network
WB	World Bank
WINE	Worldwide Intelligence Network Environment
WMD	Weapons of Mass Destruction
WSJ	Wall Street Journal

Going Cyber:
The Dynamics of Cyber Proliferation and International Security

Chapter 1: Introduction

1.1 The Puzzle and Research Question(s)

On March 21st 1963 United States (U.S.) President John F. Kennedy began his press conference in a crowded auditorium of the State Department reporting on his three-day trip to Costa Rica where he met with Presidents of five Central American countries. The event took place exactly five months after President Kennedy went on television to announce that a U-2 reconnaissance plane had discovered medium-range missile sites in Cuba, and it would establish a naval quarantine demanding the dismantling of the bases. The questions at the conference in Washington D.C. inevitably turned to President's efforts to curb the spread of nuclear weapons, about which he said: "[w]ith all of the history of war, and the human race history, unfortunately [there] has been a good deal more [war] than peace[;] with nuclear weapons distributed all through the world, and available, and the strong reluctance of any people to accept defeat, I see the possibility in the 1970's of the President of the United States having to face a world in which fifteen or twenty or twenty-five nations may [have] give these weapons. I regard that as the greatest possible danger and hazard."[1]

For at least a decade we have heard similar statements about the spread of cyber weapons from a wide range of senior policymakers and experts. In May 2017, Richard Ledgett, former deputy director of the NSA, told an audience at Georgetown Law School's annual Cybersecurity Law Institute that "well over 100" countries around the world are now capable of launching cyber attacks. In 2012, NATO's Deputy Assistant Secretary General for Emerging Security Challenges, Jamie Shea, made a similar statement: "about 100 countries in the world – 100 countries, which is the majority – are actively developing offensive, not defensive, but offensive – cyber capabilities."[2] And a few years earlier,

[1] John F. Kennedy, "News Conferences 52", John F. Kennedy Presidential Library and Museum, (1963, March 21), retrieved from: https://www.jfklibrary.org/Research/Research-Aids/Ready-Reference/Press-Conferences/News-Conference-52.aspx

[2] Jamie Shea, "Lecture 6 - Cyber attacks: hype or an increasing headache for open societies?," (2012, February 29), retrieved from: http://www.nato.int/cps/en/natolive/opinions_84768.htm; For similar statement see: INFOSEC, "The

McAfee approximated in their 2007 report that 120 countries have been developing ways to use "the internet as a weapon."[3]

Indeed, numerous states mention in their national security strategy that they prioritize the development of offensive cyber capabilities. What makes this claim even more compelling is that many states are said to be pouring resources into the creation of a military cyber command whilst their overall military expenditure has remained constant or even been reduced. For example, the Dutch government, a year after they urged the Ministry of Defence to sell their Leopard-tanks to Finland as part of reducing military expenditure, established a Cyber Command focusing on defense, intelligence and offense. [4]

The goal of this work is to offer a theoretical and empirical account of *what causes the spread and restraint of cyber weapons*. This critical question is understudied and undertheorized – yet solving the puzzle is important for both understanding the nature of cyber threat and formulating an accurate foreign policy response. [5]

1.2 Argument

The main argument of this study is that the world is *not* at the brink of mass cyber proliferation. The spread of cyber weapons will be limited in at least two ways. First, the number of states that will acquire cyber weapons is not and will not be as large as the above statements would suggest. Second, the *rate* at which these capabilities will spread in the future is not as fast.

I define cyber proliferation as the movement towards developing cyber weapons both technically and politically.[6] Surveying the cyber landscape, I show that most states are still at the stage of *no*

Rise of Cyber Weapons and Relative Impact on Cyberspace," (2012, October 5), Retrieved from: http://resources.infosecinstitute.com/the-rise-of-cyber-weapons-and-relative-impact-on-cyberspace/

[3] Cited in: Peter Griffiths, "World faces "cyber cold war" threat," *Reuters*, (2007, November 29) retrieved from: http://www.reuters.com/article/us-britain-internet-idUSL2932083320071129; also see Jarno Limnéll, "The cyber arms race is accelerating - what are the consequences?," *Journal of Cyber Policy*, 1:1 (2016)50-60

[4] Jules Seegers, "Leopard-tank toch verkocht, Defensie vindt in Finland alsnog koper," *NRC*, (201, December 19), retrieved from: ww.nrc.nl/nieuws/2013/12/19/leopard-tank-toch-verkocht-defensie-vindt-in-finland-alsnog-koper-a1428711; Ministry of Defence, "Cyber Command," (2016), retrieved from: www.defensie.nl/onderwerpen/cyber-security/inhoud/cyber-commando

[5] A similar statement was made in Scott Sagan's seminal study, written in 1996, which opens with the question: "Why do states build nuclear weapons?" See: Scott D. Sagan, "Why Do States Build Nuclear Weapons? Three Models in Search of a Bomb," *International Security*, 21:3 (Winter, 1996-1997), pp. 54-86. Revised and updated versions of this article also appear as Scott D. Sagan, "The Causes of Nuclear Proliferation," *Current History*, (April 1997), pp. 151-156; Scott D. Sagan "Why Do States Build Nuclear Weapons?" in Victor Utgoff, ed., *The Coming Crisis: Nuclear Proliferation, U.S. Interests, and World Order* (Cambridge, MA: MIT Press:1999), p. 17-50; and Scott D. Sagan, "Why Do States Build Nuclear Weapons? Three Models in Search of a Bomb," in *New Global Dangers: Changing Dimensions of International Security* (Cambridge, MA: MIT Press: 2004).

[6] I follow Solingen's definition in this research. Solingen writes that "nuclearization" concerns the "movement towards nuclear weapons acquisition even if it does not result in actual acquisition." Etel Solingen, *Nuclear Logics: Contrasting*

discernible activity; they have not made any statements or taken any observable actions to develop cyber weapons. Second, no more than forty states have *explored* the development of cyber weapons - that is, they provided public or private authorization to look into the development of cyber weapons. Third, the group of states that is *pursuing* cyber weapon is below thirty. These states have formally established an organization to develop cyber weapons. Finally, no more than a dozen states across the globe actually seem to have *acquired* cyber weapons. Going beyond these numbers, there are also significant differences in *how* states proliferate. Although several states pursuing cyber weapons are investing a significant amount of resources, the majority of cyber commands across the world have a rather small budget.[7]

The nuclear literature commonly makes a distinction between demand-side and supply-side drivers of proliferation[8] - or, as Dong-Joon Jo and Erik Gartzke classify the nuclear literature; there are arguments which focus on a state's *willingness* to develop nuclear weapons and those that privilege the *opportunity* to develop nuclear weapons.[9] This distinction can also be used to help explain the cyber proliferation landscape.

My starting observation is that most of the cyber weapons used to date are unsophisticated.[10] The financial, material, knowledge-based and organizational hurdles actors have to overcome to develop these types of cyber weapon are limited. It does not require a resourceful formal organization, long-term planning, or highly specialized knowledge to develop these capabilities. However, the barriers states have to overcome to develop sophisticated cyber weapons are significantly higher. In order to

Paths in East Asia and the Middle East, (Princeton: Princeton University Press: 2007), p. 301; Some scholars make a distinction between horizontal proliferation, meaning the build-up of weapons, and vertical proliferation, meaning the spread of weapons to multiple countries. This study only focuses on the latter.

[7] As I will show in chapter 3, states also differ in their organizational set up of offensive cyber activities and reliance on proxy actors.

[8] Hymans, "Theories of Nuclear Proliferation;" Montgomery and Sagan, "The Perils of Predicting Proliferation"

[9] This distinction is possibly better as in economic theory 'demand' consists of two factors: i) the desire for a good (i.e. taste) and ii) the possession of sufficient wealth to buy the good (i.e. ability). In the case of nuclear proliferation, the demand-side only focuses on the purchasing desire. Jo and Gartzke, "Determinants of Nuclear Weapons Proliferation,. Framework initially developed in Benjamin A. Most and Harvey Starr, *Inquiry, Logic and International Politics*, (Columbia: University of South Carolina Press: 1989).

[10] Sophistication refers to the complexity of techniques put into the development of the capability to allow for the opportunity to gain its objective. As David Aitel notes, cyber operations can differ in the sourcing and use of capabilities, networking, testing, persistence and operational security. This means there are no strict necessary and sufficient conditions when a capability can be considered 'sophisticated', but they share 'family resemblances'. The most important factors which feed into this are: the type of vulnerability exploited, the level of stealth, the degree of tool-kit customization, and the type of system penetrated. In general terms, an unsophisticated weapon exploits known-vulnerabilities using a generic tool-kit with a minimal implementation of anti-detection techniques against easy-accessible targets. Sophisticated cyber weapons exploit zero-day vulnerabilities (sometimes multiple) implement various obfuscation techniques and implement customized malware or firmware against difficult to access targets. Finally, note that I differ from Aitel as his framework does not distinguish between type of vulnerability exploited (i.e. zero-day versus non-zero-day exploits). David Aitel, 'Useful Fundamental Metrics for Cyber Power', *CyberSecPolitics*, (2016), retrieved from: https://cybersecpolitics.blogspot.com/2016/06/useful-fundamental-metrics-for-cyber.html.

gather enough information about the adversary's systems - an activity which often takes place outside cyberspace - direct access to a dedicated intelligence network is required. The material demands also go far beyond a well-stocked fridge of Club Mate and snacks for sophisticated cyber weapons. Not least, the mirroring of an Industrial Control System environment of the attacker - in order to test the effectiveness and precision of a cyber weapon - is an obstacle even well-funded institutions find difficult to overcome. Finally, for sophisticated capabilities, the specialized coding activities need to be well-coordinated - yet, also remain highly secretive. Indeed, these are not weapons for the 'weak'.

I identify four processes that could drive the cost reduction of cyber weapons: labour efficiency, specialization, product redesign, and shared experience effects. Despite these potential dynamics, there are some inherent barriers for future cost reduction. Improved defence requires the attacker to develop more complex capabilities to ensure effectiveness. It will also remain difficult to hire the right technical minds - and because it is a highly transferable skill – it will not easy to retain these people. Finally, as offensive cyber capabilities are effective for only a short period of time, any cyber weapon program requires continuous production, not just intermittent projects.

Overall, I conclude that the gap between the technical potential to develop sophisticated cyber weapons and military reality is much smaller than many scholars perceive it to be: most states only have the latent capacity to develop relatively simple offensive cyber capability. If a significant knowledge transfer occurs from more advanced cyber powers to less mature powers, the pool of states with sophisticated cyber weapons can grow. Yet, the incentives for exporting offensive cyber capabilities are weak. Cyber weapons have a high likelihood of losing their effectiveness after their first use, as the exploited vulnerability are likely to be discovered and patched.[11] This means that the use of the cyber capability by one actor greatly reduces the ability of other actors to also use it.[12] As a result, when it comes to state cooperation, mutual benefits only arise when states share views on the timing, target *and* proportionality of the cyber attack. The paradox of cyber weapons is that, although technically they can be (relatively) effortlessly replicated, their transitory nature changes the incentive structure of actors and turns weapons into indivisible goods. If any incentives exist between states, it would be in facilitating others to develop their *own* offensive capabilities - that is by providing knowledge/expertise to adapt weapons technology and providing the capacity to innovate - as this does not reduce the utility of one's own arsenal. Yet, an advanced cyber power will only

[11] The exact dynamics differ across offensive cyber capabilities. Max Smeets "A Matter of Time: On the Transitory Nature of Cyberweapons," *Journal of Strategic Studies*, (2017)1-28

[12] These incentives for *not* sharing are not as strong for espionage capabilities, as these are less likely to be discovered following usage.

consider this type of transfer with a highly select group of other states; i.e. only those actors with which the state has historically strong ties and can trust that these capabilities will not be used against them (at some point in the future). Instead, the diffusion of finished systems and the basic engineering know-how used to reproduce cyber weapons technology is more likely to come from the private sector.

Addressing the demand-side, I build on Scott Sagan three 'models' for explaining proliferation dynamics: i) international security, ii) domestic politics, and iii) norms.[13] Assessing each analytical framework in relation to cyber proliferation, it would appear that national security considerations are the predominant driving force for a state to seek cyber weapons. After all, although the current uses of cyberspace pay lip service to its benefits, the overriding tone is negative: it is a space of threats and security, rather than opportunity and freedom. Yet, I show that the framework does a poor job explaining most variation. Unlike nuclear weapons, cyber proliferation does *not* beget cyber proliferation. Cyber weapons are not an 'absolute weapon', nor is there an evident relationship between actors' build-up of a cyber weapon arsenal and their own security, given the inherent limits of cyber deterrence. Hence, at most, the national security imperative provides a weak incentive for states to proliferate. This weak stimulus seems to be insufficient to push most states over the hurdles of developing sophisticated cyber weapons - especially small powers lacking large defence budgets.

Hence, to fully comprehend the appeal of acquiring cyber weapons, an analysis of the other two frameworks is required as well. Considering the domestic politics framework, a key domestic constituency which does have a major influence on a state's procurement of cyber weapons concerns the intelligence services. Specifically, the close similarities in activities required to steal data/network exploitation and destroy data/network attack means that the intelligence apparatus can slowly expand their authority in this field. For the military, especially for states with dwindling defence budgets, the focus on offensive cyber capabilities can be a way to avoid further budget cuts and ensure job security. Even though there are reduced incentives for the private sector to drum up demand for offensive cyber capabilities (due to nature of development, current regulation and overall market size), their influence continues to grow.

Although a diverse group of actors have now called for the establishment of new 'cyber norms', cyber weapons are not currently regarded with abhorrence in the same manner as weapons of mass

[13] Sagan, "Why Do States Build Nuclear Weapons"

destruction. Whilst there is no cyber taboo, status driven motives are less favourable to explain the variation in cyber weapon development due to three intertwined reasons: it is hard to showcase or 'parade' cyber weapons, they have limited attributive ability following usage, and they are transitory in nature. What this leads to is that states are more inclined to talk boastingly about their *intentions* instead of developing *actual* cyber weapons in an effort to deter and enhance their status in the international system. The iconographic value of cyber proliferation lies not in the showcase or use of cyber weapons, but in policy and institutions which embody a state's intentions to develop them. Perhaps it is not 'all mouth and no trousers,' but policymakers and experts often confuse *apparent* proliferation with *actual* proliferation.

This means that similar to Sagan's classic study on nuclear proliferation, I present a multi-causal argument on the demand-side for cyber proliferation. But, whereas for Sagan still "the largest number of past and even current active proliferant cases are best explained by the security model", the explanatory value of this framework is more limited for cyber proliferation.[14] Indeed, the 'domestic politics' and 'normative' framework do not just explain a few, residual cases but are at the heart of the cyber proliferation puzzle. In addition, the *nature* of the causal mechanisms differs for cyber proliferation. Overall, for modern states not the *possession* of cyber weapons (like with nuclear weapons) but *visible initiatives* revealing the *intention* to develop cyber weapons serve a primary iconographic function.

This however does not mean that cyber weapons do not have any strategic value. First, I argue that the *threat* of using a cyber weapon can have strategic effects. Particularly, when states develop a reputation over time, we can expect 'cheap talk' about capabilities to become more effective. There are also various ways for states to involve domestic or international audiences to make threat postures more credible and effective in the future. Second, the *use* of cyber weapons can provide an 'extra option' to leaders. Even though cyber weapons will not displace traditional forms of force at all times, examining the use of counterforce cyber weapons (CFCW) and countervalue cyber weapons (CVCW) suggests that, under certain conditions, they can be used both as a force-multiplier for conventional military assets or as an independent capability. Cyber weapons can also be used to achieve a form of psychological ascendancy and deployed effectively with few casualties.

[14] Sagan, "Why do States Build Nuclear Weapons?," p. 85

1.4. Bridging Fields of Research

This study attempts to connect different fields of literature, through which a new field of study opens up: that of cyber proliferation.

First, I bring together both Computer Science and Political Science literature in one study, providing new frameworks and typologies for understanding the shape of the cyber danger. Lucas Kello indicates that cyber studies requires "a congress of disciplines that includes not only the engineering sciences but also the political and social sciences".[15] He believes that cyber studies can be split up, in which both political scientists and computer scientists contribute their own share to understanding different aspects of the cyber issue. In his own words, "[c]ertain aspects of the cyber issue, such as the analysis of code, belong to the computer specialist; others require the expertise of researchers versed in the contests of international anarchy."[16] We should be careful when encouraging this view, as it will quickly lead to a similar situation as the attempt of the blind men to discover the nature of the elephant: the one who touches its leg calls it a tree, another who touches its tail calls it a rope, and so on.[17]

The IR community writing on cyber security hardly ever cites computer science articles or conference proceedings, despite the fact that they are often relevant. [18] Since the properties of the cyber issue are intrinsically interconnected, in this thesis I draw on insights of *both* fields of study in the *same* analysis to obtain a holistic understanding of the dimensions of cyber weapons.[19] If we want to further our understanding an 'anti-territorial attitude' towards the 'cyber issue' is required, with cross-fertilization between different fields of study. To be clear, it does not mean that the social scientist should become a computer scientist or the other way around. Instead, the point of this thesis is that

[15] Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft", *International Security*, 38: 2 (2013)7-40, p.16
[16] Ibid, p. 16
[17] Similar analogy is used by Libicki talking about the problems with respect to defining information warfare: Martin C. Libicki, *What Is Information Warfare?* (Washington DC., RAND Corporation, 1995)
[18] Most IR journals on cyber security have a reference ratio of more than 15:1 (political science: computer science), although there is significant variation. The journal International Security which has published five articles on the cyber threat between 2000-2016 is on the high end of the spectrum in this respect. In total, 350+ articles were referenced in all studies combined, of which only five references were from computer science journals or magazines. On the other end of the spectrum one can find the Journal of Strategic Studies - primarily due to one article published by Thomas Rid and Ben Buchanan on attribution. Just below 250 papers were referenced in the eight reviewed articles of which 49 articles were computer science orientated. Note that Sagan provides a similar critique on the recent renaissance in nuclear security studies which has developed with little interchange between historians and political scientists. Scott D. Sagan, "Two Renaissances in Nuclear Security Studies," *H-Diplo/ISSF* (15 June 2014), retrieved from: https://issforum.org/ISSF/PDF/ISSF-Forum-2.pdf ; Thomas Rid and Ben Buchanan, "Attributing cyber attacks" *Journal of Strategic Studies*, 38:1-2 (2015)4-37; The article referenced 24 computer science articles of the 79 references in total.
[19] The word 'both' does *not* imply that I hold the view only political science and computer science are relevant to understand the cyber issue - other disciplines are inherently relevant as well.

social scientists can become much better social scientists if they do not get unnecessarily discouraged by differences in terminological conventions and substantive applications of other fields of study and make a conscious effort to learn from other disciplines.[20]

Second, this study brings two fields of International Relations closer together which have so far been largely disconnected: the literature on the causes for (nuclear) arms proliferation or restraint, and research on cyber conflict. This connecting exercise is beneficial as in trying to grasp the dynamics of cyber proliferation, as we do not have to start from scratch in our analysis.[21]

Discussions on research design and methodology of cyber conflict are strikingly underdeveloped in scholarly debates. The dependent variable is often underspecified as scholars fail to offer a conceptual discussion of cyber-related terms.[22] Also, although one can find reports of cyber incidents in the media on a daily basis, in small N analyses the academic literature has paid attention to a rather selective set of events.[23] These include the cyber attacks during the Russo-Georgian war, the cyber attacks on Estonia, as well as Stuxnet and its 'cousins'- Duqu and Flame.[24] Cyber scholars rarely *explicitly* justify why these cases are chosen - obscuring the relationship between the case and the population. Finally, in large N analyses, the relevant population is often unclear and evidence collection is poor.

---

[20] For a similar view on interdisciplinarity see: Pami Aalto, `Interdisciplinary International Relations in Practice," *Forum*, 29:2 (2015)255-230

[21] As Nye Jr. states "there are some important nuclear-cyber strategic rhymes, such as the superiority of offense over defense [...] the potential use of weapons for both tactical and strategic purposes. [...]Even more important than these technical and political similarities is the learning experience as governments and private actors try to understand a transformative technology - and adopt strategies to cope with it. […] It is worth examining the uneven and halting history of nuclear learning to alert us to some of the pitfalls and opportunities ahead in the cyber domain." The point here is that not only do we should not only enable these learning experiences for government and private actors, but *academic scholarship* too. The way we can use the nuclear scholarship is to understand earlier pitfalls in scholarship and advancements in methods of study of procurement. Nye Jr. , "Nuclear Lessons for Cyber Security"

[22]As I discuss in chapter 2, one can observe a mix of conceptual stretching, conceptual confusion, and conceptual contestation with respect to cyber-related terms.

[23] This was also one of the conclusions at the most recent Cyber Conflict State of the Field Conference. See: Cyber Studies Conflict Association, " Cyber Conflict State of the Field Conference," New York City: Columbia University - School of International and Public Affair, (2017, June 8-9)

[24] On Stuxnet see: Ralf Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon," *Security and Privacy*, 9:3 (2011):49-51; Jon Lindsay, "Stuxnet and the Limits of Cyber Warfare*," Security Studies*, 22,3 (2013): 365-404;" Sean Collins and Stephen McCombie, "Stuxnet: the emergence of a new cyber weapon and its implications," *Journal of Policing, Intelligence, and Counter Terrorism*, 7:1 (2012)80-91; On Georgia see: Ronald J. Deibert, "Cyclone in cyberspace: information shaping and denial in the 2008 Russia-Georgia war," *Security Dialogue*, 43 (2012):3-24; David M. Hollis, "Cyberwar case Study: Georgia 2008," *Small Wars Journal*, (2011, January); On Estonia see, Steve Mansfield-Devine, "Estonia: What Doesn't Kill you Makes you Stronger," *Network Security*, 7 (2012):12-20; Rain Ottis, "Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective," *Proceedings of the 7th European Conference on Information Warfare and Security* (Plymouth: Academic Publishing Limited: 2008), pp 163-168; on Flame see: Kate Munro, "Deconstructing Flame: the limitations of traditional defences," 10, *Computer Fraud & Security*, (2012): 8-11; Oleg Demidov and Maxim Simonenko, "Flame in Cyberspace," *Security Index: A Russian Journal on International Security*, 19:1 (2013); 69-72

The nuclear literature in turn has seen great strides in research design over the past few decades. As Hymans notes, on the demand-side, the old-style literature of listing potentially motivational variables - even though essential in moving the field forward - has increasingly been replaced with "genuine theory of proliferation with clear microfoundations linking cause to effect and with multiple testable hypotheses."[25] Also, on the supply-side, since Meyer's study in the late 1970s, we have seen increasingly more sophisticated studies..[26] In the 2000s a number of new works were published improving Meyer's input set.[27] Furthermore, recent supply-side studies have opened up an interesting avenue of research on how nuclear technology, materials, and knowledge transfer to non-nuclear weapon states affects the proliferation of nuclear weapons.[28] Overall, we can learn from the methodological development of the nuclear literature and set up a more intelligent research design at the outset on cyber proliferation.

1.5. Data Analysis

1.5.1 The Data Paradox

There is little information about cyber proliferation. The acquisition of weapon systems is normally a covert activity which takes place behind closed government doors, especially when it comes to Weapons of Mass Destruction (WMD). We therefore tend to rely on circumstantial evidence for our assessments.[29] This in turn has led to frequent misattribution, sometimes with disastrous policy

[25] Jacques E.C. Hymans, "Nuclear Proliferation and Non-Proliferation," *International Studies Encyclopaedia*, (2009) 5447-5466, p. 5455

[26] Meyer, *The Dynamics of Nuclear Proliferation;* For a more critical perspective see: Montgomery and Sagan, "The Perils of Predicting Proliferation"; Mark S. Bell, "Examining Explanations for Nuclear Proliferation: Research Note," *International Studies Quarterly*, 60 (2016)520-529

[27] Jo and Gartzke, "Determinants of nuclear weapons proliferation,"; Dong-Joon Jo and Erik Gartzke, "Data notes for Determinants of Nuclear Weapons Proliferation," (2007), Retrieved from: http://jcr.sagepub.com/content/vol51/issue1/images/data/167/DC1/Jo&Gartzke_(Feb_07).zip

[28] Matthew Kroenig, "Importing the Bomb: Sensitive Nuclear Assistance and Nuclear," J*ournal of Conflict Resolution,* 53:2 (2009)161-180; Matthew Kroenig, "Exporting the Bomb: Why States Provide Sensitive Nuclear Assistance," *American Political Science Review*, 103:1 (2009): 113-133; Matthew Kroenig, *Exporting the Bomb: Technology Transfer and the Spread of Nuclear Weapons*, (Ithaca, New York: Cornell University Press: 2010); Matthew Fuhrmann, "Spreading temptation: proliferation and peaceful Nuclear Cooperation Agreements," *International Security*, 34:1 (2009): 7-41; Matthew Fuhrmann, "Taking a walk on the supply side: the determinants of civilian nuclear cooperation," *Journal of Conflict Resolution*, 53:2 (2009):181:208; Robert L. Brown and Jeffrey M. Kaplow, "Talking Peace, Making Weapons IAEA Technical Cooperation and Nuclear Proliferation," *Journal of Conflict Resolution,* 58:3 (2014) 402-428

[29] New pieces of evidence can increase the plausibility of a given attributive theory or raise doubts about it, but are not decisive by themselves. Political Scientists doing hypothesis testing call these 'Straw-in-the-wind tests'. This type of evidence provides neither a necessary nor a sufficient criterion for accepting or rejecting a hypothesis, and they only slightly weaken rival hypotheses. It means we rely on a form of Bayesian inference, as we constantly need to link (new) pieces of evidence to update our beliefs about an actor's capabilities.

consequences.[30] Arms proliferation scholars have relied on different sources - academic case studies, declassified reports, and public statements/actions - to minimize this problem.[31]

This study cannot rely on the same sources to assess cyber proliferation. Given the immaturity of the literature, there is no significant body of previous country-specific case studies. Also, few declassified government reports exists on the cyber capabilities of other states. In fact, the incentives for states to not reveal information about their capability might be even stronger than other technical fields, like the nuclear domain, due to the transitory nature of cyber weapons.[32] With cyber weapons' effectiveness primarily coming from its element of deception, demonstrating offensive capability - like with nuclear tests - likely reduces its effectiveness.[33]

But, there is also too much information about cyber proliferation. For nuclear proliferation, we only have two actual incidents: the atomic bombings of Nagasaki and Hiroshima in 1945. In turn, the number of times a capability was used to gain unauthorized access to a computer system or network is almost incomprehensibly high. According to Verizon's 2015 Data Breach Investigations Report, more than 317 million new pieces of malicious software were created last year.[34] The New York

[30] Indeed, the U.S. invasion in Iraq, following the accusation that Sadam Hussein had WMD, is a well-known example. As Hayden states in his biography; "But we all thought that there as a case for weapons of mass destruction. I was in George Tenet's conference room when we voted on the now-infamous National Intelligence Estimate (NIE). I voted yes - on all counts. I was comfortable with the vote, then. I had earlier told Condi Rice, the national security advisor, in a private conversation, that I had a roomful of evidence that Saddam had a WMD program. 'A roomful of evidence,' I confided, 'all of it circumstantial.' Michael Hayden, *Playing to the Edge: American Intelligence in the Age of Terror*, (New York, Penguin Random House, 2016), p. 49

[31] Gartzke and Jo offer the most comprehensive dataset on nuclear weapons. The scholars rely on i) previous case studies from other scholars; ii) records of countries which have publicly declared possession of nuclear weapons; iii) records of countries that have denoted nuclear weapons.

[32] The transitory nature of cyber weapons refers to short-lived or temporary ability of cyber weapons to effectively cause harm or damage. For an elaborate discussion on this point see: Smeets, "A Matter of Time"; The inherent properties of cyber weapons may not be the only reason why we have witnessed this level of secrecy; it likely also has to do with the institutional context of this capability development. As former director the NSA and CIA, Michael Hayden states "[b]eyond complexity, developing policy for cyber ops is hampered by excessive secrecy (so says this intelligence veteran!). Look at the bloodline. I can think of no other family of weapons so anchored in the espionage services for their development (except perhaps armed drones). And the habitual secrecy of the intelligence services has bled over into cyber ops in a way that has retarded the development - or at least the policy integration - of digital combat power. It is difficult to develop consensus views on things that are largely unknown or compartmented or only rarely discussed by a select view." Hayden, *Playing to the Edge*

[33] As Fred Kaplan writes about the U.S. history 'cyber war' preparations: "[t]here was the extreme secrecy that enveloped everything about cyber war. Some things about nuclear weapons were secret, too: details about their design, the launch codes, the targeting plans, the total stockpile of nuclear materials. But the basics were well known: their history, how they worked, how many there were, how much destruction they could wreak - enough to facilitate an intelligent conversation, even by people who didn't have Top Secret security clearances. This was not true of cyber: when Admiral Rogers testified that he wanted to 'increase our capacity on the offensive side,' few, if any, of the senators had the slightest idea what he was talking about. Fred Kaplan, *Dark Territory: The Secret History of Cyber War,* (New York: Simon and Schuster: 2016), p. 284-285

[34] Verizon, "Data Breach Investigations Report," (2015), retrieved from: https://iapp.org/media/pdf/resource_center/Verizon_data-breach-investigation-report-2015.pdf; With 131.4 million births per year, that means that for each baby born in the world, more than two new pieces of malware are created. Ecology, "World Birth and Death Rates," retrieved from: http://www.ecology.com/birth-death-rates/

Times alone published almost 500 online articles on cyber activities in 2016.[35] And, unlike most other fields of study, there is a large private industry - with firms like Kaspersky Lab's GReAT, FireEye's iSIGHT, Intel Security's McAfee, Symantec's DeepSight, or Crowdstrike - focusing on uncovering cyber activities.[36]

1.5.2 Making Sense of the 'Cyber Hodgepodge'

There is something of a 'cyber hodgepodge' of overlapping and constantly evolving threat actors, operations, and malware - making it a real challenge to understand the cyber landscape. What adds to the difficulty is that cyber security firms are extremely liberal in their naming of threat actors and incidents.[37] For example, as figure 1.2 indicates, SoFacy - the cyber espionage group associated with the Russian military intelligence agency GRU - has received at least seven different labels.[38] The confusing labelling creates a barrier for others who do not have the time or knowledge to cross-reference the alphabet soup of labels.[39]

[35] The reports found may refer to issues other than offensive cyber operations. I conducted an online search with search term 'cyber'. Dates used were 2016, January 1 - 2017, January 1. See: https://query.nytimes.com/search/sitesearch/?action=click&contentCollection&region=TopBar&WT.nav=searchWidget&module=SearchSubmit&pgtype=Homepage#/cyber/from20160101to20170101/

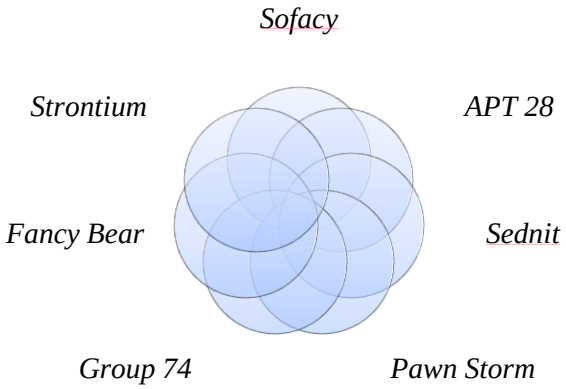
[36] See Appendix 2 for a more comprehensive discussion on the potential biases in threat reporting of these firms.

[37] Indeed, like palaeontologists or astronomers, cybersecurity firms like to name their new discoveries. TEDx Talks, "The shape-shifting skulls of dinosaurs | Jack Horner | TEDxVancouver," *YouTube*, (2011, April 13) retrieved from: https://www.youtube.com/watch?v=xYbMXzBwpIo

[38] Granted, attribution is more difficult in cyberspace. Unlike palaeontologists, cyber threat intelligence firms cannot use carbon dating to identify the origins or age of their discoveries. But that makes it all the more important that firms are cautious with their labelling. Cybersecurity firms mostly rely on circumstantial evidence, and different firms rely on different data, techniques and resources to extract this information. New pieces of evidence can increase the plausibility of a given attributive theory or raise doubts about it, but are not decisive by themselves. It means security researchers constantly need to link (new) pieces of evidence to update their beliefs about a threat actor. By giving the same threat different names, they might miss out on knitting the pieces of evidence together. Also see: Max Smeets, "When Naming Cyber Threat Actors Does More Harm Than Good," *Council on Foreign Relations: NetPolitics*, (2016, October 24), retrieved from: https://www.cfr.org/blog/when-naming-cyber-threat-actors-does-more-harm-good

[39] Also the same term may have various meanings. For example, take the relatively well-known case of 'Duqu'. First, the term 'Duqu' may refer to the malware; that is the software components such as the espionage features, kernel drivers, and injection tools which serviced the attackers. Duqu could also refer to the still unknown programming language used or to the Microsoft Windows flaw that was used to execute the malware. Finally, we may talk about 'Duqu' as an operation - one of which the goals are still unknown.

Figure 1.1: Overview of Labels used for Threat Actor 'SoFacy'



In fact, even trained analysts frequently confuse terms, leading to erroneous analysis. One of the most important reports published over the past year was a joint report from the U.S. Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI) titled "GRIZZLY STEPPE - Russian Malicious Cyber Activity".[40] The report documents other groups identified as the Russian Military and Civilian intelligence Services (RIS). As Robert M. Lee notes:

> This would be exciting normally. Government validation of private sector intelligence helps raise the confidence level of the public information. Unfortunately, the list in the report detracts from the confidence because of the interweaving of unrelated data. As an example, the list contains campaign/group names such as APT28, APT29, COZYBEAR, Sandworm, Sofacy, and others. This is exactly what you'd want to see although the government's justification for this assessment is completely lacking […]. But as the list progresses it becomes worrisome as the list also contains malware names […] (which are different than campaign names). […] It gets worse though when the list includes things such as 'Powershell Backdoor'. This is not even a malware family at this point but instead a classification of a capability that can be found in various malware families.[41]

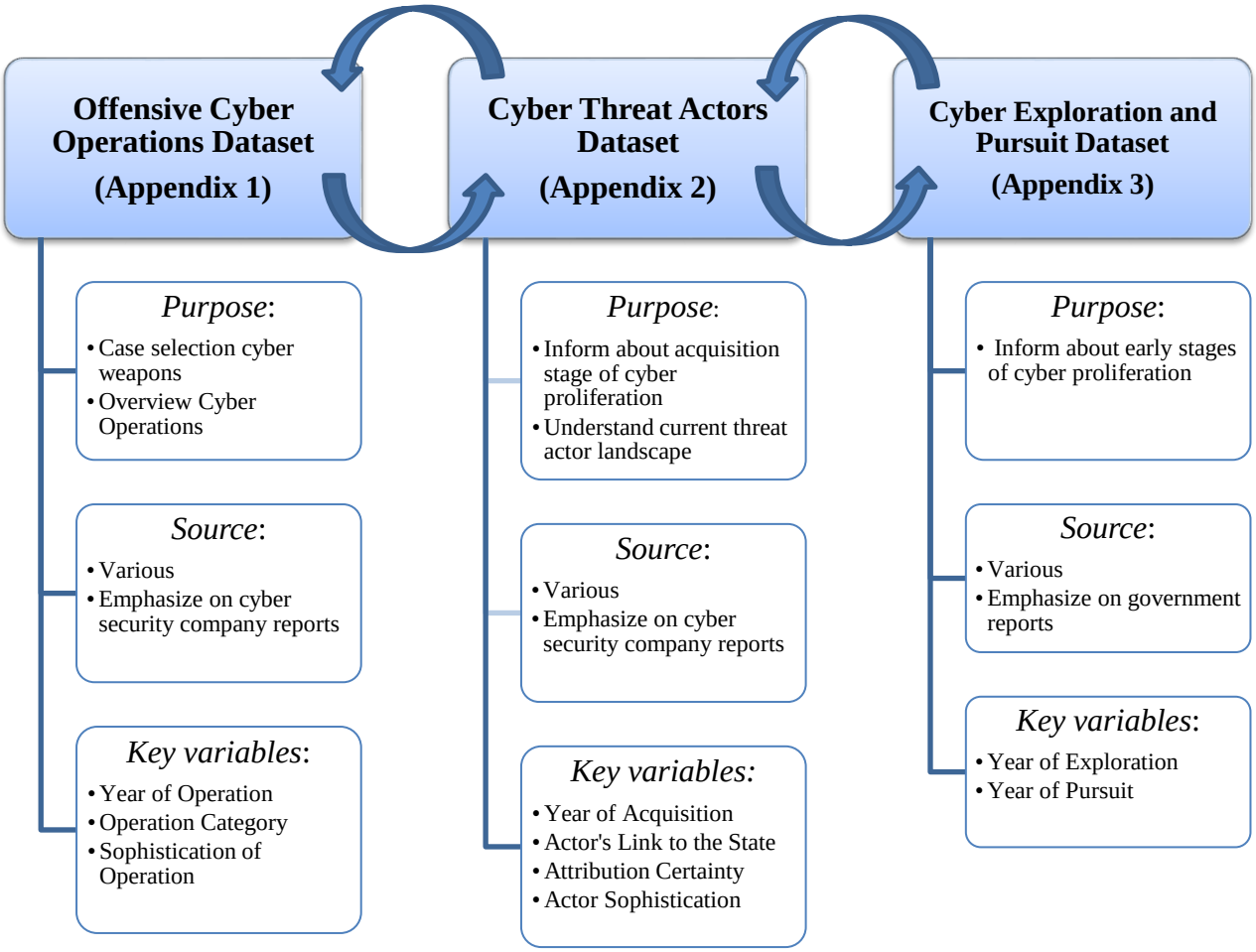
Hence, it requires great analytic rigour of the researcher to accurately capture the cyber threat landscape, and thus 'cyber proliferation'. With this in mind, I developed three new datasets: the *Cyber*

[40] The White House, "Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment", *Office of the Press Secretary*, (2016, December 29), retrieved from: https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity; US Department of Homeland Security and the Federal Bureau of Investigation, "GRIZZLY STEPPE - Russian Malicious Cyber Activity," *Joint Analysis Report*, (2016, December 29), retrieved from: https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

[41] Robert M. Lee, "Critiques of the DHS/FBI's GRIZZLY STEPPE Report," (2016, December 30), retrieved from: http://www.robertmlee.org/critiques-of-the-dhsfbis-grizzly-steppe-report/; A similar problem is found in a prominent analysis on Chinese intrusions by Jon Lindsay. Although the scholar provides an excellent analysis of China's cyber activities, when it aims to provide an overview of Chinese activity it conflates intrusions (such as Titan Rain, F-35 JSF) and threat actors (such as APT1, APT12, Ixeshe, and Lurid). See: Jon R. Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction," *International Security*, 39:3 (2014/2015):7-47

Exploration and Pursuit Dataset (Appendix 1), *the Cyber Threat Actors Dataset* (Appendix 2), and *the Offensive Cyber Operations Dataset* (Appendix 3).

Figure 1.2: General Overview of datasets



1.5.3 Offensive Cyber Operations Dataset

Let us first consider the *Offensive Cyber Operations Dataset*. The *Offensive Cyber Operations Dataset* primarily serves to improve our understanding and case selection of cyber weapons. Most events part of the 'cyber hodgepodge' concern minor cases of hacktivism or criminal activity. As a result, identifying the cases in which a cyber weapon was actually utilized is it a bit like foraging for edible mushrooms in a forest. Finding the desired species of mushrooms can be a challenge - even if it is known to grow in a certain region - as there is so much other fauna around. The *Offensive Cyber*

Operations Dataset helps to overcome this setback, allowing me to carefully delineate the overall population of cyber weapons from the general population of cyber events.[42]

Cyber attacks are often described as discrete events; i.e. a system gets breached, the intrusion gets detected, and a system gets patched. Part of the reason I use the term 'offensive cyber operation' in this research is to indicate that these attacks are often *not* discrete events but continuous, evolving activities. If an adversary is unable to gain initial access, it often tries to enter in a different manner. And if an adversary gets kicked off a network, it often works hard to regain entry.

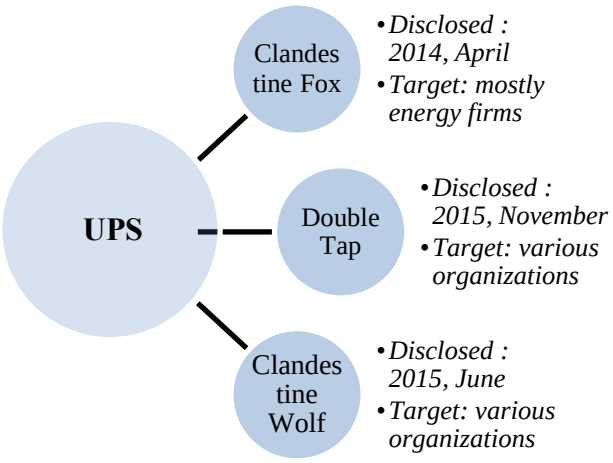
1.5.4 Cyber Threat Actors Dataset

Second, the *Cyber Threat Actors Dataset* surveys which actors have offensive cyber capabilities. The aggregate findings of this dataset facilitate our understanding of which states have acquired cyber weapons (i.e. helps us to inform which state is at the 'final' stage of cyber proliferation). The dataset also allows us to make more nuanced claims about threat actors level of sophistication and connection to the state.

There is an obvious link between the *Offensive Cyber Operations Dataset* and the *Cyber Threat Actors Dataset*. We can consider cyber operations to be snapshots of attackers' capabilities and intentions. For example, consider UPS (see figure 1.3), a threat actor allegedly based out of China.[43] We know that the group has conducted at least three different operations: Clandestine Fox, Double Trap and Clandestine Wolf. Each operation provides different and additional insights as to how the group operates and has evolved.

[42] This allows for a more comprehensive assessment in chapter 4 of the costs of (each type of) cyber weapon(s).
[43] Ned Moran, Mike Scott, Mike Oppenheim, Joshua Homan, "Operation Double Tap," *FireEye*, (2014, November 21), retrieved from: https://www.fireeye.com/blog/threat-research/2014/11/operation_doubletap.html

Figure 1.3: Overview of UPS' reported cyber operations



Taking this holistic approach to understanding actors is important because one operation may not reveal the exact nature of an actor. As a report from Arbor Networks observes: "[a]ctors will typically not only use the amount of force necessary to accomplish their actions on objectives and will not typically burn 0day exploit code or the most advanced techniques against targets that do not require them."[44]

Threat actors' characteristics and activities may also evolve over time. One possibility is that threat actors change their target base. For example, Iron Tiger, allegedly originating from China, used to target government and other political entities in East Asia around 2010. Yet, Trend Micro indicated that the APT had shifted their attention in 2013, starting to target U.S. entities.[45] Today, they seem to be active in Europe too.[46] In addition, actors may also become more or less dexterous in their cyber

[44] Arbor Networks, "ASERT Threat Intelligence Report 2016-03 The Four-Element Sword Engagement," (2016), retrieved from: https://www.arbornetworks.com/blog/asert/wp-content/uploads/2016/04/ASERT-Threat-Intelligence-Report-2016-03-The-Four-Element-Sword-Engagement.pdf; In addition, at times cyber attacks may also be used as 'testing ground' for potential future activity. A McAfee report, for example, draws this conclusion for the campaign called 'Ten Days of Rain': "DDoS, malware-leveraging encryption, and multitier botnet architectures are not new. Nor are attacks against South Korea that suspiciously align with North Korea's agenda. However, the combination of technical sophistication juxtaposed with relatively limited execution and myopic outcome is analogous to bringing a Lamborghini to a go-cart race. As such, the motivations appear to outweigh the attack, making this truly seem like an exercise to test and observe response capabilities." See: McAfee, "Ten Days of Rain Expert analysis of distributed denial-of-service attacks targeting South Korea," *White Paper*, Retrieved from: https://www.mcafee.com/us/resources/white-papers/wp-10-days-of-rain.pdf, p. 12

[45] In both cases the APT-style operations started with well-written spear phishing emails. Christopher Budd, "Operation Iron Tiger: Attackers Shift from East Asia to the United States," *TREND Micro*, (2015, September 15), retrieved from: Newsroom.trendmicro.com/blog/operation-iron-tiger-attackers-shift-east-asia-united-states

[46] A case which is at least as interesting is referred to as the 'Umbrella Revolution' attacks, in which multiple actors were part of the same operation, altering its conventional target base. As Crowdstrike writes: "the PRC's efforts to quietly quell the Umbrella Revolution in Hong Kong bore fingerprints and tradecraft attributed to multiple PANDA groups, suggesting Beijing called several known groups off of their normal targeting to address an issue of importance

activities. Although cyber security firms tend to report on how actors grow in sophistication, the opposite may occur as well. FireEye writes about UPS (see figure 1.3) "[t]he attacker leveraged multiple exploits [...]. Since Operation Clandestine Fox, we have observed this actor execute multiple attacks that did not rely on zero-day exploits. The combination of this sustained tempo and lack of zero-day exploits may indicate that this group has changed strategy and has decided to attack more frequently and does not have steady access to zero-day exploit code."[47]

Finally, there is often significant overlap between actors and operations.[48] The overlap makes it often difficult to discern, based on public information, whether these are new actors or the same actors (with potentially new members/employees).[49] For example, Crowdstrike has separately reported on Stone Panda and Nightshade Panda. Yet, as researchers from the Institute for Critical Infrastructure Technology write: "Nightshade Panda [...] shares many similarities to its sister campaign, Stone Panda. Nightshade Panda also specializes in network reconnaissance, lateral network exploration, data exfiltration, and cyber espionage. Nightshade likely delivers malware through targeted spear-phishing emails. Nightshade Panda relies on the PoisonIvy malware, also used by Stone panda and Axiom, and on the PlugX malware, used by Naikon."[50] Considering these similarities, there is little certainty membership or resources in these threat actor groups do not overlap.

1.5.5 Cyber Exploration and Pursuit Dataset

Third, the *Cyber Exploration and Pursuit Dataset* is the least complicated data collection effort compared to the other two datasets. It helps to understand the activity at the early stages of

---

to the PRC government." See: Adam Kozy, "Rhetoric Foreshadows Cyber Activity in the South China Sea," *Crowdstrike*, (2015, June 1), retrieved from: https://www.crowdstrike.com/blog/rhetoric-foreshadows-cyber-activity-in-the-south-china-sea/Threat Connect, "A Tale of Two Targets,"(2016, October 17), retrieved from:Threatconnect.com/blog/threatconnect-discovers-chinese-apt-activity-in-europe/https://www.crowdstrike.com/blog/rhetoric-foreshadows-cyber-activity-in-the-south-china-sea/;

[47] Moran, et al., "Operation Double Tap,"

[48] The constant urge to (re)name makes it also more likely that cybersecurity firms refer to old threats as new ones. Being too quick in naming new threat actors, firms are more likely to lose sight of how actors might have evolved. They are more likely to exaggerate network learning effects (i.e. that one threat actor learned from another actor) and underestimate a single threat actor's ability to learn (i.e. that the same actor acquired new skills). See: Smeets, "When Naming Cyber Threat Actors Does More Harm Than Good"

[49] Crowdstrike provides a similar statement when discussing a malware called Sakula:"[o]ften during the investigation of sophisticated threat actors, the demarcation between the different attackers and campaigns are blurry. Researchers need to rely on tradecraft and analytic rigor to understand the unseen components of the attack, this often necessitates an intelligence assessment. The use of an intelligence assessment around a set of activities introduces room for error, which is generally balanced with confidences and likelihoods." Matt Dahl, "Sakula Reloaded", *Crowdstrike*, (2015, November 18), Retrieved from: www.crowdstrike.com/blog/sakula-reloaded/

[50] James Scott and Drew Spaniel, "China Espionage Dynasty: Economic Death by A Thousand Cuts," *Institute for Critical Infrastructure Technology*, (2016, July 28), retrieved from: http://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2016/2016.07.28.China_Espionage_Dynasty/ICIT-Brief-China-Espionage-Dynasty.pdf

proliferation (i.e. exploration and pursuit). It relies on a wide range of sources, including: academic publications, public sources, and leaked documents.

Combined with information from the *Cyber Threat Actors Dataset* it helps to provide a complete picture of cyber proliferation, in that it captures the four stages of 'No discernible activity', 'exploration', 'pursuit', and 'acquisition'.

1.6 Structure of the Thesis

The body of this thesis consists of five chapters. Chapter 2 describes the current conceptual problems which exist within the cyber literature, suggests ways to resolve these conceptual issues, and moves towards a more consistent and analytically useful definition and application of cyber-related concepts. This conceptual clarification not only facilitates the security dialogue between and across academic communities undertaking cyber research, but also provides a key building block for understanding the nature of cyber proliferation. Following Gary Goertz' work, I conduct a multidimensional and multi-level analysis of the concept 'cyber weapon', dividing it into four levels for analytical purposes: i) the base, ii) qualificatory, iii) secondary, iv) and indicator level. Cyber weapons are defined as a capability designed to access a computer system or network to damage or harm living or material entities.[51]

After this conceptual exercise, chapter 3 surveys the current landscape of cyber proliferation. Estimates on how many states have so far proliferated vary widely. Chapter 3 analyses which states currently have explored, pursued or acquired cyber weapons. The data collection and analysis also makes it possible to capture potential variation in governments' reliance on proxy actors for conducting offensive cyber operations. The final part of the chapter looks at whether potential entry order effects exist (i.e. the 'first mover' and 'latecomer' advantages) when it comes to states' development of offensive cyber capabilities.

Following this largely descriptive exercise, my analysis moves towards the explanatory realm. In chapter 4 I turn to the supply-side of cyber proliferation, addressing the requirements for a state to develop cyber weapons. In the first part of this chapter, I provide an overview of the key cyber incidents since the Morris Worm was released into the wild in 1988 in order to identify in which of these incidents a cyber weapon was utilized. The second part of this chapter offers an empirical

[51] As cyber weapons are primarily non-physical, it makes more sense to talk about cyber weapons as a capability rather than a tool.

analysis of the development costs of different types of cyber weapons.[52] The chapter also delves into drivers for cost reduction and the incentives for the transfer of cyber weapon technology.

Chapter 5 looks at the demand-side factors of cyber proliferation. Taking Sagan's classic conceptualization as a starting point of analysis, three analytical frameworks are defined and empirically assessed about why states develop cyber weapons. The three frameworks are further specified based on a large body of more recent literature which has improved our understanding of the governments' motives for weapons development and restraint. For each theoretical framework, I compare their theoretical insights of the causes of cyber weapon development, present alternative interpretations of several cases, and contrast the frameworks implications for policies of cyber weapon restraint, and refer to general theories and debates about state behaviour in international relations.

Finally, chapter 6 extends the demand-side analysis and assesses the strategic utility of cyber weapons. This is a largely prescriptive exercise, as there is a sense that state leaders and policy makers themselves do not have a strong conception of its strategic advantages and limitations. Weapons are normally considered to have two broad forms of strategic value. First, weapons can sometimes have a strategic value as a signalling and/or bargaining device in which the threat of usage leads to the obtainment of a political goal. Second, the strategic utility can come from the actual deployment of a weapon to attack a certain target. This chapter addresses each dimension in turn.

Chapter 7 concludes by summarizing the main results and laying out a future research agenda to address the weaknesses in our current understanding of the causes of cyber proliferation. It also outlines the contributions of the thesis to international relations theory and debates.

[52]As the population of cyber weapon cases is not very large, I was able to conduct a 'thin' small N analysis of *all* cases.

Chapter 2: The Concept of 'Cyber Weapon'

Just like mutual and shared understandings of values are considered to be the essential building blocks of any society, so are mutual and shared understandings of concepts considered to be the foundation of any academic area of research. In this chapter, focusing on concept clarification and development, I therefore aim to lay the foundation for understanding the requirements for developing cyber weapons and formulating propositions on the requirements of developing these capabilities. The first section lays out the current conceptual problems which exist within the cyber literature. Drawing on the relevant literature on cyberspace - both within and outside the IR discipline - section 2.2 develops a conceptual understanding of the term 'cyber weapon', dissecting the concept into four levels: i) the base, ii) qualificatory, iii) secondary, iv) and indicator level. Section 2.3 concludes and summarizes the essential features of a cyber weapon.

2.1 Current Conceptual Problems

Cyber-related concepts - such as 'cyberspace', 'cyber domain', 'cyber-attack', and 'cyber weapon' - have stubbornly entered the daily vocabulary of scholars, practitioners and media officials. The prefix 'cyber-' lends its original meaning from the word 'cybernetics', popularized by mathematician Norbert Weiner in 1961 in his book "Cybernetics Or Control and Communication in the Animal and the Machine".[53] Weiner, unifying control theory with communications theory, borrowed the ancient Greek adjective 'κυβερνητικός', meaning *governing, piloting, or skilled in steering*, to describe what was at the time a futuristic idea; that one day there would be a self-governing computer system, completely running on (information) feedback.[54]

The term 'cyberspace' was further developed and popularized by speculative fiction novelist William Gibson in 1984, defining it as "[a] consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts. [...] A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding."[55] In 1996, the term was imported to the political realm by libertarian John

[53] Norbert Weiner, *Cybernetics Or Control and Communication in the Animal and the Machine,* (Cambridge: the MIT press: 1961); also see: Thomas Rid, *Rise of the Machines: A Cybernetic History*, (New York: W. W. Norton & Company: 2016)
[54] Ibid.
[55] William Gibson, *Neuromancer*, (New York: Ace: 1984); 51-67. Gibson coined the term 'cyberspace' in opposition to the term 'meatspace'. The latter has never found its way into the common language.

Perry Barlow, who starts his essay with "[g]overnments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather."[56]

Even though there is little speculation on the origins of the cyber-related terms, unresolved conceptual issues regarding the current use are still abound. Ret. General Michael Hayden, former director of the CIA and NSA, observes that "rarely has something been so important and so talked about with less clarity and apparent understanding than this phenomenon."[57] One can observe a mix of conceptual *stretching*, conceptual *confusion*, and conceptual *contestation* with respect to the cyber-related terms.

First, the prefix 'cyber' is conceptually *stretched* as it has been loosened up to such an extent that it often also seems to apply to incidents which have little to do with interconnected computer systems.[58] The various applications of the prefix "cyber" - such as cyber law, cyber nationalism, cybercafé, cyber warfare, cyberhate - can be considered to be examples of this activity. In the words of Giovanni Sartori, the imprudent application of the concept has led to a distortion in which the prefix cyber does not fit the new cases.[59]

Second, cyber-related concepts have also been conceptually *confused* as the term has often been misunderstood and misinterpreted. The concepts 'information technology', 'digital', 'virtual', 'computer systems', and 'the internet' have often been considered to be synonymous to 'cyber'.[60] In similar vein, some authors use 'cyber warfare', 'network centric warfare', and 'information operations' interchangeably without understanding the implications of using a different term - leaving the distinguishing features of each concept unidentified. The prefix 'cyber-' has consequently received multiple meanings without scholars being aware of the fact that the term could refer to the *application* of computers, the *network* of computers, or he *data* produced by computers.

[56] Barlow wrote his article in response to the enactment of the Communications Decency Act in 1996 which was considered to be a threat to the independence of cyberspace. John Perry Barlow, "A Declaration of the Independence of Cyberspace, " *Electronic Frontier Foundation*, (1996) retrieved from: https://www.eff.org/cyberspace-independence
[57] Michael V. Hayden, "The Future of Things Cyber," *Strategic Studies Quarterly*, 5:1(2011):3-8; p.3
[58] Giovanni Sartori, "Concept Misinformation in Comparative Politics," *The American Political Science Review*, 64:4 (1970): 1033-1053; also see: David Collier and James E. Mahon, Jr., "Conceptual "Stretching" Revisited: Adapting Categories in Comparative Analysis," *The American Political Science Review*, 87:4 (1993):845-855
[59] Sartori, "Concept Misinformation in Comparative Politics"
[60] See for example: Lucas Kello "The Virtual Weapon: Dilemmas and Future Scenarios." *Politique étrangère,* 79: 4 (2014-15); Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School", 53,4 (2009):1155-1175; Gadi Evron, "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War," *Georgetown Journal of International Affairs*, 9:1 (2008): 121-126

Third, even though the use of cyber-related concepts has often followed the James Bond principle of 'Live and Let Die' - not recognizing that one's own use of the term is contested by others in the hope they would silently go away - one can also observe conceptual *contestation* as some scholars explicitly disagree on the meaning of the cyber-related terms.[61] It remains however unclear how substantial this disagreement is - that is, whether the prefix 'cyber' is an 'essentially contested' or merely 'hotly disputed'.[62]

The central objective of this chapter is to suggest ways to resolve these conceptual issues and move towards a more consistent and analytically useful definition and application of cyber-related concepts. This undertaking is more than mere logomachy for a number of reasons. First, conceptual clarification facilitates the security dialogue between and across academic communities undertaking cyber research, allowing to establish a common ground for discussion between those with disparate views. Second, it permits more effective knowledge accumulation, enabling hypothesis testing and theory development. For this study, it is the key building block for understanding what obstacles actors have to overcome to develop cyber weapons, with an emphasis on the technical aspects of weapons acquisition.[63] It also essential if we aim to contrast the different frameworks on the motives underlying cyber weapon acquisition. Third, conceptual clarification on cyber-related concepts has important policy implications. Governments are gradually coming to terms with the cyber perils and are establishing guidelines, policies, and institutions to deal with this (potentially) transformative technology.[64] The National Cyber Security Strategies (NCSS), periodically prepared by most countries, broadly outline the plan of actions a state intends to implement to enhance the security and

[61] Kello, "The Meaning of the Cyber Revolution"; Gartzke, "The Myth of Cyberwar"

[62] On a more theoretical discussion on the difference between essentially contested' and 'hotly disputed' see the works of Walter Gallie, particularly: Walter B. Gallie, "Essentially Contested Concepts," *Proceedings of the Aristotelian Society,* New Series, 56 (1955 - 1956):167-198; See: James Shires and Max Smeets, "What do we talk about when we talk about 'cyber'?" *SSRN: Working Paper*, (2016, October 5), retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2860839

[63] Meyer in his classic account on the dynamics of nuclear proliferation writes "No aspect of nuclear proliferation has been dealt with so comprehensively as the technology of nuclear weapons and nuclear weapons production. The intricacies of designing and building plutonium production reactors and reprocessing plants and the problems and pitfalls of enriching uranium have all been discussed in great detail. Options for diverting nuclear fuel from civil nuclear power facilities have received the most attention of all. And whatever can be said in the open literature (and probably some things that should not) about designing and building an atomic bomb has already been said." The opposite is true for cyber weapons; we still do not have a good understanding of what is required to design and develop different types of cyber capabilities. Meyer, *The Dynamics of Nuclear Proliferation,* p. 19

[64] Indeed, as Knake indicates, "the rise of cyber crime, the emergence of cyber espionage, and the specter of cyber warfare have led many foreign governments to exert sovereign authority over their networks and to press international organizations to take up these issues." See: Robert Knake, "Internet Governance in an age of cyber insecurity, "*Council on Foreign Relations,* Council Special Report No. 56 (2010, September)

resilience of its national critical infrastructure.[65] Most, however, do not have firm understanding of what constitutes the 'cyber issue'. Most Members States of NATO do not define any of the cyber-related concepts in their respective NCSS. Only for those who view the cyber security policies proposed in the NCSS as a panacea, as remedies for the cyber-problem regardless of its character, the current modus operandi is the correct approach. But, it is a fallacy to think that one can jump to (loose) policy formulations before clarifying the nature of the phenomenon we are dealing with. Concept development should *precede* strategy development.

2.2 Conceptualizing Cyber Weapons as a Multilevel Concept

There are a variety of ways one can construct a concept. Similar to Gary Goertz' work, this study proposes a causal, ontological, and realist view of the concept 'cyber weapon'.[66] This study's analysis is *ontological* because it focuses on what constitute a cyber weapon. It is *causal* because it aims to identify which scientific properties of the cyber weapon play a role in explanations of the development and use of cyber weapons.[67] It is *realist* because an empirical analysis is provided on cyber weapons.[68]

The concept 'cyber weapon' is multidimensional and multilevel in nature. One can dissect the concept into four levels; i) the base, ii) qualificatory, iii) secondary, iv) and indicator level. In this study, the base level requires an analysis of the basic term 'weapon'. The next level down, the qualificatory level, the cognitively central word 'cyber' should be analysed.[69] In turn, at the secondary level, one can lay out the constitutive dimensions of cyber weapons. In the words of David Collier and James Mahon, Jr., it highlights the "boundaries and defining properties that are shared by all members and that serve to locate it in the hierarchy".[70] Finally, at the indicator level, the lowest level of conceptual analysis, one can specify the dimensions further making operationalization possible. In moving down the levels, the analysis becomes more technical allowing for (and requiring) the integration of various different disciplinary studies on the cyber issue.

---

[65] At the moment, all members of NATO have established a National Cyber Security Strategy, and about the 55+ countries worldwide have developed a strategy. The National Cyber Security Strategies serve as both a priority list and logbook to ensure that key national objectives on cyber security are achieved within a multiyear timeframe.
[66] Gary Goertz, *Social Science Concepts: A User's Guide* (Princeton: Princeton University Press: 2005)
[67] As Goertz indicates "[o]ne cannot neatly separate the ontology of a concept from the role it plays in causal theories and explanations." Goertz, *Social Science Concepts*, p. 28
[68]The term 'realist' in this context should not be confused with the IR theories of 'classical realism' and 'structural realism'.
[69] As will be discussed below, this level is added to Goertz' framework in an attempt to clarify that cyber weapons are a subpart of weapons.
[70] Collier and Mahon, "Conceptual 'Stretching' Revisited", p. 845

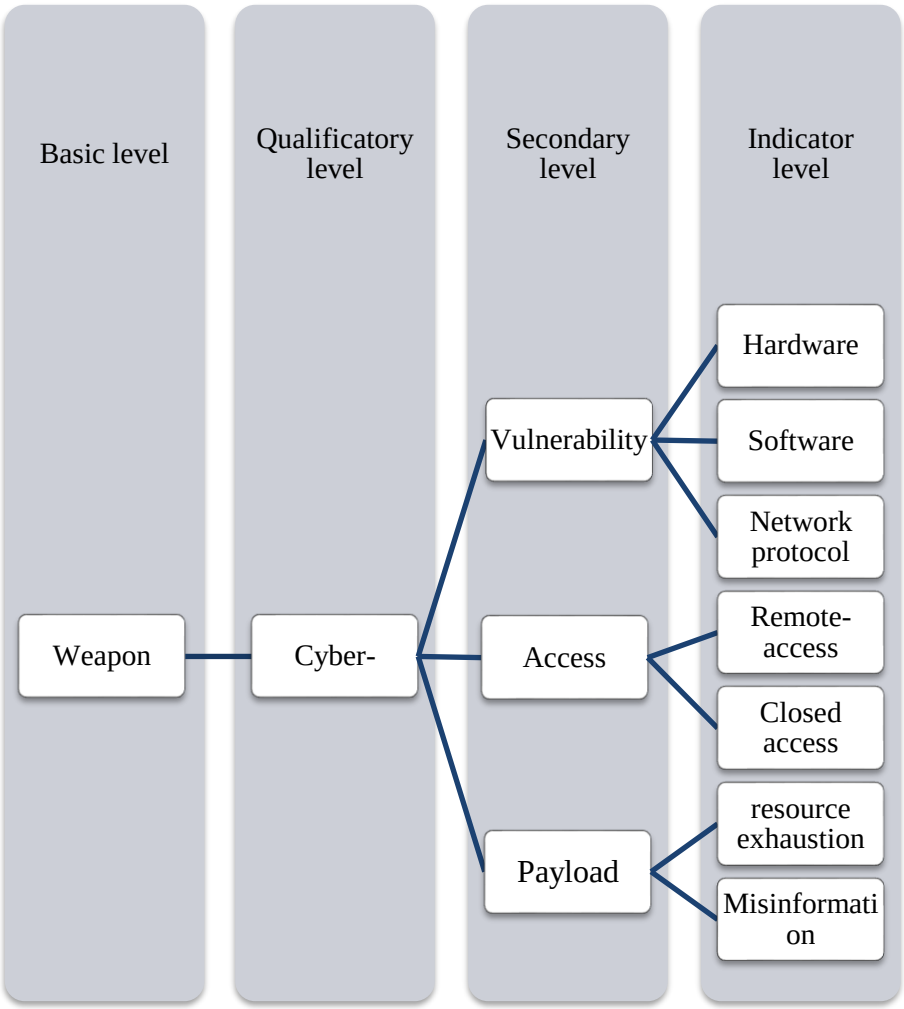
This study adds the ’qualificatory level’ is added to Goertz original multilevel framework. This level of conceptual analysis deserves separate classification and analysis as the prefix of a concept can change the semantic meaning of it.[71] More specifically, the qualificatory level can alter the secondary-level dimensions which constitute the base level.

Also, what is considered to be the ’base level’ of a concept very much depends on the purposes underlying the academic conduct of the scholar. Take for example the case in which a conceptual analysis of ’warship’ is conducted. Military strategists will consider the term ’war’ to be essential (i.e. the base level) for theory and model development. A ’ship’ from their perspective is simply one of the tools employed in warfare - like a tank, aircraft, or other weapon system. The military strategists’ perspective can be contrasted to scholars primarily interested in ship building. They will find the term ’ship’ to be most important for their conceptual development. Indeed, a warship for them is simply a particular kind of ship potentially worth studying as case study.[72]

A summary overview of the conceptual analysis can be found in figure 2.1.

[71] Prefixes can be either inflectional, changing the syntactic category, or derivational, changing either the lexical category or the semantic meaning. In English, there are no inflectional prefixes.
[72] I thank James Shires for providing this example.

Figure 2.1: Summary Conceptual Analysis of a Cyber Weapon [73]



2.2.1 The Base Level: Weapons

A first step definition of 'cyber weapons' is inherently based on the meaning of weapons more generally. It is said that we often take for granted the very things in life that are most common to us. A similar dynamic seems to exist with respect to term 'weapon'. The meaning of the concept primarily exists through its long-lived and widespread practical use rather than theoretical

[73] The indicators underlying each of these properties might overlap to a certain degree. For example, with respect to the access vector, as Lin indicates, "a close-access cyberattack might result in the implantation of friendly code in online, Internet-propagated updates to a widely used program." Owens, Dam, and Lin, "*Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*," p. 85

discussion.[74] Most of the social science dictionaries do not even define the term 'weapon'.[75] The U.S. Department of Defence, even though it charges the military secretaries to "[e]nsure that a legal review of the acquisition of all non-lethal weapons is conducted," has no directive defining the term weapon.[76] Also the law-making community generally avoids defining the term. In spite of the fact that 71 nations have ratified Additional Protocol I to the 1949 Geneva Conventions, no accepted definition of the term 'weapon' exists in international law.[77]

The most common used definition of a weapon is that it is *a tool or instrument used to inflict harm or damage.*[78] Following this basic definition, one can formulate three general statements about the identification of a weapon.

First, it is easier to determine if a tool or instrument is a weapon if it causes a high level of (observable) harm or damage. The question 'when is harm caused?' has kept many scholars busy for centuries. It has particularly been prominently addressed in the legal scholarship. Following from the 'Harm Principle' of John S. Mill in On Liberty, 'causing harm to others' is set as one of the key principles for legitimate coercion. Following the Millian scholarship, one of the most prominent ways to think of harm as actions that affects actor's interests negatively.[79] Interests do not just refer to an actor's ultimate goals: such aims as obtaining a PhD for a student or hosting the Olympic Games for a state. It also concerns less grand interests - generally of a kind shared by most others. In this category belong interests such as staying healthy for a person or ensuring survival for a state/regime.[80]

---

[74] The lack of thinking about the term can be linked to the intellectual development of International Relations (IR) as a discipline. As the IR discipline matured as an interdisciplinary field of study during the Cold War, no one seemed to bother about defining the concept. A tendency which is not strange considering that it was the Hiroshima bomb, instantly killing 80,000 people in the blast or from the firestorms that raged moments later, that opened up this period of history. The unprecedented destructiveness of the atomic bomb meant that in the case of nuclear weapons, the focus was on the (strategic) consequences of the prefix 'nuclear' rather than the conceptual meaning of the term 'weapon'. Similar point made in: Rid, and McBurney, "Cyber-Weapons"

[75] See for example: Robert L. Miller and John D. Brewer, *The A-Z of Social Research: a dictionary of key social science research concepts,* (London: Sage: 2003); Craig Calhoun, *Dictionary of the Social Sciences,* (Oxford: Oxford University Press: 2002)

[76] The US Department of Defense does provide a definition for the term 'non-lethal weapons'. However, it uses the term 'weapon' without further elaboration starting that "non-lethal *weapons*" are "*weapons* that are explicitly designed and primarily employed so as to incapacitate personnel or materiel, while minimizing fatalities, permanent injury to personnel, and undesired damage to property and the environment." Duncan Blake and Joseph S. Imburgia, " 'Bloodless weapons?' The Need to Conduct Legal Reviews of Certain Capabilities and the Implications of Defining them as 'Weapons,'" *The Air Force Law Review*, 66 (2010)

[77] Also see: Ibid.

[78] Oxford English Dictionary, W*eapon*, (Oxford: Oxford University Press, 2011)

[79] Rees is influential in distinguishing between actions that merely affect others, and those than affect people's *interests*. John C. Rees, "A Re-Reading of Mill On Liberty", in John Gray and G.W. Smith (eds.), *J. S. Mill On Liberty in Focus*, (London: Routledge: 1996), p. 174.

[80] Feinberg makes a similar point related to the moral limits of the criminal law. See Joel Feinberg, *The Moral Limits of the Criminal Law Volume 1: Harm to Others*, (Oxford: Oxford University Press: 1987), p. 37. As Mill states, interests differ for persons: "When we talk of the interests of a body of men, or even of an individual man, as a principle

Although perhaps less obvious, 'damage' can also be thought of in terms of interests. As Joel Feinberg writes, "although far more things are capable of being damaged or broken than of being harmed (in a proper sense), not everything we can name is capable even of being damaged or broken. It is impossible, for example, to break or damage the number seven or the law of gravity."[81] Feinberg continues to state that; "[e]ven so mundane an object as a rock is not the sort of thing that can be broken or damaged in normal circumstances, though it can be split, shattered, chipped, and the like. For a rock to be coherently described as broken or damaged, it must either have some special value to a human being or have some function in a larger complex that has now been impaired."[82] An example of the sort that can cease 'working' would be the traffic control system or manufacturing processes. It also means that, if you destroy a (working) machine already on a metal scrap recycling waste belt you do not cause any damage. Yet, if you destroy the same machine when still used in a factory, damage is caused.

Following the first principle, it is difficult to deny that nuclear missiles are not weapons due to the sheer destructiveness it can cause. But, how great must the damage or harm be after the use of a tool for it to be called a weapon? A tool merely causing inconvenience or an unpleasant state of affairs cannot be called a weapon. In that respect, the common law principle, *de minimis non curat lex* ("the Law does not concern itself with trifles") can also be used a satisfactory principle for conceptualizing weapons. Excluding trivial harms and damages makes the unnecessary securitization of cyber weapons less likely and avoids the unnecessary promotion of fear.

Second, it is easier to determine if a tool or instrument is a weapon if it causes direct - rather than indirect - harm or damage to a certain entity. If a weapon's effects are mostly indirect we have to know and separate the nature and consequences of the weapon from the intervening mechanisms. A person stabbing a knife into the victim's body is an archetypal example of a situation causing direct harm.

Third, it is easier to determine something is a weapon if it is expressly designed for the purpose of inflicting harm or damage. Numerous instruments - such as spears, guns and missiles - are specifically designed for harmful purposes. These single purpose objects are easier to define as weapons. Yet,

---

determining their actions, the question what would be considered their interest by an unprejudiced observer, is one of the least important parts of the whole manner […].What it is the man's interest to do or refrain from, depends less on any outward circumstances, than upon what sort of man he is. If you wish to know what is practically a man's interest, you must know the cast of his habitual feelings and thoughts. Everybody has two kinds of interests, interests which he cares for, and interests which he does not care for." John Stuart Mill, "Considerations on Representative Government", in John Robson (ed.), *Collected Works XIX*, , (Toronto: Routledge, Kegan and Paul: 1977), p.444.

[81] Feinberg, "*The Moral Limits of the Criminal Law Volume 1,"* p. 33

[82] Ibid, p. 33

many everyday objects can also be used to cause harm; one can think of a kitchen knife, bottle, hammer or saw. These tools are dual-use in nature; they can be used for both harmful and non-harmful purposes. Hence, in this case, it is more difficult to determine (in the abstract) if it concerns a weapon or not. For these instruments which are dual-use in nature, the aspect of *intend* is crucial.

The implications of the notion are important to consider. The total load of unexploded munitions of the total dropped on Germany during World War II is somewhere between five and fifteen percent, or between 95,000 tons and 285,000 tons.[83] The fact that some of these bombs did not explode does not mean that they are not weapons. After all, the key motivation behind the use of these bombs was to cause mass destruction. Devices which are intended to cause harm or damage but are unsuccessful in doing so are simply 'bad weapons', but not 'non-weapons'. In similar vein, an instrument that was used without the aim to cause harm or damage, even if it led to major havoc, is *not* a weapon.

2.2.2 The Qualificatory Level: the Prefix "Cyber-"

In order to address these questions with respect to 'cyber weapons' an assessment of the meaning of the prefix 'cyber-' is required.[84] A good starting point to grasp the meaning of the prefix 'cyber-' concerns the discussion on cyberspace in the literature. After all, as Kello states, cyberspace is "the most elemental concept in the cyber field as it establishes the technical markers within which the [cyber] weapon can operate."[85]

Yet, numerous articles provide a highly simplistic view of cyberspace, considering the concept to be synonymous to the 'information realm', 'non-physical dimension', 'internet' or 'virtual environment' - without elaborating much further on it.[86] That said, there is an increasing recognition that cyberspace

[83] Spiegel, "Routine Disposal Goes Wrong: Three Killed in Explosion of World War II Bomb in Germany", *Spiegel Online International*, (2 June, 2010), Retrieved from: http://www.spiegel.de/international/germany/routine-disposal-goes-wrong-three-killed-in-explosion-of-world-war-ii-bomb-in-germany-a-698245.html

[84] It is remarkable that many scholars only discuss the meaning of the term 'weapons' but fail to conceptualize the prefix '-cyber'. Rid and McBurney seem to consider it synonymous to 'computer codes'. The Tallinn Manual, in their framing of definitions seem to constantly shift the conceptual problematique. It states that "cyber weapons are cyber means of warfare that are by design, use, or intended use capable of causing either (i) injury to, or death of, persons; or (ii) damage to, or destruction of objects, that is, causing the consequences required for qualification of a cyber operation as an attack (Rule 30). " In turn, "Cyber means of warfare include any cyber device, materiel, instrument, mechanism, equipment, or software used, designed, or intended to be used to conduct a cyber attack (Rule 30)." It then states in the glossary (not mentioning it in the text) that cyber "[c]onnotes a relationship with information technology". Rid and McBurney, "Cyber-Weapons"; Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, (Cambridge: Cambridge University Press, 2013)

[85] Kello, "The Meaning of the Cyber Revolution", p. 17

[86] See for example: Ya-Wen Lei, "The Political Consequences of the Rise of the Internet: Political Beliefs and Practices of Chinese Netizens," *Political Communication*, 28:3 (2011) 291-322; Aim Sinpeng, "State Repression in Cyberspace: The Case of Thailand," *Asian Politics and Policy*, 5:3 (2013): 421-440; Barney Warf and John Grimes, "Counterhegemonic Discourses and the Internet," *Geographical Review*, 87:2 (1997) 259-274

should be conceptualized as a complex, multi-layered phenomenon with both physical and non-physical properties.[87] Hannes Ebert and Tim Maurer, for example, adopt the broad definition of the U.S. Cyberspace Policy Review which considers cyberspace to be both the "interdependent network of information technology infrastructures, [which] includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries" as well as the "virtual environment of information and interactions between people."[88] In similar vein, Sami Saydjari indicates that cyberspace "refers to both networked infrastructure (computers, routers, hubs, switches, and firewalls) and the information assets (critical data on which an organization depends to carry out its mission)."[89]

Perhaps the most sophisticated conceptualization of cyberspace concerns Martin Libicki's work "Cyberdeterrence and Cyberwar".[90] Libicki indicates that cyberspace consists of three separate but interconnected layers; i) the physical layer, ii) the syntactic layer, and iii) the semantic layer:[91]

> All information systems rest on a physical layer consisting of boxes [i.e. computer systems] and (sometimes) wires. Remove the physical layer, and the system disappears as well. […]The syntactic level contains the instructions that designers and users give the machine and the protocols through which machines interact with one another […] The topmost layer, the semantic layer, contains the information that the machine contains the reason computers exist in the first place.[92]

Libicki likens the layers of cyberspace to a party hall with private rooms, in that all these rooms "are part of the same physical structure and are mutually accessible, but that does not mean that what goes on in one room say much about what goes on in the next."[93] Adopting this definition indicates that

---

[87] See: Joseph S. Nye, Jr., "Cyber Power," *Belfer Center for Science and International Affairs*, (2010, May), retrieved from: http://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf; Gregory D. Koblentz and Brian M. Mazanec, "Viral Warfare: The Security Implications: of Cyber and Biological Weapons," *Comparative Strategy*, 32:5 (2013)418-434; Jones Robinson and Helge Janicke, "Cyber warfare: Issues and Challenges," *Computers & Security*, 49 (2015) 70-94

[88] Hannes Ebert and Tim Maurer, "Contested Cyberspace and Rising Powers," *Third World Quarterly*, 34:6 (2013): 1054-1074

[89] Sami Saydjari, "Defending Cyberspace," *Computer*, 35:12 (2002):125-127

[90] Martin Libicki, *Cyberdeterrence and Cyberwar*

[91] In an earlier publication, Libicki also discusses a fourth layer called 'pragmatics', viewed as the intentions that lie behind the speech acts. David Betz and Tim Stevens have subsequently used Libicki's model of cyberspace as their key conceptual framework to evaluate dominant cyber security analogies. See: David Betz and Tim Stevens, "Analogical Reasoning and Cyber Security," *Security Dialogue*, 44:2(2013):147-164. David Betz, "Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed," *Journal of Strategic Studies*, 35:5, (2012), 689-711, p. 691

[92] Also, according to Libicki, "[i]t turns out that hostile conquest in cyberspace takes place largely at the physical and syntactic layers, while friendly conquest in cyberspace, because it has to do more with the exchange and encoding of knowledge tends to take place at the syntactic and sematic layers." Libicki, *Cyberdeterrence and Cyberwar*, p. 12; Libicki, *Conquest in Cyberspace*

[93] Libicki, *Conquest in Cyberspace*, p. 9

cyberspace concerns all computer systems and their connections, receiving its *form* from the protocols set up and its *meaning* from the information it contains.

Robert Keohane writes that a definition "should be judged not only on the relevance of its categories but also on the power of the explanations that it suggests. An intuitive definition that makes clear and relevant distinctions is better than any definition that does not; but a clearly categorizing definition based on concepts that suggest valid explanations is best of all."[94] The definition adopted above directs us towards a number of powerful explanations of the role and attributes of cyber weapons.

First, Libicki's conception of cyberspace demands careful consideration of the ontology of cyber weapons. The fact that weapons are 'devices' implies a material ontology. The often-used analogical and metaphorical reasoning suggests that cyber weapons fit this ontological conception.[95] For example, Ralph Langer describes Stuxnet as a precision "military-grade cyber missile" that was used to launch an "all-out cyber strike against the Iranian nuclear program."[96] Yet, as cyber weapons largely consist of lines of code, they clearly have a non-physical dimension as well. In fact, Randall Dipert goes so far to state that, "cyberattack technology is more like an idea than like a physical thing."[97] Hence, as cyber weapons contain both physical and non-physical elements, it makes more sense to talk about cyber weapons as a *capability* rather than a *tool* or instrument.

Second, the definition also indicates that the common notion of cyberspace as a 'fifth domain' of warfare is unhelpful when it comes to understanding how cyber weapons can be used. In 2011, the U.S. military forces officially added cyber as the fifth domain of warfare following air, sea, land, and space as the traditional domains of military operations.[98] A number of countries have subsequently adopted a similar approach.[99] Yet, this conceptualization has numerous problems. First, *all* three

[94] Robert O. Keohane, "Review: Lilliputians' Dilemmas: Small States in International Politics," *International Organization*, 23:2(1969):291-310
[95] Betz and Stevens, "Analogical Reasoning and Cyber Security"
[96] Ralph Langer, "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve," The Langer Group, Retrieved from: ; Also quoted in: James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War", *Survival: Global Politics and Strategy*, 53:1 (2011):23-40;
[97] Randall Dipert, "The Ethics of Cyberwarfare," *Journal of Military Ethics*, 9:4 (2010):284-410; As Ryan Jenkins indicates, this raises numerous legal issues as to whether cyber weapons are therefore subject ot the same ethical constraints as conventional weapons. Ryan Jenkins, "Is Stuxnet Physical? Does it Matter?" *Journal of Military Ethics*, 12:1 (2013): 68-79
[98] Keith B. Alexander, "Warfighting in Cyberspace," *Joint Force Quarterly*, 46 (2007):58-61
[99] There are also various scholars arguing in favour of this. See for example: Paul Cornish, David Livingstone, Dave Clemente and Claire Yorke, "On Cyber Warfare," A *Chatham House Report*, (2010, November), p. viii; Isaac R. Porche III, Christopher Paul, Michael York, Chad C. Serena, Jerry M. Sollinger, Elliot Axelband, Endy Y. Min, Bruce J. Held, *Redefining Information Warfare Boundaries for an Army in a Wireless World*, (Santa Monica, CA: RAND: 2013)

layers of cyberspace are 'manmade' implying that it is not a given environment in which defence departments have to manoeuvre in the same way as their enemies.[100] Indeed, as Libicki argues in a more recent article, "the task in defending the network is not so much to manoeuvre better or apply more firepower in cyberspace but to change the particular features of one's own portion of cyberspace itself so that it is less tolerant of attack."[101] Second, as Rid indicates, cyberspace is unique in that the use of computer systems and networks permeates all other domains of military conflict; land, sea, air, and space.[102] It means that, as Rid continues to state, "an institutional division of labour is [...] far more difficult to implement, especially in a military context: the air force doesn't have tanks, the army has no frigates, but everybody has computer-run command-and-control networks."[103]

How do the four previously described propositions on weapons - harmfulness, directness, usability and intent - relate to cyber weapons? First, the degree to which cyber weapons are harmful or damaging is a much discussed topic going to the heart of the debate on the cyber revolution. Some hold the belief that a well-targeted cyber weapon could cause major havoc.[104] Due to the reliance of our social and economic infrastructure on computer networks, it is claimed that a cyber-attack can severely affect the functioning of (international) society. U.S. Defence Secretary Leon Panetta famously claimed that "a cyberattack perpetrated by nation states or violent extremists groups could be as destructive as the terrorist attack on 9/11. Such a destructive cyber-terrorist attack could virtually paralyze the nation."[105] Robert Knake and Richard Clarke also describe a particularly vivid scenario on how a cyber-attack causes a power blackout in metropolitan areas, the burning of oil-supplies, a freeze in the financial system, and the explosion of pipelines.[106] Others avow that the cyber

[100] As Libicki correctly notices: "[e]veryone concedes that cyberspace is man-made. This is what makes it different from its predecessors. Most then proceed as if the difference between a natural and a man-made combat medium is of no greater importance than the difference between natural and manmade fibres. But it is not the man-made nature of cyberspace that makes it different. Cities are man-made, but city combat shares many of the rules of country combat. What matters is that cyberspace is highly malleable by its owners, hence its defenders, in ways other media are not. Cities, although man-made, are not particularly malleable (at least not by those defending them)." Martin C. Libicki, "Cyberspace Is Not a Warfighting Domain," *I/S: A Journal of Law and Policy*, 8:2 (2012)321-336; p. 324
[101] Libicki, "Cyberspace is Not a Warfighting Domain"
[102] Thomas Rid, "What War in the Fifth Domain?," *Kings of War,* (2012, August) Retrieved from: http://kingsofwar.org.uk/2012/08/what-war-in-the-fifth-domain/
[103] Ibid
[104] See for example: Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*, (New York: Penguin Press: 2011); Mike McConnell, "Cyberwar is the New Atomic Age," *New Perspectives Quarterly,* 26:3 (2009):72-77; Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: Harpercollins: 2010);
[105]Leon E. Panetta, "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City, " *News Manuscript U.S Department of Defense*, (2012, October) Retrieved from: http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136.
[106] Clarke and Knake, *Cyber War*; Also see for example; Yoram Dinstein, "Computer Network Attacks and Self-Defense," *International Law Studies*, 76(2002):103.

threat has been severely exaggerated. The constructivist scholarship, adopting the framework from securitization theory, has in particular contributed to this argument.[107] Ralf Bendrath concludes in his study that "there is no link at all between the cyber-threat perception and the real world. Not directly as a 1:1 connection, and not even indirectly through the real interests of actors who try to use the discourse for their own purposes. Rather, the prefix 'cyber' gets attached to the mainstream security-policy discourse and works as an amplifier for any threat perception."[108] Yet, also a more positivist scholarship has criticized the 'doomsday thinking'. Thomas Rid, observing a striking absence of physical violence in the type of attacks that are conducted in cyberspace, concludes that events that have been habitually characterized as cyber warfare are, in fact, nothing of a kind. To date, no one has ever been (directly) killed by a cyber weapon. It also seems unlikely that it will be a brute force weapon in the future. In that sense, the effects caused by cyber weapons are mostly disruptive rather than destructive.[109]

Second, part of the reason why the cyber revolution is a bone of contention is due to the indirect path in which a cyber weapon potentially causes harm or damage. As Rid writes "the actual use of cyber force is to be a far more complex and mediated sequence of causes and consequences that ultimately result in violence and casualties."[110] In those Cassandra-esque scenarios in which a cyber weapon inflicts a lot of material damage or people suffer serious injuries or be killed, "the causal chain that links somebody pushing a button to somebody else being hurt is mediated, delayed, and permeated by chance and friction."[111] As it was stated in a report on the cyber attack against a German steel factory; there was an "accumulation of breakdowns of individual components of the control system or of entire facilities."[112] This in turn led to a malfunction in the heating system and disabled the

[107] Myriam Dunn Cavelty, *Cyber-Security and Threat Politics US Efforts to Secure in the Information Age* (Abingdon: Routledge: 2008); Ralf Bendrath, "The American cyber-angst and the real world - any link?" Paper presented at: International Studies Association Annual Convention, University of Bremen (2004) p. 72; Ralf Bendrath, "The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection," 7, *Information & Security,* (2001):80-103 Helen Nissenbaum, "Where Computer Security Meets National Security," *Ethics and Information Technology*, 7, 2(2005): 61-73; Rachel Yould, "Beyond the American Fortress: Understanding Homeland Security in the Information Age." In *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*, ed. Robert Latham. (The New Press, 2003); Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School"

[108] Ralf Bendrath, "The American Cyber-Angst and the Real World," in *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*, (ed.) Robert Latham (New York: The New Press: 2003).

[109] Daniel K. Rosenfield, "Rethinking Cyber War," *Critical Review: A Journal of Politics and Society*, 21:1(2009):77-90; Paulo Shakarian, "Stuxnet: Cyberwar Revolution in Military Affairs," *Small Wars Journal*, (2011); Collins and McCombie, "Stuxnet"

[110] Rid, *Cyber War Will Not Take Place*, p. 9

[111] Ibid, p. 9

[112] Thomas de Maizière, "Die Lage der IT-Sicherheit in Deutschland 2014," *Bundesamt für Sicherheit in der Informationstechnik*, (2014), retrieved from: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=pu

ability to shut down properly, resulting in significant physical damage to the operating system. Although there are still many unknowns about the cyber attack, based on the scenario, it is likely that other systems - such as the centralized controls, alarm systems, Safety Instrumented Systems (SIS), and Human Machine Interface (HMI) - were impacted as well.[113] Overall, cyber weapons are more likely to cause *mediated* destruction rather than *immediate* destruction.[114]

Third, on the mono-usability versus dual-usability of cyber weapons significantly less has been written.[115] Rid and McBurney suggest that cyber weapons are dual-purpose in use. Similar to a knife, they can be used for non-harmful purposes as well.[116] Yet, as Jon Lindsay correctly points out, there "are no general-purpose munitions that can simply be aimed and fired to destroy a complex industrial target at will."[117] To develop a well-targeted cyber weapon requires detailed intelligence on both the mechanical as well as the organizational dimension of a target to gain access to the computer network, exploit a specific system vulnerabilities, and activate a custom-engineered payload to sabotage it. In the case of Stuxnet, the developers had to take an incredible amount of technical particulars into consideration to penetrate deeply into Iran's industrial computer control system. Hence, as Trey Herr indicates, "the nature of software makes it nearly impossible to 'brandish' it, as you might a rock, textbook, or other object not designed as a weapon but quite capable of causing harm"[118] Generally speaking, as sophisticated cyber weapons have to be tailored toward the targeted computer system, it is a mono-purpose tool rather than a dual-purpose tool as Rid and McBurney purport it to be.[119]
Finally, the question of intent seems to be particularly important for cyber weapons. Like the unexploded bombs, a computer code developed to cause harm or damage but that did not work due a bug should still considered to be a weapon. And, the other way around as well; a cyber capacity that

blicationFile; Robert M. Lee, Michael J. Assante, and Tim Conway, "German Steel Mill Cyber Attack," *SANS Industrial Control Systems*, (2014, December 30), retrieved from: https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf

[113] Lee, Assante, and Conway, "German Steel Mill Cyber Attack"

[114] The discussion here should not be confused with Kello's distinction between direct and indirect effects. According to Kello, there are direct effects, "which unfold within the logical environment of the target machine complex"; and indirect effects "which hinder activity or functions that lie beyond the logical habitat of the compromised computer system but which rely on that system". Yet, the point here is that the effects caused by what, Kello calls 'direct effects' generally have a long causal chain. See Kello, "The Meaning of the Cyber Revolution," p. 20-21.

[115] Those articles which do provide useful insights generally discuss this issue in an indirect manner, as their key focus is on the replicability of cyber weapons.

[116] Rid and McBurney, "Cyber-Weapons"

[117] Lindsay, "Stuxnet and the Limits of Cyber Warfare," p. 378

[118] Herr and Rosenzweig, "Cyber Weapons and Export Control," p. 12

[119] Rid and McBurney, "Cyber-Weapons". Notice that this discussion is not about whether cyber weapons can be replicated or not. The argument made is not that the replication of cyber weapons is impossible. Instead, I assert that it is impossible for a cyber capacity, initially developed for non-harmful purposes, to directly and easily use it for purposes to cause harm or damage. That said, certain cyber capabilities can have elements which can be used for other purposes.

was never designed to cause damage but ended up doing so, is *not* a cyber weapon. The situation in which the effect of the computer code is misaligned with the intention is potentially more common than in conventional warfare. Although a missile could miss target and hit a different entity, it is difficult to imagine a scenario in which a missile intends to destroy a building but instead destroys a complete city.

Yet, historically it has frequently happened that there was a severe disjunction between the aim of a cyber attack and the actual outcome of the action.[120] When graduate student Robert Morris released one of the first computer worms distributed via the internet in 1988, he never intended to create an overall system downtime - leading computers to slow down to the point of being unusable.[121] The worm's purpose was to measure the size of the Internet but a critical bug in the spreading mechanism transformed it into a highly disruptive attack. Perhaps the prime example of this phenomenon are the so called, 'helpful' or 'friendly' worms, which are computer worm variants aiming to fix or halt the malicious actions of another worm. For example, in August 2003 the Blaster worm got 'in the wild' causing about $2 billion in damage.[122] The worm exploited a vulnerability twenty-six days after discovery of an exploitable Microsoft buffer overflow. It was categorized by Symantec as a dangerous computer virus known as a 'blended threat', combining characteristics of viruses, worms, Trojan horses, and other malicious code.[123] Soon after, the 'friendly' Welchia worm, also called 'Nachia', was developed.[124] Welchia looked for computers infected by the malicious Blaster worm, utilizes the same exploit, disinfects them and then tries to download and install a Windows security patch.[125] The

[120] This is especially the case for early malware. Another interesting case is Code Red Worm. As report from SANS demonstrates, the Code Red Worm "uses the same seed address by using the same IP addresses over and over again, therefore attacking the same systems over and over again." Sharon Bristow, "Code Red Worm Invasion," *SANS Institute* (2001) Retrieved from: https://www.sans.org/reading-room/?utm_source=web&utm_medium=text-ad&utm_content=generic_rr_pdf_logo1&utm_campaign=Reading_Room&ref=36909

[121] Bob Page, "A Report of the Internet Worm," (1988, November 7). Retrieved from: http://www.ee.ryerson.ca/~elf/hack/iworm.html ; Ted Eisenberg, David Gries, Juris Hartmanis, Don Holcomb, M. Stuart Lynn, Thomas Santoro, "The Cornell Commission: On Morris and the Worm," *Communications of the ACM*, 32:6, (1989), p. 706-709

[122] Symantec, "Internet Security Threat Report," (2003, September), Retrieved from: http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_iv.pdf, p. 1

[123] Symantec, "W32.Blaster.Worm," (2015) , Retrieved from: https://www.symantec.com/security_response/writeup.jsp?docid=2003-081113-0229-99 , p. 11; For definition of blended threat; Symantec, "Internet Security Threat Report,"

[124] As Kaspersky states, "Welchia belongs to the family of viruses that attack other malware, fighting for control of the system. The most famous worm of this group appeared in September 2001: the CodeBlue worm which scanned the Internet for machines infected by CodeRed worm and disinfected them." See: Kaspersky Lab, "Welchia - The Anti-Virus Virus?," (2003, August 19), Retrieved from: http://www.kaspersky.com/about/news/virus/2003/Welchia_The_Anti_Virus_Virus_ Other examples of 'helpful worms' include Cheeze, CodeGreen, and Mellenium.

[125] Kaspersky Lab, "Welchia"

'helpful' virus is said to have caused more harm than good, however, due to its general resource consumption and automated rebooting feature (without consent of the user). Similar problems occurred with other 'helpful' worms such as DenZuko (to remove Pakistani Brain in 1988), Cheese (to get rid of the LiOn worm in 2001), CodeGreen, and CRClean (both developed against the CodeRed worm in 2001).[126]

Cases such as the one described above are susceptible to the erroneous classification of a weapon whereas in reality they are not - as they were never intended or aimed to cause harm or damage. What about the cases which have a tendency to be classified as non-weapons but are in fact cyber weaponry? In other words, what about the 'unexploded bombs' in cyberspace? Shamoon is an interesting case in this respect, targeting the world's largest oil company Saudi Aramco in August of 2012 for which a group named "Cutting Sword of Justice" claimed responsibility.[127] The virus' payload was to erase files (the wiper component) and send the information about the files back to the attacker (the reporter component)[128]. According to Bill Trivitt, it caused "the destruction of 30,000 workstation[s] and forced Aramco to shut down its internal network for over a week." [129] As Kaspersky's Dmitry Tarakanov however discloses, Shamoon contained a number of significant coding errors. Not only had it a flawed date comparison, the author(s) of the code also failed to create a full path string - mistakenly put a lowercase 's' instead of an uppercase 'S' in the code- meaning that no file was able to be dropped. And with no file, there is no execution either so Shamoon does not have a functionality to execute other programs.[130]

Overall, cyber weapons can be defined as *a capability designed to access a computer system or network to damage or harm living or material entities.* The definition indicates that a cyber weapon is a *capability* and not a *tool* (with merely a material ontology). The *access* to computer systems and network (or 'its connections') denotes the interaction between the three levels - the physical layer, syntactic layer, and semantic layer. The fact that these weapons are purposefully *designed* signifies the importance of the aspect of intend. In addition, the aspect of *damage* and *harm* are both connected

[126] For early discussion on the advantages and disadvantages of helpful worms, see; Bryan Barber, "Cheese Worm: Pros and Cons of a Friendly Worm," *Sans Institute GSEC v1.2e*, (2001) retrieved from: https://www.sans.org/reading-room/whitepapers/malicious/cheese-worm-pros-cons-friendly-worm-31 .
[127] Lucian Constantin, "Kill timer found in Shamoon malware suggests possible connection to Saudi Aramco attack," Computerworld, (2012, August 23), retrieved from: http://www.computerworld.com/article/2491501/malware-vulnerabilities/kill-timer-found-in-shamoon-malware-suggests-possible-connection-to-saudi-ar.html
[128] The files are overwritten with corrupted jpeg files making it impossible for the victim to recover the files.
[129] Bill Trivitt, "The Evolution of APTs (Advanced Persistent Threats)," *Information System Security Association*, retrieved from: http://kern.issa.org/wp-content/uploads/2013/08/The-Evolution-of-APTsv1_2.pdf, p. 9
[130] Dmitry Tarakanov, "Shamoon The Wiper: further details (Part II)," *SecureList*, (2012, September 11), retrieved from: https://securelist.com/shamoon-the-wiper-further-details-part-ii/57784/

through the underlying notion of 'negatively affected interests', excluding trivial matters, but often caused in an indirect manner in cyberspace. Finally, the last part of the definition, on 'living and material entities', reveals that non-human entities can be affected as well.

2.2.3 The Secondary level: the Necessary and Sufficient Features of Cyber Weapons

Having laid out the basic definition of cyber weapons, the next step in the process of concept formation is to specify the multiple dimensions that ontologically embody the basic concept.[131] In deciding as to what is important about an entity, it is generally the level where most of the conceptual contestation takes place.[132] The key question to address at the secondary level is: what are the necessary and sufficient conditions for a capability to be called a cyber weapon?

Herbert Lin asserts that a successful cyber-attack requires three elements; i) a vulnerability, ii) access to the vulnerability (i.e. access vector), and iii) a payload to be executed (i.e. malicious code).[133] Lin offers a useful analogy to understand each of the three elements. In a non-cyber context, a vulnerability might be an easily pickable lock of a file cabinet. The access would be the available path for reaching the file cabinet - if the file cabinet is located in Fort Knox or on the moon it poses additional problems. And the payload would be the destructive action taken once the intruder has been able to open the file cabinet.[134]

Lin's framework has been adopted by other scholars with both positive and negative implications.[135] Trey Herr's application has usefully clarified that the three conditions for cyber-attacks can be successfully translated into 'cyber weapons', using a variety of examples. [136] Yet, his application has also proved to be confusing in that it has unnecessarily narrowed the application of the concept (only focusing on software vulnerabilities) and altered the order of conditions (putting propagation method

---

[131] Goertz, *Social Science Concepts*

[132] As Goertz averts, "[t]o develop a concept is more than providing a definition: it is deciding what is important about an entity." Ibid, p. 27

[133] Herbert S. Lin, "Escalation Dynamics and Conflict Termination in Cyberspace," *Strategic Studies Quarterly*, 6:3 (2012)46-70; Lin, "Offensive Cyber Operations and the Use of Force,"; Owens, Dam, and Lin, "*Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*"

[134] Lin, "Escalation Dynamics and Conflict Termination in Cyberspace," p. 47

[135] Lindsay has used this framework in its analysis on the Stuxnet attack, showing that framework is excellent for analytical use. Lindsay, "Stuxnet and the Limits of Cyber Warfare".

[136] Lin's discussion on the elements of a cyber-attack can easily be adopted to lay out the necessary and sufficient conditions of a cyber weapon. Trey Herr has attempted to do this in what he called the "PreP-framework". A Propagation Method (Pr) is "the means by which malware is inserted into a target network or system"; an Exploit (E) is the "code designed to compromise some aspect of a software system which allows third parties to effect unintended operations or consequences." A Payload (P) is "the code with a malicious purpose whose delivery and execution are the goals of any piece of malware." See: Trey Herr, "PrEP: A Framework for Malware & Cyber Weapons," *The Journal of Information Warfare*, 13:1 (2014)1-28, p.2

before exploit).[137] It is for this reason that this study follows Lin's original terminology - but logically takes Herr's insights into consideration.

First, in most basic terms, a *vulnerability* concerns a specific problem in a computer system that can be used by the attacker to compromise one of the three layers of cyberspace.[138] As Lin notes, weaknesses may be accidentally introduced (a 'bug') - through a design or implementation flaw - or intentionally. Unintentional defects - in both hardware and software - that have been exploited by an attacker where there is no prior knowledge of the flaw in the general information security community are called zero-day vulnerabilities.[139] There is almost no defence against zero-day attacks as (in the case of software vulnerabilities) the anti-virus products cannot detect the attack through signature-based scanning.[140] On average, about one of a million pieces of malware that antivirus researchers discovered each year use a zero-day exploit.[141] Leyla Bilge and Tudor Dumitras, using data from Symantec, developed a technique for identifying and analysing zero-day attacks from the data available through the Worldwide Intelligence Network Environment (WINE).[142] Its findings are that the detection of zero-day attacks last between 19 days and 30 months, with an average of approximately 10 months and a median of 8 months.[143]

Second, the *attack vector* of a cyber weapon refers to the route used by the attacker to get into the computer system. There is a great variety in types of access to targets. At one end of the spectrum, there are certain targets to which access can be gained relatively easily - such as targets known to be connected to the internet. Indeed, public websites are the low-hanging fruit in this respect as they generally run on generic server software and are connected to the Internet; even relatively unskilled individuals can launch a website defacement attack.[144] At the other end of the spectrum, there are

[137] Ibid
[138] After all, as Libicki notes, "[t]here is no forced entry into cyberspace". There is no forced entry into cyberspace. Libicki, *Conquest in Cyberspace*, p. 31
[139] Owens, Dam, and Lin, "*Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*"
[140] Signature based scanning most common method that antivirus software uses to identify malware. It is when a malicious file is identified, a signature is written to ensure that anti-malware programs are able to detect (a component of) the file in the future.
[141] Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," *Wired*, (2011, November 7) retrieved from: http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/
[142] World Leyla Bilge and Tudor Dumitras, "Before We Knew It An Empirical Study of Zero-Day Attacks In The Real World," CCS '12 Proceedings of the 2012 ACM conference on Computer and communications security (2012) 833-844; WINE is a platform for data intensive experiments in cyber security. It includes field data collected by Symantec on 11 million hosts around the world.
[143] Ibid
[144] As is stated in the Internet Security Threat Report 2014; "[c]ompromising a legitimate website may seem to be a challenge for many, but vulnerability scans of public websites carried out in 2013 by Symantec's Website Security Solutions division found that 77 percent of sites contained vulnerabilities." See: Symantec Corporation, "Internet Security Threat Report 2014," (2014), retrieved from: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf, p. 2.

certain targets which are very difficult to access. If an adversary aims to target air-gapped systems, not running on a commercial operating system, it would have great difficulty in getting access to it.

Finally, the *payload* concerns the part of the weapon designed to execute on a computer system or network and achieve some predefined, malicious goal. As Herr and Rosenzweig point out, the payload is the "raison d' être" of a cyber weapon.[145] Payloads can be programmed to do more than one thing when inserted into an adversary computer system or network. A cyber weapon can deliver multiple payloads and the timing of these actions can be varied. Also, as Lin states, if a communications channel to the attacker is available, payloads can be remotely updated.[146] In fact, in some cases, the initial delivered payload consists of nothing more than a mechanism for scanning the system to determine its technical characteristics and an update mechanism to retrieve from the attacker the best packages to further its attack.

In making the argument that the payload is an essential component of a cyber weapon, I fundamentally disagree with Rid and McBurney's understanding of a cyber weapon.[147] Rid and McBurney claim that a "psychological dimension" also comes into play "if a weapon is used as a threat, or if its use is announced or anticipated: the target's perception of the weapon's potential to actually harm."[148] Rid and McBurney use a fictional example of a robber entering a bank with a paintball pistol. They contend that the paintball pistol is a weapon if the clerk believes it is a loaded with live bullets; it is not a weapon if the clerk realizes it is a fake gun.[149] One can only argue that a paintball gun (or a cyber-capability without a payload) becomes a weapon, without its properties having changed, if the term 'weapon' is defined in an overly-broad manner - that is, as any tool that can be used to persuade another person. Yet, if the definition of a weapon is contingent upon such an inclusive concept of influence, it becomes very difficult in practice to determine what cyber weapons are not. Instead, in line with the definition used in this study, to avoid vague definitions, only capacities with a payload that leads to harm or damage are cyber weapons.[150]

[145] Herr and Rosenzweig, "Cyber Weapons and Export Control," p. 8
[146] Lin, "Offensive Cyber Operations and the Use of Force," p. 67
[147] Rid and McBurney, "Cyber-weapons"; As cyberspace is both material and immaterial, I also disagree with their conception that a cyber weapon is a 'tool'.
[148] Ibid, p. 7
[149] Ibid, p. 8
[150] In that sense, I follow both Herr and Rosenzweig in concluding that the "the distinction between cyber weaponry and non-weapon malicious software lies in the payload component of the tool, which must be capable of creating destructive digital or physical effects, but that the other components are essential aspects of the weapon that have a dual-use nature (that is, they equally have commercial, non-military uses)." See: Herr and Rosenzweig, "Cyber Weapons and Export Control," p. 88

2.2.4 The Indicator Level

The base and secondary level of concepts lay out the aspects which *all* cyber weapons have in common. Instead, the indicator level serves to understand along which dimensions cyber weapons *differ*. As most indicators are substitutable —that is, they need not all be present together to indicate the presence of secondary level concepts—they provide a "natural way to incorporate [the] historical [and technical] diversity [of cyber weapons] into a larger theoretical framework."[151] The indicator level also serves to specify the empirical aspects which serve to signify the presence of the concept itself.

There are a variety of ways one can separate the three components of cyber weapons into 'indicators'. In line with the purposes of this study, I split up the components based on the way in which different weapons are potentially more or less sophisticated.

First, the vulnerability a cyber weapon exploits can be divided into three indicators. One can distinguish between hardware, software and network infrastructure and protocol vulnerabilities.[152] This study is not the appropriate place to explain each vulnerability in detail, so I offer only a telegraphic summary. First, a *hardware*-based cyber weapon alters the physical elements that comprise a computer system and/or network. The key source of hardware-based cyber weapons is derived from the unauthentic or illegal clones of hardware which can be found on the Internet Technology (IT) market.[153]

For years, Moore's Law has predicted the success of the semiconductor integrated circuit (IC or chip) manufacturing business: the idea that a new chip can be produced, which has twice as many transistors as a similar IC made less than two years prior.[154] In this rapidly changing technological and competitive environment - in which companies must constantly update their tools to support the new technology - companies outsource much of their manufacturing to offshore facilities known as foundries in an attempt to lower their production costs.[155] Today, only a few companies still have

[151] Goertz, "Social Science Concepts," p. 65.
[152] Julian Jang-Jaccard and Surya Nepal, "A Survey of Emerging Threats in Cybersecurity," *Journal of Computer and System Sciences*, 80:5 (2014)973-993
[153] Ramesh Karri, Jeyavijayan Rajendran, Kurt Rosenfeld, Mark Tehranipoor, "Trustworthy hardware: Identifying and classifying hardware Trojans," *Computer*, 43:10(2010)39-46; Also, as the authors indicate, IT companies often buy untrusted hardware such as chipsets and routers from online auction sites or resellers which in turn may contain harmful hardware-based Trojans.
[154] Gordon E. Moore, "Cramming More Components onto Integrated Circuits," *Electronics Magazine*, 38:8(1965); Gordon E. Moore, "Lithography and the Future of Moore's Law," *Proceedings of SPIE*, 24:37(1995).
[155] As Adee indicates, semiconductor offshoring dates back to the 1960s, when U.S. chip makers began moving the labour intensive assembly and testing stages to Singapore, Taiwan, and other countries with educated workforces and

their own fabrication plants to produce all their chips.[156] Outsourcing the design and manufacture to foundries in the foreign countries, however, inherently affects the evidence for the integrity of the manufactured product. After all, it requires relatively little effort for a skilled person/group with access to the production process to slightly alter the final product.

The threat is potentially significant considering the number of chips put into modern military equipment. For example, an aircraft like the next generation F-35 Joint Strike Fighter (JSF), potentially contains several thousand chips.[157] Hardware vulnerabilities, according to Sally Adee, generally fall into two categories: a backdoor and a kill switch.[158] A kill switch concerns any manipulation of the chip that would lead to die outright.[159] This could for example be used to shut off a JSF's missile-launching electronics. A backdoor, instead, gives a person unauthorized access to the system to disable or enable a certain function. As this method works without shutting down the whole chip, users often remain unaware of the intrusion. Using this method an adversary could for instance use it to bypass battlefield radio encryption.[160]

A *software*-based cyber weapon exploits a certain weakness/defect in the code of a computer program.[161] Currently, most cyber weapons utilize vulnerabilities in application or system software. Most common software vulnerabilities happen as a result of exploiting software bugs in the memory, user input validation, race conditions and user access privileges.[162] First, memory safety violations are performed by attackers to modify the contents of a memory location. Most exemplary technique is buffer overflow which occurs when a program tries to store more data in a buffer (i.e. memory location) than it was intended to hold. Since buffers are created to contain a finite amount of data, the

relatively inexpensive labour. Sally Adee, "The Hunt for the Kill Switch," *IEEE Spectrum*, (2008) Retrieved from: http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch

[156] David A. Hodges and Robert C. Leachman, "Outsourcing and Offshoring in the Semiconductor Industry," Sloan Industry Centers Annual Conference Atlanta, GA (2004)

[157] There was controversy on potential backdoor found in Chinese chips found by Sergei Skorobogatov. Sergei Skorobogatov and Christopher Woods, "Breakthrough silicon scanning discovers backdoor in military chip," Cryptographic Hardware and Embedded Systems Workshop, 9-12 September 2012,(Leuven), retrieved from: https://www.cl.cam.ac.uk/~sps32/ches2012-backdoor.pdf

[158] Adee, "The Hunt for the Kill Switch,"

[159] Ibid

[160] Ibid; also see: Gedare Bloom, Eugen Leontie, Bhagirath Narahari, and Rahul Simha, "Chapter 12: Hardware and Security: Vulnerabilities and Solutions" in Sajal K Das, Krishna Kant, Nan Zhang (eds.), *Handbook on Securing Cyber-Physical Critical Infrastructure: Foundations and Challenges*, (Elsevier: 2012), p.306; the scholars indicate that IC fabrication concerns originate from the military sector, with US Defence Advanced Research Projects Agency (DARPA) issuing a issuing a Broad Agency Announcement (BAA) in 2006, and again in 2007, requesting proposals for the trust in Integrated Circuits

[161] Definition partially adopted from: Jaziar Radianti and Jose. J. Gonzalez, "Understanding Hidden Information Security Threats: The Vulnerability Black Market," Proceedings of the 40th Hawaii International Conference on System Sciences (2007)

[162] Katrina Tsipenyuk, Brian Chess, Gary McGraw, "Seven pernicious kingdoms: A taxonomy of software security errors," *Security and Privacy*, 3:6 (2005)81-84

additional information can overrun the original location's boundary and overflow into adjacent physical memory storage locations, overwriting or corrupting the data originally contained in them. It allows attackers to interfere into existing process code. Second, input validation is the process (or routine) of ensuring that the input data follows certain rules.[163] Incorrect data validation can lead to data corruption such as seen in Structured Query Language (SQL) injection, often used to exploit a program bug in a website's software.[164] An attacker injects SQL commands from the web form either to alter the database content or dump the database contents - like credit card details or passwords - to the attacker. Third, race condition error or race hazard exploits a flaw in a process where the output of the "process is unexpectedly and critically dependent on the timing or sequence of other events."[165] Fourth, privilege confusion or privilege escalation occurs when a bug is exploited providing elevated access to resources that are normally protected from an application or user.[166] The result is that adversaries with more privileges perform unauthorized actions such as accessing protected secret keys.

As numerous studies point out, with the growth of cyberspace, the number of software vulnerabilities has inherently increased as well. Whereas in 1996 only 70.9 million computers were sold on the global PC market,[167] in 2015 this number has exponentially increased to 315.9 million - not taking into consideration any other new information technology devices.[168] Not only are there now many more computer devices, they have also become increasingly complex in recent years leading to a higher potential for bugs in the code.[169] For example, consider the different versions of Microsoft

[163] Allen Jones, Adam Freeman, Matthew MacDonald, Rakesh Rajan, *Visual C# 2010 Recipes: A Problem-Solution Approach*, (New York: Apres: 2010)

[164] For a more technical overview of SQL injection: Nana Yaw Asabere and Wisdom Kwawu Torgby, "Structured Query Language Injection (SQLI) Attacks: Detection and Prevention Techniques in Web Application Technologies*," International Journal of Computer Applications*, 71:11 (2013) 29-39

[165] Mary Lovelace, Jichan Chong, Marcos Figueiredo Jr, Curtis Neal, Gabor Penzes, Naren Rajasingam, Joe Roa, Alexander Saupp, John Sing, Shradha Nayak Thakare, Mladen Vukoje, "Chapter 6: Networking considerations," in *IBM Redbook: SONAS Concepts, Architecture, and Planning Guide*, retrieved from: http://www.redbooks.ibm.com/redbooks/SG247963/wwhelp/wwhimpl/js/html/wwhelp.htm, p. 202; also see: Antoon Rufi "Chapter 1: Vulnerabilities, Threats, and Attacks" in *Network Security 1 and 2 Companion Guide* (ed.) Antoon Rufi, (Cisco Networking Academy: 2006)

[166] Johannes Horm, "Exploit CVE-2015-0274," Unpublished Manuscript, (2015) Retrieved from: http://kodu.ut.ee/~mroos/turve/2015/referaadid/CVE-2015-0274_Johannes_Horm.pdf

[167] Jeffrey van Camp, "HP Wants to Sell its PC Business, Kill Webos: so What Happens Now?," Digital Trends, (August, 2011) Retrieved from: http://www.digitaltrends.com/mobile/hp-wants-to-sell-its-pc-business-kill-webos-so-what-happens-now/

[168] Gartner, "Gartner Says Worldwide PC Shipments Grew 1 Percent in Fourth Quarter of 2014," (2015, January), Retrieved from: http://www.gartner.com/newsroom/id/2960125

[169] The software market is sometimes compared to the economic principle of a 'market for lemons'. Buyers are generally unable to distinguish between secure and insecure products in the software market. This means vendors have little incentive to develop a security technology that is as sound as possible. As buyers take this economic dynamic into consideration, software product of superior quality will be driven out of the market. See: Ross Anderson, "*Why Information Security Is Hard, an Economic Perspective*," Proceedings of 17th Annual Computer Security Applications Conference (2001)

Windows operating system. The Windows NT 3.0 operating system released in July 1993 had 4-5 million *source lines of code* (*SLOC*) with an estimated development costs of $10 billion.[170] Windows '98 had already 29 million SLOC with the development costs having more than tripled as well.[171] The 2012 released version Windows 8 has a staggering 80 million SLOC.[172] More than 3000 developers have worked on this version with an estimated development costs of $83 billion and an estimated maintenance costs of $192 billion. With the enormous increase in the lines of code of computer programs, the number of vulnerabilities has inherently increased as well.[173]

A *network infrastructure and protocol*- based cyber weapon concerns a capability which exploit vulnerabilities in the network infrastructure and protocols. A network protocol is a set of rules and conventions that governs the communication between network devices.[174] After all, in order for two computers to talk to each other, they basically must be speaking the same 'language.'[175] There are a variety of layers of network protocols. The most frequent network attacks occur by exploiting the limitations of the commonly used network protocols such as Internet Protocol (IP), Transmission Control Protocol (TCP) or Domain Name System (DNS).[176]

The IP is the main communication protocol of the network layer providing the information needed for routing packets among routers and computers of the network - essentially establishing the internet. The original IP protocol, introduced by Vincent Cerf and Bob Kahn in 1974, did not have any general-purpose mechanism to validate the authenticity and privacy of data being transmitted.[177] This allowed the data subject to being intercepted or changed while they are transmitted over unknown network between two devices.[178] To prevent this problem, IPSec was developed providing encryption of IP

[170] Edward E. Ogheneovo, "On the Relationship between Software Complexity and Maintenance Costs. Journal of Computer and Communications," *Journal of Computer and Communications*, 2 (2014)1-16
[171] Ibid
[172] Ibid
[173] Windows 2000 operating systems, has an estimated 63,000 bugs in the software when it was first released.
[174] As Song, Cadar, and Pietzuch write, "The messages exchanged by these entities are called packets, and a sequence of packets is referred to as a packet stream. When a network protocol is designed, all the information regarding methods, behaviour and packet formats are described in documents, which form the protocol specification, to be referenced by developers of a protocol implementation." See JaeSeung Song, Cristian Cadar, and Peter Pietzuch, "SYMBEXNET: Testing Network Protocol Implementations with Symbolic Execution and Rule-Based Specifications" *IEEEE Transactions on Software Engineering*, 40:7 (2013)695-709
[175] Others consider more layers of networking protocols – consider, for example, the Open Systems Interconnection (OSI) Reference Model which defines seven layers of networking protocols. The complexity of these layers, however, is beyond the scope of this study. Florida Center for Instructional Technology "Chapter 2: What is a Protocol?" (2013), Retrieved from: http://fcit.usf.edu/network/chap2/chap2.htm
[176] Jang-Jaccard and Nepal, "A survey of emerging threats in cybersecurity"
[177] Barry M. Leiner, Vinton G. Cerf,David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff, " A Brief History of the Internet, " *ACM SIGCOMM Computer Communication Review*, 39:5 (2009)22-31
[178] Ibid

traffic and user data. For many years, as Jang-Jaccard and Nepal indicate, IPSec has been used as one of the main technology for the creation of a virtual private network (VPN) which creates a secure channel across the internet between a remote computer and a trusted network" (it basically extends a private network across a public network).[179] TCP sits on top of the IP to transmit the packets running on hosts communicating over an IP network in reliable and ordered delivery of the packets. Major internet applications such as the World Wide Web, email, file transfer and remote administration all rely on TCP as the protocol.[180]

DNS is the protocol that translates domain names into IP addresses which can easily be remembered by humans. It is the internet's primary directory services signalling routers to which IP address to direct packets when the user gives a certain URL. There are two major concerns when it comes to the vulnerability of DNS. First, because DNS responses are not authenticated, an attacker may be able to send malicious DNS messages to impersonate an Internet server. The second related problem is about the availability of DNS. As DoS attacks have frequently shown, a successful attack against a DNS service can create a significant disruption in communications.[181]

Second, it is common to broadly distinguish between two types of *access paths*. There are *remote-access* system attacks, in which the cyber weapon employed launches an attack at some distance from the adversary computer or network of interest. The canonical example of a remote access attack is that of an adversary computer attacked through the access path provided by the Internet. As Lin writes, other examples might include accessing an adversary computer through a dialup modem attached to it or through penetration of the wireless network to which it is connected and then proceeding to destroy data on it.[182] There are also *closed-access* system attacks in which, as Kello writes, the cyber weapon employed launches an attack against a computer system "not interdependent at logical or information layers."[183] In this case, the cyber weapon accesses an adversary computer or network through the local installation of hardware or software functionality by friendly parties (this could either be vendors or covert agents) in close proximity to the computer or network of interest. It can also happen through exploiting the ignorant human element. Buckshot Yankee in 2008,

[179] Jang-Jaccard and Nepal, "A survey of emerging threats in cybersecurity"
[180] Ibid
[181] Also see chapter 4.
[182] Owens, Dam, and Lin, "*Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*," p 87
[183] Lucas Kello, "Cyber Disorders: Rivalry and Conflict in a Global Information Age," Presentation, International Security Program Seminar Series, Cambridge, Mass. International Security Program, Belfer Center for Science and International Affairs, Harvard Kennedy School (2012, May), Retrieved from: http://www.belfercenter.org/publication/cyber-disorders-rivalry-and-conflict-global-information-age; p. 16

considered to be the most significant breach of U.S. military computers, is a good case in point.[184] There are two main stories as to how this was able to happen. One is that infected USB flash drive was left on the parking lot of DoD facility in the Middle East - which a soldier, official or contractor picked up and ignorantly inserted in his/her laptop.[185] Another version of the story that someone went to an Internet café inserted a USB flash drive in a machine infected by the worm and subsequently inserted the USB in a classified computer of the DoD.[186] In any case, in both versions of the story, the 'weakest link' was exploited.

Third, the *payload* of a cyber weapon can vary widely in sophistication and potential to do harm. Herr distinguishes between six types of payloads - without much elaboration:[187]

1. Espionage: to steal user or system data
2. Resource exhaustion: consume computing resources on a target system
3. Misinformation: alter data without a target user's knowledge efforts.
4. Obfuscation: hide payload from intrusion detection and other defence information security
5. Command and Control: communicate out from an infected system and possibly retrieve new payload modules
6. Persistence: Allow access to a target system if the initial infection is detected or removed.

I maintain that the only *two* payloads of cyber weapons, described in Herr's list, are *resource exhaustion* and *misinformation*. If the raison d'être of a cyber-capability is to steal user or system information, it does not conform the basic definition of a 'weapon' as it does not (intend to) cause harm or damage to human beings, organizations, or systems. Obfuscation, command and control, and persistence are merely components which enable a harmful payload to be employed instead of key indicators of a cyber weapon.[188]

The main resource overloading attacks are Denial-of-Service (DoS) and Distributed-Denial-of-Service (DDoS) attacks, consisting of an overwhelming quantity of packets being sent from multiple

[184] The worm that was inserted was called "Agent.btz" which had the ability to send data from DoD computers to a remote command and control server through opened backdoors. Noah Schachtman, "Insiders Doubt 2008 Pentago Hack Was Foreign Spy Attack," *Wired*, (2010, August 25), retrieved from: https://www.wired.com/2010/08/insiders-doubt-2008-pentagon-hack-was-foreign-spy-attack/
[185] Alexander Gostev, "Agent.btz: a Source of Inspiration?" *Securelist*, (2014, March 12), Retrieved from: https://securelist.com/blog/virus-watch/58551/agent-btz-a-source-of-inspiration/
[186] Ellen Nakashima, "Cyber-intruder sparks response, debate," *The Washington Post*, (2011, December 8) , Retrieved from: https://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html
[187] Trey Herr, "PreP A Framework for Malware and Cyber Weapons", see table 2
[188] I do not claim that a payload free cyber capability cannot potentially cause harm or damage. Yet, the point is that it is difficult to conceive of a cyber capacity, intended to cause harm or damage, which does not have payload.

attack sites to a victim site.[189] The goal of the attacker in these kind of attacks is to tie up a certain key resource at the victim, usually by sending a high volume of seemingly legitimate traffic requesting some service from the victim.[190] The overconsumption of the resource leads to degradation or denial of the victim's service to its legitimate clients.[191] The main difference between DoS and DDoS attacks is in scale — DoS attacks use one attack machine to generate malicious traffic, while DDoS attacks use large numbers of attack machines.[192] DDoS attacks occur on a daily basis. Yet, the DDoS attacks against Estonia in 2007 and Georgia in 2009 have received the most widespread attention; both of which were allegedly conducted by Russian state-sponsored proxies and were strong enough to degrade important services, including the financial sector. Other politically motivated DDoS attacks concern the attack on the Kyrgi government in January 2009 - around a time of tension on the future of an American air force base in Manas - and the July 2009 attacks - directed at the websites of government, financial and news organizations in both South Korea and the United States.[193]

Data alteration can cause significant damage to a targeted computer system (i.e. sabotage) - of which Wiper is a typical example. Although redundancy systems and backups are normally created to ensure that data that's altered for any reason can be restored, changing records can lead to severe financial losses.

2.3 Conclusion

The purpose of this chapter was to offer a conceptual understanding of cyber weapons in order to provide a benchmark for the analysis of the capability's proliferation in the international system. The study's extension of Goertz three-level framework to a four-level framework allows for an enhanced understanding of cyber weapons as a multilevel and multidimensional concept. I argued that cyber weapons should be viewed as a type of weapon; it concerns a capability designed to access a computer system or network to damage or harm living or material entities. It has three necessary and sufficient

[189] Alefiya Hussain, John Heidemann, Christos Papadopoulos, "A framework for classifying denial of service attacks," Proceedings of the SIGCOMM 2003 conference on Applications, technologies, architectures, and protocols for computer communications, p. 99-110

[190] Jelena Mirkovic, D-WARD: Source-End Defense Against Distributed Denial-of-Service Attacks, *PhD Manuscript*, retrieved from: http://ieeexplore.ieee.org/abstract/document/1510618/?reload=true ; Sílvia Farraposo, Laurent Gallon, Philippe Owezarski, "Network Security and DoS Attacks" Unpublished Manuscript, (2005)

[191] Ibid

[192] The scale difference also invokes differences in operation modes. The large number of attack machines allows DDoS perpetrators a certain recklessness — they frequently trade sophistication for brute force, using simple attack strategies and packet contents to overload victim resources.

[193] Symantec Security Response, "Born on the 4th of July," *Symantec Official Blog*, (2009, July 9), retrieved from: https://www.symantec.com/connect/blogs/born-4th-july ; John Sudworth, "New 'cyber attacks' hit S Korea," *BBC News*, (2009, July 9), Retrieved from: http://news.bbc.co.uk/1/hi/world/asia-pacific/8142282.stm

components; a vulnerability, access vector and payload. These components can in turn be separated into various ‘indicators’.

This study however has revealed that to empirically distinguish between a cyber weapon and a more general cyber capacity is not easy. The usage of a cyber weapon generally leads to limited harm or damage through a mediated sequence of causes. There is also often a mismatch between the intended effect of a cyber-attack and the actual harm or damage caused. Chapter 4 nevertheless attempts to take up the difficult task of identifying which cyber weapons have been used over the past decades. This exercise is part of a more general analysis to understand the exact requirements of cyber weapon development.

Chapter 3: A Survey of the Cyber Proliferation Landscape: The Past and Present

3.1 Introduction

Judging from statements of some experts and policy makers, the world is at the brink of 'mass cyber proliferation'. In May 2017, Richard Ledgett, former deputy director of the NSA, told an audience at Georgetown Law School's annual Cybersecurity Law Institute that "well over 100" countries around the world are now capable of launching cyber attacks.[194] A decade earlier, McAfee approximated in their 2007 report that 120 countries have been developing ways to use "the internet as a weapon."[195]

Others are more conservative in their estimates. In early 2017, James Clapper, Director of National Intelligence, and Adm. Michael Rogers, Director of the NSA and U.S. Cyber Command, said in a Joint Statement in front of U.S. Congress that "[a]s of late 2016 more than 30 nations are developing offensive cyber attack capabilities."[196] Paul Nicholas, Senior Director of Global Security Strategy and Diplomacy at Microsoft, follows this analysis in a recent keynote at the International Conference on Cyber Conflict (CyCon) in June 2017.[197] Similarly, in 2015, Kim Zetter reported that "[i]n recent years, more than 20 countries have announced their intent to launch or beef up their offensive cyber capabilities."[198]

These widely diverging views illustrate how little is still known about cyber proliferation. The contrast with nuclear proliferation is stark. Since WWII there has been uncertainty about the nuclear progress of *certain* countries. Indeed, lively debates took place about how far away countries - like Libya or Israel - were from developing the bomb. Yet, the lack of consensus in the case of cyber proliferation is of much greater magnitude: are we talking about a handful of states or about almost all states in the world developing these capabilities?

---

[194] Mike Levine, "Russia tops list of 100 countries that could launch cyberattacks on US"
[195] Cited in: Peter Griffiths, "World faces "cyber cold war" threat"
[196] This does not mean they are less concerned about the cyber threat. The two senior officials continue to state that: "The proliferation of cyber capabilities coupled with new warfighting technologies will increase the incidence of standoff and remote operations, especially in the initial phases of conflict." James R. Clapper, Marcel Lettre, and Michael S. Rogers, "Joint Statement for the Record to the Senate Armed Services Committee Foreign Cyber Threats to the United States," (2017, January 5), Retrieved from: http://www.globalsecurity.org/intell/library/congress/2017_hr/160105_clapper-lettre-rogers_sasc.pdf
[197] Paul Nicholas, "Keynote on Defending the Core," 9th *International Conference on Cyber Conflict*, Tallinn, Estonia (2017, May 30- June 2)
[198] Kim Zetter, "We're at Cyberwar: A global Guide to Nation-state Digital attacks," *Wired*, (2015, September 1), retrieved from: https://www.wired.com/2015/09/cyberwar-global-guide-nation-state-digital-attacks/

Hence, an investigation into *why* states develop cyber weapons should consider the question: w*hat* is the current landscape of cyber proliferation? The purpose of this chapter is to reduce the level of uncertainty about which states currently (seek to) have cyber weapons.[199] Conducting this exercise provides an empirical basis for later chapters to render theoretical explanations of states' behaviour.

Even though the level of secrecy makes it more difficult to obtain an historical overview of cyber proliferation, it is *not* the main cause of these widely ranging estimates. As the above statements reveal, two senior officials (Adm. Michael Rogers and Richard Ledgett) of the *same* intelligence agency provide two vastly different estimates of cyber proliferation. Instead, what is more likely to be the root cause is conceptual ambiguity - concepts like 'developing' or 'offensive' are generally left undefined - as well as the lack of transparency of used methodology.[200]

The remainder of this chapter is outlined as follows. Section 3.2 provides an historical overview of states *exploring, pursuing, and acquiring* cyber weapons. The main argument which comes to fore from this section is that cyber proliferation - at all stages - is more limited than some have suggested.

But, the manner in which states proliferate may differ significantly - something the basic overview of section 3.2 does not capture. In section 3.3 I therefore assess the variation in cyber proliferation, along the following three levels: sophistication, reliance on proxy actors, and organizational structure and investment. Addressing each dimension provides several valuable insights. It shows that the most advanced cyber powers - China, Russia, and the U.S. - follow distinct approaches in their conduct of offensive cyber operations. Also, I note that factors other than 'plausible deniability' potentially provide a better explanation for the use of cyber proxies by states. Finally, although some states do pour a large amount of resources into the development of offensive cyber capabilities, for many others, the command has only limited means to conduct offensive cyber operations. In fact, it seems that for some states the military cyber command (or equivalent organization) is nothing more than an empty-shell; it exists on paper but no substantial activity takes place.

Surveying the cyber proliferation landscape leaves us with a final question to consider: does it matter *when* a state proliferates? In order to answer this question, in section 3.4 I assess the 'order of entry' effects of cyber proliferation. I argue that these effects are especially beneficial to latecomers (and not early movers) when it comes to cyber proliferation.

[199] I can merely 'reduce' - not mitigate - the amount of uncertainty surrounding cyber proliferation.
[200] Most estimates do not follow from academic studies.

3.2 Exploration, Pursuit and Acquisition of Cyber Weapons

I distinguish between four stages of cyber proliferation. The first stage of 'no discernible activity' is when there is no evidence that a state is contemplating developing cyber weapons. Second, a state is said to 'explore' cyber weapons when senior officials have provided public or private authorization to look into the development of cyber weapons.[201] Third, a state is considered to 'pursue' cyber weapons when it has formally established an organization to develop these types of offensive cyber capabilities. Once a state is known to have these capabilities, it is said to 'acquire' cyber weapons and has reached the final stage.

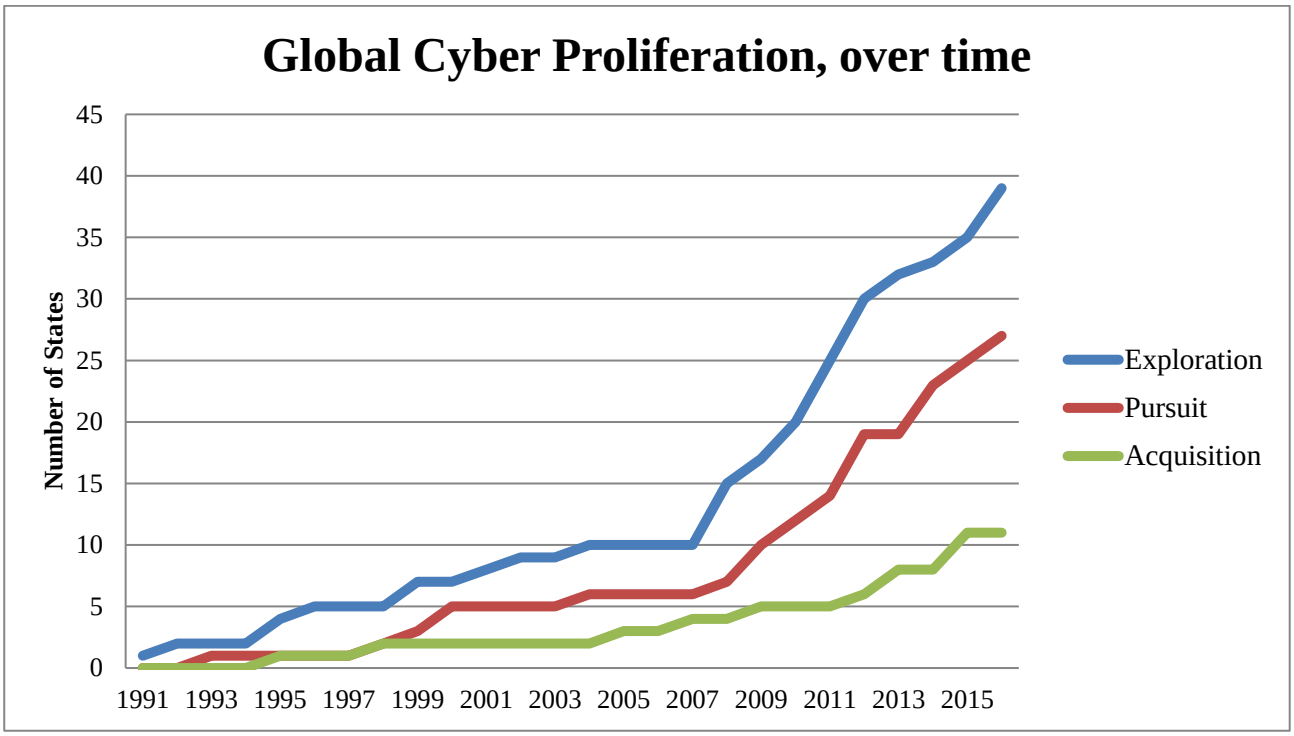
Like the stages of human life, cyber proliferation is a continuous process; meaning the categories are inherently superficial. Yet, unlike the stages of life, the stages of cyber proliferation are not inevitable or deterministic.[202] A state may be forever 'stuck' in an early stage of cyber proliferation or revert to its initial course of action.

An elementary historical representation of when states started to explore, pursue and acquire cyber weapons is provided in figure 3.1. The figure's data is based on two new datasets: the *Cyber Exploration and Pursuit Dataset* and the *Cyber Threat Actors Dataset*.[203]

The figure indicates that currently just below forty states are exploring the development of cyber weapons, below thirty states are at the pursuit stage of cyber proliferation, and not more than a dozen states have actually acquired cyber weapons. Even though these estimates are inherently conservative considering the coding procedures, it suggests that far fewer countries are considering this new military option that some have argued in the past.

[201] The 'exploration' stage is both for nuclear and cyber proliferation to least clearly defined and hardest to ascertain category of behaviour. On nuclear proliferation see: Jo and Gartzke, "Determinants of Nuclear Weapons Proliferation"
[202] Unless you are Peter Pan and you never grow up.
[203] See Appendix 1 and Appendix 2 for codebooks of the datasets. The data can be found in 'Going_Cyber_Data_Smeets.xls'.

Figure 3.1 States' Exploration, Pursuit and Acquisition of Cyber Weapons, over time



We can broadly distinguish between four periods of proliferation. The exploration of developing cyber weapons started with several early movers in the 1990s. It is hardly surprising that the United States, Russia, and China were amongst the first countries exploring the development of these capabilities.[204] First, the U.S. Department of Defence established a special task for in 1967 to study computer vulnerabilities.[205] Following the hack of teenage hacker group 'the 414s', the Congress also held a hearing on cyber security in 1983.[206] According to Michael Warner, historian of the U.S. Cyber Command, the realization that computer attacks could be built into their military arsenals came in the

[204] Beyond these three states, we may consider several other states. First, the United Kingdom may be seen as an early mover, though there is little public data available on this. Second, there is also an unconfirmed statement of the former director of the French Intelligence Agency at a talk at French University, that France was already exploring cyber weapons in the early 1990s. Third, an early case often overlooked is Greece, establishing an Office of Computer Warfare in 1999. Fourth, it has been suggested that Israel was exploring military cyber options in the late 1990s as well. Finally, North Korea's General Staff Department's Electronic Warfare Bureau is known to have existed since at least 2000.

[205] Aki J. Peritz and Michael Sechrist, "Protecting Cyberspace and the US National 3 Interest," *Discussion Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School*, (2010, September); Michael Warner, "Cybersecurity: A Pre-history," *Intelligence and National Security*, 27, 5 (2012):781-799

[206] Washington Post, "The U.S. Government and Cybersecurity", (2003, May 16), retrieved from: http://www.washingtonpost.com/wp-dyn/articles/A50606-2002Jun26.html ; the event occurred a year after "The Cuckoo's Egg" event, when hacker Markus Hess who broke into the computers of the Lawrence Berkeley Laboratory was tracked down by astronomer Clifford Stoll. See: Clifford Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*, (Pocket Books: 2000)

1980s and 1990s.[207] It is suggested that Operation Desert Storm in 1991 gave further impetus to the importance of developing offensive cyber capabilities.[208]

Although China avoids talking about offensive cyber capability development in public, it is said to have paid close attention to these developments in the U.S. in the early 1990s - also publishing various articles about U.S. interest in this new form of 'warfare'.[209] There was a similar development in Russia around this time. In 1996, President Boris Yeltsin, while nominating a new Minister of Defence, said that it was important for Russia to "devote more attention to the development of the entire complex of the means of information warfare".[210]

It took some time until these great powers institutionalized their early interest. In the US, information warfare centres were created at the Air Force in 1993 and a year later at the Navy and Army. In the same period, the NSA set up the Tailored Access Operations (TAO) unit. [211] Since then, the institutional landscape has evolved significantly, not least with the establishment of the U.S. Cyber Command, currently said to have 133 operating units.[212] Much less is known about China's organizational development. PLA Unit 61398 (also known as Comment Crew), located in the Pudong New Area of Shanghai, is said to be responsible for most cyber attacks since the mid- 2000s.[213]

In the 2000s we witnessed a relatively 'quiet' second period, with only a few states expressing (public) interest in the development of cyber weapons. Whereas the first group may be called 'early movers', we may categorize the second group as 'early followers'. One prominent state is Australia. In a comprehensive account of Australia's offensive cyber capabilities, Desmond Ball notes:

> [t]here has been considerable development of doctrine by the [Australian Defence Force] since the early 2000s. In June 2002, the ADF released its doctrinal statement on Australia's approach to warfare. This occurred at about the same time that the notions of being able to gain an information advantage, dispersing forces, and networking them began to appear. The ADF argued that its aim for the future was to obtain common and enhanced battlespace

[207] Rid provides a similar statement: " Defense intellectuals slowly began to discern an offensive and a defensive logic in what Post called 'cybernetic war' in 1979. This development took some time". Warner, "Cybersecurity: A Pre-history"; Rid, *Rise of the Machines*, p. 98;
[208] Also see chapter 5.
[209] For a longer discussion on this topic see chapter 5.
[210] See Warner, "Cybersecurity: A Pre-history"
[211] For a longer discussion on the evolvement of the NSA see chapter 5.
[212] Also an order in May 2016 established a unit with as mission to develop offensive cyber capabilities in order to target ISIS's computer systems. US Cyber Command, "Cybercom Fragord 01 to taskord 16-0063 to Establish Joint Task Force (JST-ARES to Counter the Islamic State of Iraq and the Levant (ISIL) in Cyber Space," (2016, May 5), retrieved from: http://nsarchive.gwu.edu/dc.html?doc=3678213-Document-07-USCYBERCOM-to-CDRUSACYBER-Subj
[213] However, the Chinese Defense Ministry states that the government "has never supported any hacker activities". Zoe Li, "What we know about the Chinese army's alleged cyber spying unit, " *CNN* (2014, May 20), retrieved from: http://edition.cnn.com/2014/05/20/world/asia/china-unit-61398/index.html

> awareness and, with the application of that awareness, deliver maximum combat effect. It would seek to achieve this through networked operations, which would necessitate a comprehensive 'information network' that would link sensors (for detection), command and control (C2) (for flexible, optimised decision-making), and engagement systems (for precision application of force).[214]

Figure 3.1 points out that the most significant spike in interest took place during the third period of cyber proliferation between 2007 and 2013. Around this time, most European states and several other middle powers (such as South-Africa, India, South-Korea, Brazil and Iran) published documents and strategies talking about new opportunities for using offensive cyber capabilities for military purposes. We may describe this group as the 'late followers'.

For example, the Danish government writes in their Defence Agreement 2013-2017 that "the defence must have the capability for military operations in cyberspace, including the ability to protect own network infrastructure, and also to affect opponents' use of cyberspace."[215] It also explicitly states that it should develop a "capacity that can execute defensive and offensive military operations in cyberspace."[216] In addition, the 2013 cyber security strategy of Finland states that the government seeks to "create a comprehensive cyber defence capability for their statutory tasks. […] A military cyber defence capacity encompasses intelligence as well as cyber attack and cyber defence capabilities."[217] In their 2012 National Cyber Security Strategy, Spain wrote that one 'line of action' is to "boost military and intelligence capabilities to deliver a timely, legitimate and proportionate response in cyberspace to threats or aggressions that can affect National Defence."[218] Outside of Europe, the South African government also noted in 2012 that "[t]echnological development […] increases the potential of cyber and space-based warfare".[219]

---

[214] The website of the Australian government provides additional information on the institutional development over the years: "[i]n January 2010 the then Defence Signals Directorate established the Cyber Security Operations Centre to develop a comprehensive understanding of ICT security threats to critical Australian systems, and coordinate a response to those threats across government and industry. The CSOC has since evolved into the Australian Cyber Security Centre (ACSC), opened in November 2014, which is the next evolution of Australia's cyber security capability." See: Australian Government Department of Defence, "CSOC - Cyber Security Operations Centre," retrieved from: https://www.asd.gov.au/infosec/csoc.htm

[215] The report also mentions that "[f]ocus on transverse planning and deployment of capabilities, challenges in the Arctic and in cyberspace, as well as the adaptation of not least the army, will dominate the development of the defence."See: The Danish Ministry of Defence, "Danish Defence Agreement 2013-2017", (2012, November 30), retrieved from: http://www.fmn.dk/eng/allabout/Documents/TheDanishDefenceAgrement2013-2017english-version.pdf, p. 4 and p.8

[216] Ibid, p. 16

[217] Finish Ministry of Defence, "Finland´s Cyber security Strategy," (2013, January 24), retrieved from: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/FinlandsCyberSecurityStrategy.pdf, p. 8

[218] Rajoy Brey, "National Cyber Security Strategy of Spain," (2013), retrieved from: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_ESen.pdf, p.32

[219] Government of South Africa, "South African Defence Review 2012," retrieved from:

For those states too, there is inherently a 'lagged effect' between cyber exploration and pursuit - as it normally takes at least a few years before cyber weapon aspirations are translated into institutional development. For example, in 2008 Brazil's National Defense Strategy called for the need to establish an organization that focuses on developing capabilities for the military.[220] Yet, it was only eight years later the government finally approved the establishment of a cyber command - this was several years later than expected.[221]

Finally, one may expect a possible future 'wave' of military cyber commands in the Middle East. We see that some of those countries have expressed an interest, but few have formally established a military institution responsible for the development and deployment of cyber weapons.[222] The most concrete initiative in the region has so far come from the United Arab Emirates, which is said to be gearing up to launch a cyber command within the General Headquarters of its armed forces.[223]

3.3 Variations of Cyber Proliferation

The above discussion only provides a basic overview of states' cyber proliferation. Although it helps to present a broad picture of the field, it fails to capture that states inherently differ in *how* they have moved closer towards developing cyber weapons. In the words of Hollis and Smith, we need to 'open up the box' and look at what happens *within* the state.[224] I discuss three important variations of cyber proliferation below: level of sophistication, reliance on proxy actors, organizational integration and budgets/funding.

http://www.gov.za/sites/www.gov.za/files/defence%20review_daft.pdf, p. 66

[220] Brazil's Ministry of Defence, "National Strategy of Defense," (2008, December 18), retrieved from: https://www2.gwu.edu/~clai/recent_events/2010/Brazil_Defense/National_Strategy_of_Defense.pdf

[221] Victor Barreira, "Brazil announces establishment of new cyber defence command," *Jane's 360*, (2016, December 29), retrieved from: http://www.janes.com/article/66601/brazil-announces-establishment-of-new-cyber-defence-command

[222] For a more extensive list of potential proliferators see Appendix 3

[223] Bindiya Thomas, "UAE Military To Set Up Cyber Command," *Defense World*, (2014, September 30), retrieved from: http://www.defenseworld.net/news/11185/UAE_Military_To_Set_Up_Cyber_Command#.WXIfz4jyiUk

[224] Martin Hollis and Steve Smith, *Explaining And Understanding International Relations*, (Oxford: Oxford University Press:1991)

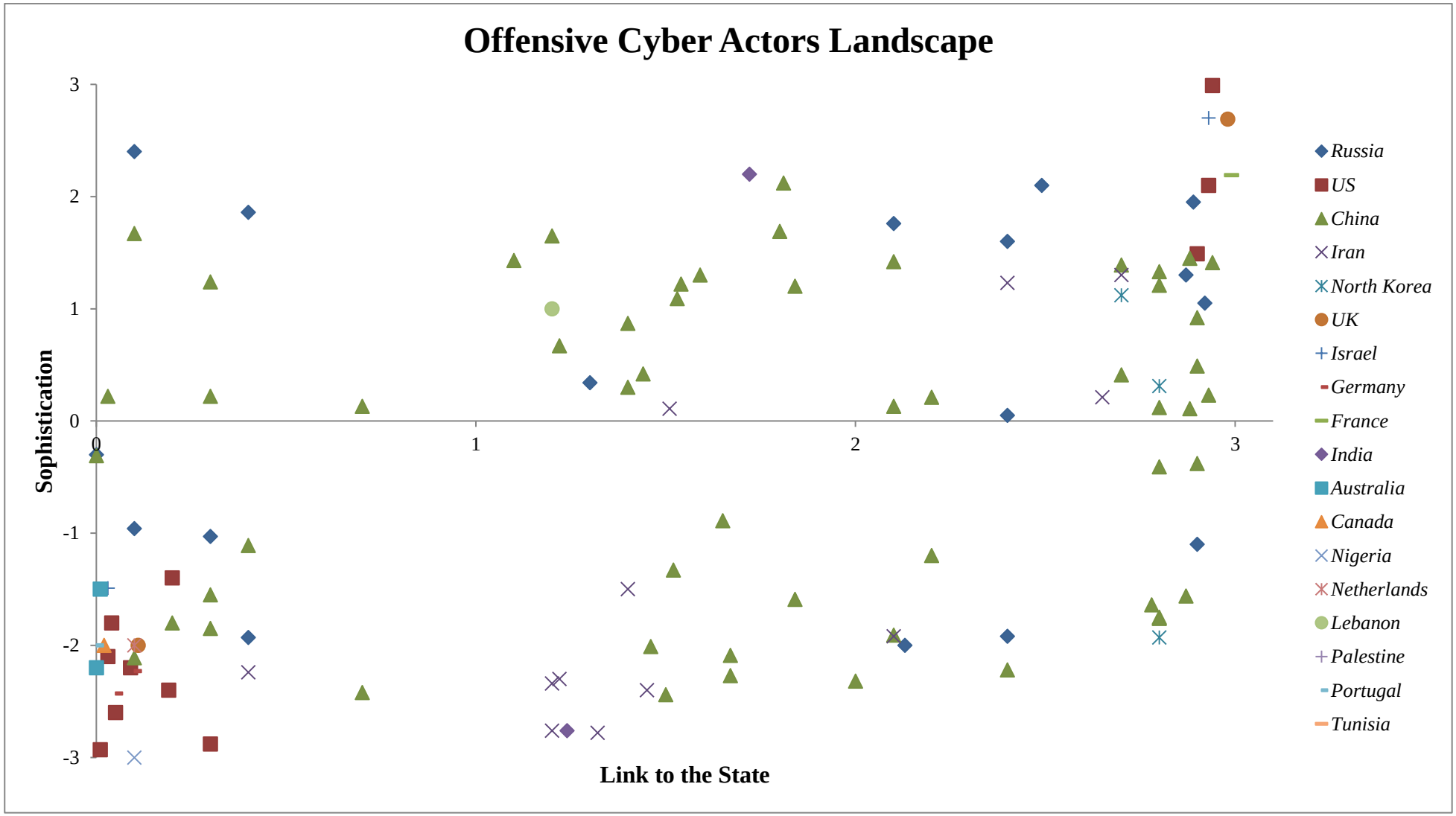
3.3.1 Sophistication[225]

The principal phrase of the American Revolution is that 'all men are created equal'. A key phrase of the 'Cyber Revolution' is that 'actors are (still) unequal'. Whilst not always acknowledged, there is considerable variation in the ability of actors to conduct advanced offensive cyber operations.

Figure 3.2 provides an overview of all the cyber threat actors reported by cyber security firms.[226] It displays i) the actor's state of origin, ii) level of sophistication, iii) and link to the state. Figure 3.2 implies that some of the most sophisticated capabilities reside within a small group of Western states (the United States, UK, France, and Israel). A large group of actors within Russia and China seem to be able to conduct intermediate to sophisticated cyber attacks. Note that both Iran and North Korea have the ability to conduct cyber attacks - yet their abilities seem to be limited.

[225] The discussion on 'sophistication' here follows the definition provided in the introduction.
[226] Appendix 2 provides offers a discussion on coding procedures and biases.

Figure 3.2: Offensive Cyber Actors Landscape



Let us consider in more detail the three states - US, China, and Russia - which lead the military race in cyberspace. Figures 3.3-3.5 offer bar charts of all the actors within a state, ranked on the basis of their level of sophistication. First, as figure 3.3. demonstrates, there are only a few actors known to operate from the United States. Yet, we know that the key actor of this selected group is highly advanced; the 'God' of cyber, NSA's 'Equation group' has developed the most sophisticated suite of surveillance platforms to date.[227] The group has been connected to weaponized cyber capabilities, including Stuxnet, as well.[228] The exact arsenal management of the NSA (and the Cyber Command) - and the U.S. government more generally - currently remains unclear. Healey's study implies that the government probably retains dozens rather than hundreds or thousands per year - a number much lower than most expected.[229]

Second, figure 3.4 reveals that many more cyber threat actors are known to operate from China. In contrast to the US, most actors have the ability to only conduct relatively unsophisticated cyber-attacks. These findings support Lindsay's claim that, "there is little evidence of skill or subtlety in China's military cyber operations. Although Chinese strategists describe cyberspace as a highly asymmetric and decisive domain of warfare, China's military cyber capacity does not live up to its doctrinal aspirations."[230] An increase in resources and a potential reorganization of the PLA cyber activities suggests that this may change in the future.[231]

Third, figure 3.5 indicates that some of the most advanced actors operating in cyberspace are based in Russia. An early case of Russian cyber activity is dubbed 'Moonlight Maze', an espionage

[227] The 'Equation Group' was initially disclosed by Kaspersky Lab. For an excellent timeline and overview see: Kaspersky Lab, "Equation: The Death Star of Malware Galaxy," (2015, February 16), retrieved from: https://securelistcom/blog/research/68750/equation-the-death-star-of-malware-galaxy/; Kim Zetter, "Suite of Sophisticated Nation-State attack tools found with connection to Stuxnet," *Wired*, (2015, February 16), retrieved from: https://www.wired.com/2015/02/kapersky-discovers-equation-group/

[228] See chapter 3 for a more extensive discussion on Stuxnet. According to the Washington Post (reporting a leaked document), the NSA carried out 231 offensive cyber-operation in 2011. See: Barton Gellman and Ellen Nakashima, "U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show,"(2013, August 30), *The Washington Post*, retrieved from: https://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html?utm_term=.dfb3852da14a; on NSA implants see: Ryan Gallagher and Glenn Greenwald, "How the NSA plans to infect 'millions' of computers with malware," *The Intercept,* (2014, March 12), Retrieved from: https://theintercept.com/2014/03/12/nsa-plans-infect-millions-commputers-malware/

[229] Jason Healey, "Feds and 0Days: From Before Heartbleed to After FBI-Apple," *DefCon, Las Vegas* (2016)

[230] Lindsay lists 37 cases of alleged Chinese CNE from 2005 through 2013, ordered by the date the intrusions were publicly reported in Western media and showing the estimated duration of each intrusion. Jon R. Lindsay, "Exaggerating the Chinese Cyber Threat," Harvard University, Belfer Center for Science and International Affairs, Policy Brief, (2015, May); Joe McReynolds, "China's Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy," *China Brief*, 15:8 (2015).

[231] FireEye, "Redline Drawn: China Recalculates its use of cyber espionage," (2016, June 20), retrieved from: https://www.fireeye.com/blog/threat-research/2016/06/red-line-drawn-china-espionage.html.

operation against U.S. government networks that was discovered in 1998.[232] The Dukes espionage platform, active since at least 2008, and Pawn Storm, are good examples of more recent Russian activity.[233] The Russian perception of this field, however, is different from the United States. Russia shies away from using the term 'cyber', and instead uses the more holistic term 'information war'.[234] As Keir Giles states, for Russia it is as much about 'hostile content' as it is about 'hostile code'.[235] The information warfare notion is derived directly from *spetspropaganda* (special propaganda) theory developed in the early 1940s.[236] Key thinkers like Igor Panarin and Aleksandr Dugin have further contributed to Russia's understanding. A report from the UK House of Commons states "[a] recurring theme in Russian military strategy is the ability to combine various tools seamlessly, to give a fully integrated, comprehensive approach. The Russian attitude to cyber as a tool of warfare is no different, with a full-spectrum approach integral to the strategy of the Russian Government."[237] The use of the word 'seamlessly' might be misleading considering Russia's conscious on-going efforts to develop this approach, learning from its mistakes along the way.[238] Indeed, Russia's attack on Georgia in 2008 was only partially successful, yet the more recent attacks on Ukraine suggests that it studied the lessons learned.[239]

[232] Rid, *Rise of the Machines*
[233] F-Secure, "The Dukes: 7 years of Russian cyberespionage," *Whitepaper,* (2011, January 29), retrieved from: https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf; Jen Weedon, "Beyond 'Cyber War': Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine," in Kenneth Geers (Ed.), *Cyber War in Perspective: Russian Aggression against Ukraine,* (Tallinn: NATO CCD COE Publications: 2015)
[234] Russia only uses the term to denote Western and Chinese activities. See: Shires and Smeets, "What do we talk about when we talk about 'cyber'?"
[235] To understand how this is woven into official military and policy strategy see: Russian government, "Information Security Doctrine of the Russian Federation" (200, September 9), retrieved from: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf; David J. Smith, "How Russia Harnesses Cyberwarfare," *American Foreign Policy Council (2012, August), retrieved from:* http://www.afpc.org/files /august2012.pdf.
[236] Jolanta Darczewska, "The anatomy of Russian information warfare; the Crimean operation, a case study," *Centre for Eastern Studies,* (2014) retrieved from: https://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf; The notion is possibly even older, going as far as back as the Bolsheviks.
[237] UK Parliament, "Russia: Implications for UK defence and security," (2016, June 30), retrieved from: https://www.publications.parliament.uk/pa/cm201617/cmselect/cmdfence/107/10710.htm
[238] Sputnik News, "Russia Considering Cyber Security Command," (2012, March 21), retrieved from: http://en.rian.ru/russia/20120321/172301330.html
[239] Smith, "How Russia Harnesses Cyberwarfare"

Figure 3.3: Reported Cyber Threat Actors based in the US

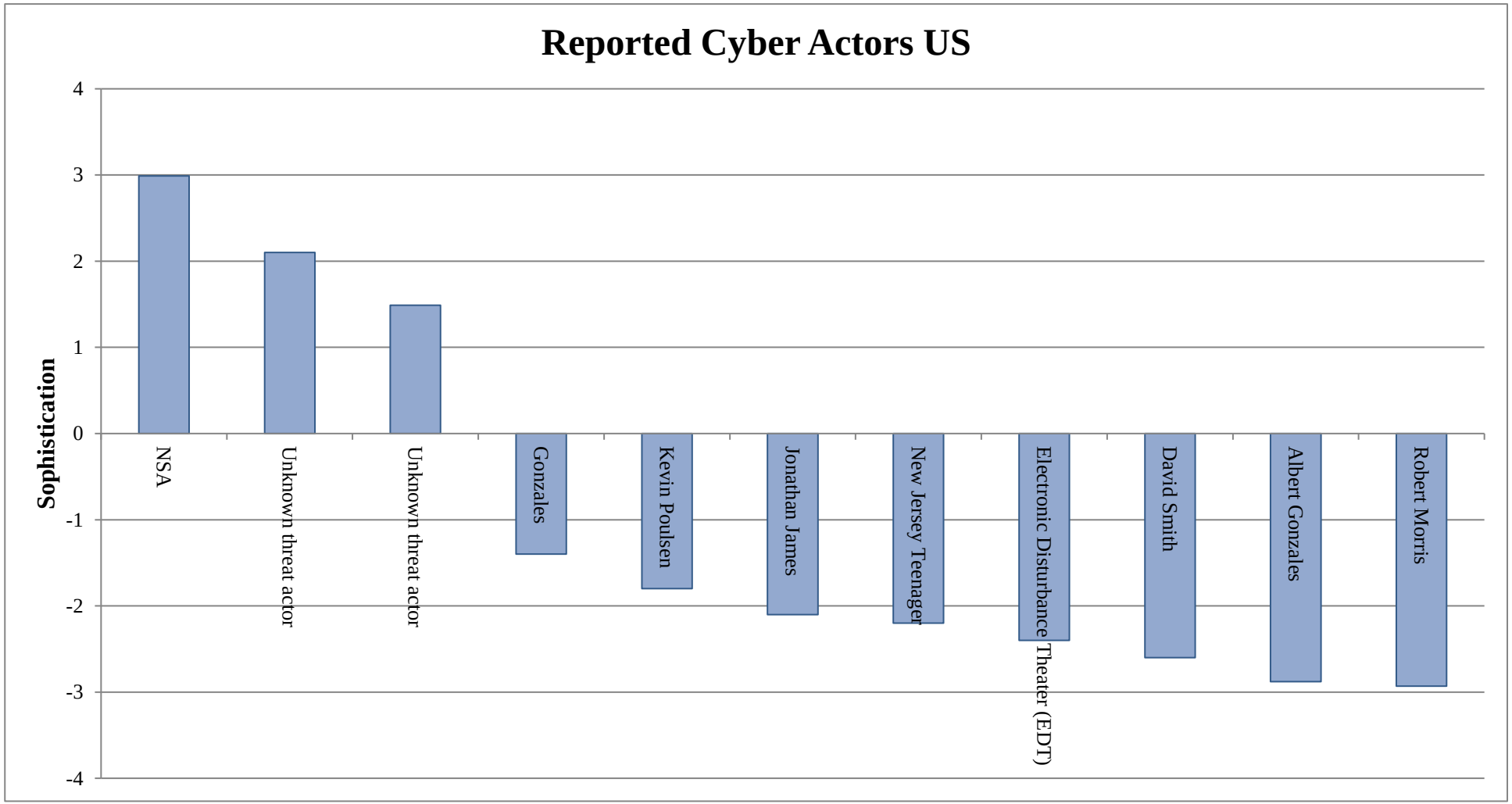
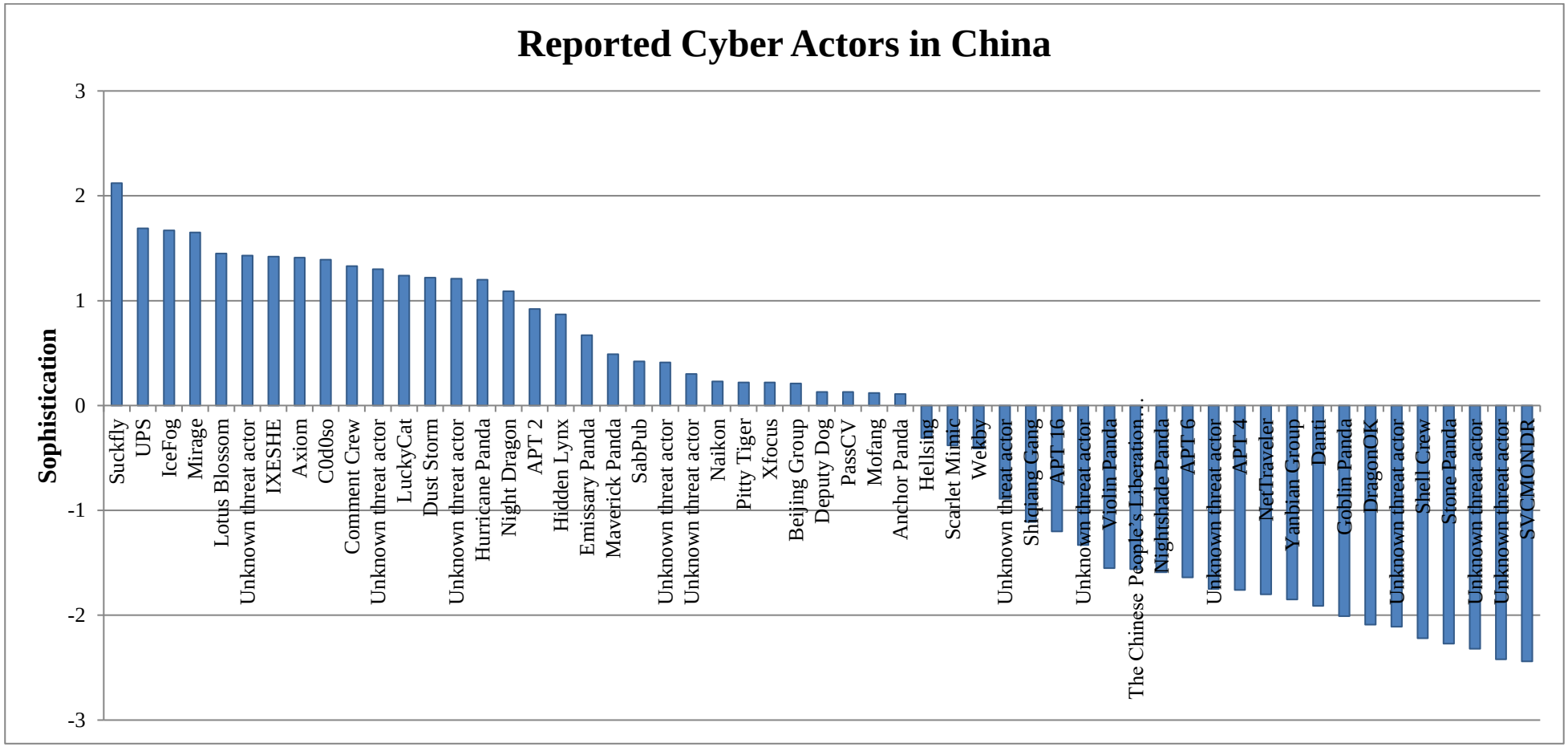


Figure 3.4: Reported Cyber Threat Actors based in China



** The following cyber threat actors originating from China are not shown in the figure due to a lack of data on sophistication: APT 22, APT 26, Big Panda, Electric Panda, Eloquent Panda, Foxy Panda, Gibberish Panda, Hammer Panda, Impersonating Panda, Karma Panda, Keyhole Panda, Lotus Panda, Mana Team, Pale Panda, Pirate Panda, Predator Panda, Radio Panda, Spicy Panda, Su Bin, SVCMNDR, TEMP.Zhenbao, Test Panda, Toxic Panda, Union Panda, Wet Panda, Wisp Team, Poisonous Panda.*

Figure 3.5: Reported Cyber Threat Actors based in Russia



** The following cyber threat actors originating from Russia are not shown in the figure due to a lack of data on sophistication: Angel Bear, FSB 16th and 18th Centers, and Fort Disco.*

3.3.2 Proxy Actors [240]

State and non-state actors coexist in cyberspace - and at times there are strong links between the two. We can broadly categorize non-state cyber actors into four groups: i) state-free, ii) state-encouraged; iii) state-sponsored; and iv) state-conducted.[241] Combined, the second (state-encouraged) and third (state-sponsored) groups of actors can also be described as 'cyber proxies', i.e. non-state actors used by a state actor to conduct an offensive cyber operation.

Figure 3.2 suggests that there is not only variation in the ability of states to conduct sophisticated cyber operations, but there is also an unequal reliance by states on proxy actors. Figures 3.6-3.8 capture this variation in more detail for the US, China and Russia. The figures display both the threat actor's level of sophistication and link to the state, and the error bars show the level of attribution certainty.[242]

The U.S. seems to be primarily conducting state-led operations (figure 3.6). Although we only know of a few actor groups, given the leakage of information we have a high level of certainty about the nature of these actors (i.e. we know that the Equation group is the U.S. government). Figure 3.8 suggests that Russia's most sophisticated groups are primarily state-led or state-sponsored. Yet, we have much less attribution certainty about these actors. Indeed, most reports make suggestions about a link to the state but provide little information to back up these claims. Finally, the Chinese offensive cyber actor landscape (figure 3.7) seems to be the most dense and diverse. It suggests that a large network of both state and non-state actors - linked to various degrees - conduct both unsophisticated and moderately sophisticated attacks. Also, even though there has been a significant amount of reporting from cyber security firms on Chinese threat actors, as the length of the error bars suggests, there is little certainty about the actor's link to the state in most cases.

---

[240] Around 'weak governments' we often see patriotic hacking group taking the name of the country. For example, there is the Ukraine Cyber Force, Yemen Cyber Army, and the Tunisian Cyber Army. There is also an Armenian hacker group called the Monte Melkonian Cyber Army (MMCA). Using these names has much to do with branding; it adds legitimacy to the group's activities. Yet, all of them remain limited in their offensive capability and are often not connected to the state. Eugene Dokukin, a web specialist has established the 'Ukrainian Cyber Forces' which is supportive of the governments and aims to counteract recent Russian malicious activity. Waqas, "Armenian Hackers Leak Azerbaijani Banking and Military Data," (2016) Retrieved from: https://www.hackread.com/armenian-hackers-leak-azeri-banking-military-data/; Info Security, "Cyberwar between India and Bangladesh escalates," *Info Security*, (February 16, 2012), Retrieved from: http://www.infosecurity-magazine.com/news/cyberwar-between-india-and-bangladesh-escalates/; Nicole Perloth, "Hunting for Syrian Hackers' Chain of Command," *The New York Times*, (2013, May 17), retrieved from: http://www.nytimes.com/2013/05/18/technology/financial-times-site-is-hacked.html?pagewanted=all&_r=0; E Hacking News, "Tunisian cyber army Cyber attack against French websites," (2013, February), retrieved from: http://www.ehackingnews.com/2013/02/tunisian-cyber-army-cyber-attack.html

[241] A description of the categories can be found in Appendix 2.

[242] Appendix 2 provides a longer discussion on attribution.

Despite this variation, little research has been conducted on the use of cyber proxies. Although an extensive discussion goes beyond the scope of this analysis, there are three dimensions which deserve to be scrutinized further.

First, there seems to be a general consensus in the sparse literature that states use cyber proxies as a vehicle because they can plausibly deny any relationship. Maurer, using a quote from privateering, states "[a] general political incentive for states to use proxies is summed up by the concept of 'plausible deniability".[243] Similarly, Borghard and Lonergan write: "[s]pecifically, the informal, plausibly deniable nature of the relationship - which we claim is its most theoretically significant aspect - is the core defining feature of the relationship across all kinds of non-state cyber actors, regardless of their motivations."[244] The underlying logic here is that a state can potentially avoid political and reputational costs and reduce the risk of retaliation.[245]

Yet, the plausible deniability argument explains little variation. Based on the plausible deniability argument, we should expect democracies especially - states which high levels of public accountability and more receptive to reputational costs than authoritarian regimes - to rely on these types of actors.[246] Yet, we observe the reverse pattern; it seems to be Russia - as well as other states like Iran - that primarily act through cyber proxies.

This means we have to look at other factors - beyond plausible deniability - to explain the pattern of this relationship. Potentially more important factors concern the availability and cost-effectiveness of using non-state actors. Indeed, as the Defence Committee of the House of Commons notes, "[Russia] still retains the core Soviet strength in the STEM subjects: science, technology, engineering and mathematics. They are producing an inordinate number of skilful engineers, technicians and mathematicians, and that feeds into the cyber-realm."[247] Drawing on this group helps to solve some

[243] Tim Maurer, "Cyber Proxies and the Crisis in the Ukraine," in Kenneth Geers (ed.), in Kenneth Geers (Ed.), *Cyber War in Perspective: Russian Aggression against Ukraine*, (Tallinn: NATO CCD COE Publications: 2015); Tim Maurer, "Hackers for hire: Cyber-mercenary industry grows worldwide," *IHS Jane's Intelligence Review*, (2015, September)
[244]Erica D. Borghard and Shawn W. Lonergan, "Can States Calculate the Risks of Using Cyber Proxies?," *Orbis*, 60:3 (2016) 395-416, p. 405
[245] Ibid
[246] Melvin J. Dubnick and Barbara S. Romzek, "Accountability and the Centrality of Expectations in American Public Administration," *Research in Public Administration*, 2 (1993): 37-78
[247] House of Commons, "Russia: Implications for UK defence and security ," *First Report of Session 2016-17,* (2016), retrieved from: https://www.publications.parliament.uk/pa/cm201617/cmselect/cmdfence/107/107.pdf; Similar point made in: Franz-Stefan Gady and Greg Austin, "Russia, The United States, And Cyber Diplomacy Opening the Doors" *East West Institute*,(2010) retrieved from: https://info.aiaa.org/tac/isg/SOFTC/Public%20Documents/Technical%20Working%20Groups/Cybersecurity/USRussiaCyber_WEB.pdf

of the problems President Vladimir Putin addressed in the *2000 Information Security Doctrine*, with the deployment of non-state actors providing a cost-effective solution.[248]

Second, the relationship between the state and cyber proxies is generally characterized using a 'principal agent framework'.[249] From this perspective, the agent (i.e. the cyber proxy) acts on behalf of the principal (i.e. the state) and does not have a conflict of interest in carrying out the act. This understanding suggests that the actions of cyber proxies are in line with the intentions of the state. Yet, most conventional control mechanisms which normally exist to avoid agency slacking - like contract establishment, monitoring, agency selection and screening, institutional design, and punishment - are each more difficult to establish in this specific type of relationship.[250]

This means that cyber proxies are likely to have greater independence than is generally assigned to them - especially if they are able to exploit asymmetric information advantages. It also suggests that even if a link between a state and a non-state actor is known to exist (e.g. observed flow of resources or received instructions) it does *not* mean that the cyber proxy's actions are perfectly aligned with the state's intentions. As a result, states may have to reconsider how they should respond to threats from these actors.[251]

Third, the current presumption in the literature on cyber proxies is that non-state actors are merely used to maximize the utility of the state actor, and to help deal with a policy problem through conducting cyber operations - and its benefit as discussed above might come from reducing risk or being more cost efficient. Yet, following the constructivist literature, cyber proxies might have the ability to do much more than this; they may also create (collective) 'systems of meaning' and help state actors define the meaning of appropriate behaviour in various geopolitical situations.[252] Indeed, little research has been conducted on how cyber proxies can shape what states might want.

---

[248] Cited in: Gady and Austin, "Russia, The United States, and Cyber Diplomacy Opening the Doors"

[249] For an extensive application see: Tim Maurer, "'Proxies' and Cyberspace," *Journal of Conflict & Security Law,* 21:3 (2016) 383-403

[250] John Brehm and Scott Gates, *Working, Shirking, and Sabotage: Bureaucratic Response to a Democratic Public,* (Michigan: University of Michigan Press: 1997) The general argument is made that the general goal of bureaucratic behaviour is expansion; expansion of budgets, of powers, and of existence over time. One might say that for cyber proxies it could be both financial gain as well as general prestige/power.

[251] Koh states that argues that "states are legally responsible for activities undertaken through 'proxy actors', who act on the State's instructions or under its direction or control." Yet, considering the high chance of agency slacking, this view could be highly escalatory as the cyber proxy may well conduct activities not in line with the principal's objectives. Cited in Maurer, "Proxies' and Cyberspace"

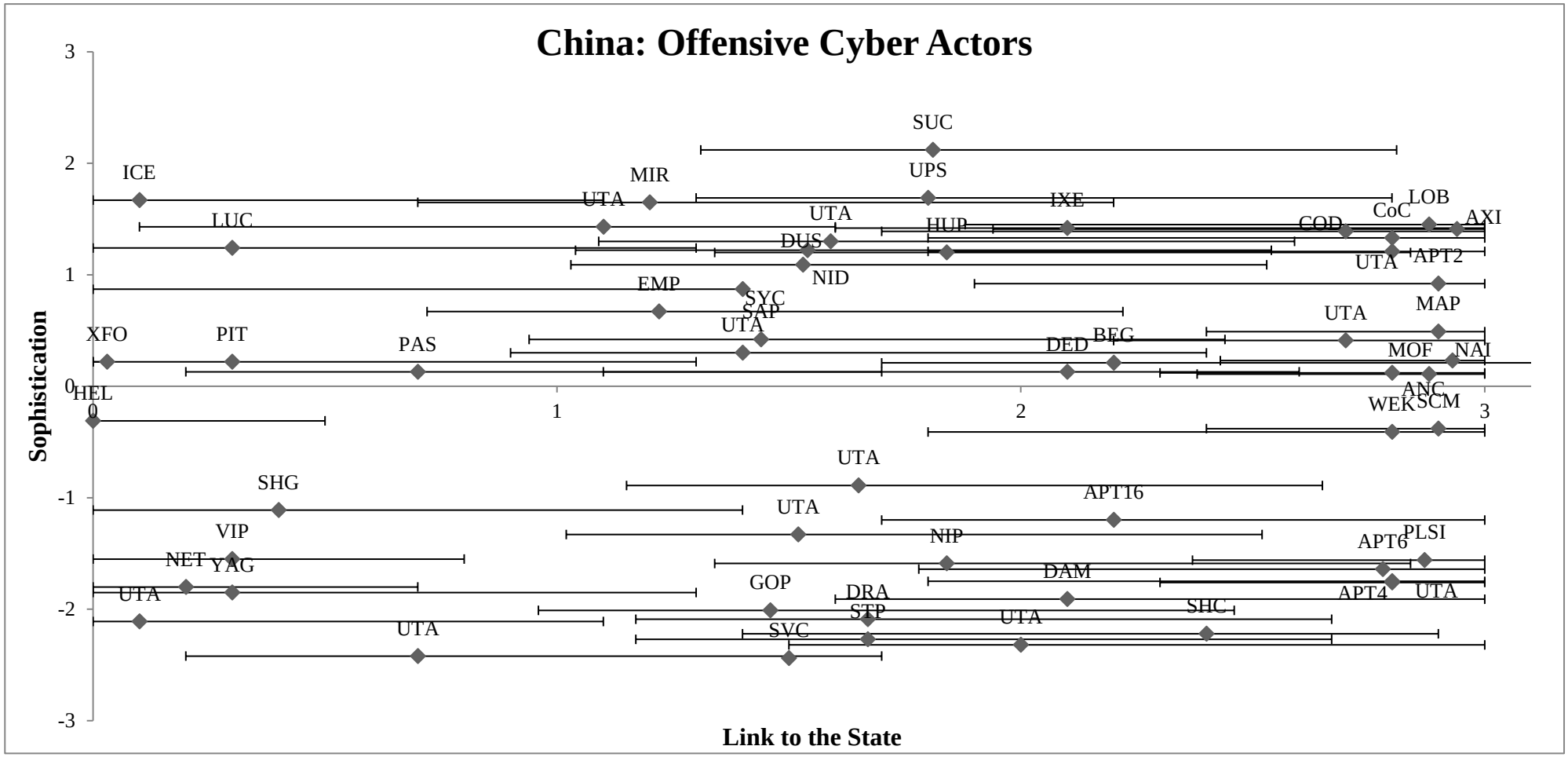
[252] The argument of constructivist scholars is that systems of meaning are created through knowledgeable practices of purposeful agents. Thomas Risse, 'Let's Argue,*' International Organization*, 54 (2000) 1–41; Christian Reus-Smit, "Constructivism" in Scott Burchill, Andrew Linklater, Richard Devetak, Jack Donnelly, Matthew Paterson, Christian Reus-Smit and Jacqui True (eds.), Theories of International Relations, (Hampshire: Palgrave Macmillan: 2009), pp. 212-236

Figure 3.6: Offensive Cyber Actors in the U.S. and Attribution Certainty



**The names associated with the abbreviations can be found in the descriptions file of the Cyber Threat Actor dataset. UTA refers to 'Unknown Threat Actor'*

Figure 3.7: Offensive Cyber Actors in China and Attribution Certainty



** The following cyber threat actors originating from China are not shown in the figure due to a lack of data on sophistication: APT 22, APT 26, Big Panda, Electric Panda, Eloquent Panda, Foxy Panda, Gibberish Panda, Hammer Panda, Impersonating Panda, Karma Panda, Keyhole Panda, Lotus Panda, Mana Team, Pale Panda, Pirate Panda, Predator Panda, Radio Panda, Spicy Panda, Su Bin, SVCMNDR, TEMP.Zhenbao, Test Panda, Toxic Panda, Union Panda, Wet Panda, Wisp Team, Poisonous Panda*

Figure 3.8: Offensive Cyber Actors in Russia and Attribution Certainty



***The following cyber threat actors originating from Russia are not shown in the figure due to a lack of data on sophistication: Angel Bear, FSB 16th and 18th Centers, and Fort Disco. Also ItaDuke and Crouching Yeti were excluded because of a lack of attribution information.*

3.3.3 Organizational Structure and Budgets

A final variation in cyber proliferation between states to consider is in the set-up of offensive cyber programmes. Principally, states make different decisions on how to organizationally integrate defence, exploitation/intelligence, and attack.[253] Organizational integration of offensive cyber capabilities (OIOCC) can come in many shapes and forms: through appointing the same director for the intelligence services as for the command conducting military activities; through establishing a significant intelligence constituency within the military command; through offering the same training programme to those conducting espionage operations and those conducting offensive (destructive) cyber operations; and through moving people from an intelligence gathering unit to a military unit and vice versa.[254]

The current trend is to establish a military command that serves to combine all three forms of operations (whilst keeping the intelligence unit partially separate). Yet, there are exceptions to this rule. Israel's main offensive cyber capability is at the Defence Forces' Unit 8200 and the C4I Corps. Although there have been talks about creating an overarching cyber command - not least because the conduct of cyber operations fits well within Israel's overall military doctrine - Israel has rejected the establishment of such a department in early 2017.[255]

States also have vastly different budgets and personnel allocated to their military cyber command (or counterpart). Beyond the three most significant cyber powers - U.S., Russia, and China - several countries pour significant resources into cyber capability development. France's new cyber command, is said to "employ 2600 cyber-security experts by 2019 and receive an initial commitment of €2.1 billion in funding".[256] The UK's most recent cyber security strategy indicated it will spend

[253] I follow Lawrence and Lorsch's definition of organizational integration (OI) as 'the process of achieving unity of effort among the various subsystems in the accomplishment of the organisation's tasks'. In more poetic terms, integration is about achieving a harmonious marriage of activities. Like any good marriage, there are many ways in which OI can be successfully achieved. Paul R. Lawrence and Jay W. Lorsch, 'Differentiation and Integration in Complex Organisations', *Administrative Science Quarterly*, 12:1 (1967), 1-47; also see Henri Barki and Alain Pinsonneault, 'A model of Organizational Integration, Implementation Effort, and Performance', *Organization Science*, 16:2 (2005)165-179. For a contrasting view of marriage, see Tolstoy's Anna Karenina Principle.

[254] I do not argue that there is an ideal configuration of integration as it likely depends on the size and capital (also human capital) of the cyber operations.

[255] For a more extensive discussion see: Max Smeets, "Organizational Integration of Offensive Cyber Capabilities: A Primer on the Benefits and Risks", in Henry Roigas, Raik Jakschis, Lauri Lindstrom, and Tomáš Minarik (Eds), *9th International Conference on Cyber Conflict* (Tallinn, NATO CCD COE Publications: 2017)

[256] Tom Reeve, "France unveils cyber command in response to 'new era in warfare' ," *SC magazine*, (2016, December 16), retrieved from: https://www.scmagazineuk.com/france-unveils-cyber-command-in-response-to-new-era-in-warfare/article/579671/

£1.9 billion to 'defend', 'deter', and 'develop.[257] Germany reports that it aims to hire a total of 13,500 personnel for its new cyber command.[258]

Yet, the majority of states allocated budgets of only a few million dollars. According to the Wall Street Journal, the Danish government "[a]llocates about $10 million a year for 'computer-network operations,' including defense and offense, since 2013."[259] Other media reports indicate that, in 2015, $75 million was allocated for offensive cybercapabilities through 2017. In 2014, Spain for the first time allocated a budget of €2.3 million to enhance its ability to conduct offensive cyber operations.[260] In the Netherlands, the initial budget was €50 million to establish the new cyber command, with an annual budget just above €20 million for the following years. Greece is also an interesting case. The government established an Office of Computer Warfare in 1999.[261] Five years later, in 2004, the Department of Cyber Defence was established, which was subsequently 'upgraded' to the Directorate of Cyber Defence in 2011.[262] Even though this institutional development looks significant, as Nomikos writes, there is currently a lack of funding due to austerity measures, making it difficult to operate.[263] Although the differences in budget and personnel allocated can partially be explained based on the above description of the variations in OIOCC and Gross Domestic Product (GDP), the differences remain noteworthy.

3.4 'Order of Entry' Effects in Cyber Weapon Development: First Mover and Latecomer Advantages

The above sections of this chapter have provided an overview of which states have explored, pursued and acquired cyber weapons. Two basic observations came to the fore (in section 3.2). First, we witnessed a growing interest among states in developing cyber weapons (and offensive cyber capabilities more generally). Second, there is significant variation between states as to when they start

[257] In other words, this budget includes both offensive and defensive activities. See: UK government, "Britain's cyber security bolstered by world-class strategy," (2016, November 1), retrieved from: https://www.gov.uk/government/news/britains-cyber-security-bolstered-by-world-class-strategy
[258] The German cyber command has a relatively broad mandate.
[259] Jennifer Valentino-Devries and Danny Yadron, "Cataloging the World's Cyberforces," *Wall Street Journal* (2015, October 11), retrieved from: http://graphics.wsj.com/world-catalogue-cyberwar-tools/
[260] Brey "National Cyber Security Strategy of Spain," (2013), p. 32
[261] United Nations Institute for Disarmament Research (UNIDIR), "The Cyber Index International Security Trends and Realities," (2013), retrieved from: http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf
[262] Ibid
[263] An encouraging way to describe these cyber commands is to call them 'incubators'; relatively new organizations with limited 'seed capital' which aim to develop innovative ways to approach the cyber threat. A less positive description is that these cyber commands are 'empty-shells'; they exist on paper, but in reality conduct little to no meaningful activity.

to proliferate. This dual observation leaves us with the following question: does it matter *when* a state actor starts to proliferate?

The effects of 'order of entry' have been extensively examined when it comes to a firm's performance - the industrial economics literature has paid particular attention to this topic.[264] Early studies emphasize that 'earlymovers' have an advantage over 'newcomers' as they can create various strategic barriers of entry. Later economics research has subsequently provided a more balanced account, showing that there are also advantages for latecomers.

The aim of this section is to critically review the insights from this body of literature. First, I assess whether potential entry order advantages exist for early movers when it comes to cyber proliferation. In this context, an 'early mover' concerns a state which already in the late 1990s and early 2000s pursued, explored, and/or acquired offensive cyber capabilities.[265] Second, I look at the potential latecomers advantages (and disadvantages of moving early). This group refers to both states which have recently started to pursue, explore and acquire cyber weapons as well as future proliferators.

There are a number of reasons why a discussion of 'order of entry' effects is particularly relevant in this context. Most importantly, it furthers our understanding about whether the global process of offensive cyber capability development has a bias towards convergence or divergence. In that sense, it reveals how (and for how long) states, which currently have acquired sophisticated cyber capabilities, are able to stay ahead of the curve. Also, the incentives to invest a disproportionate amount of resources into early capability development today are significantly reduced if states know they can catch up in the future.[266] More generally, order of entry effects can change the incentive structure of, what some term, a 'cyber arms race'; if states are aware they are unable to catch up, there might be incentives to shift competition to a different domain - if possible.

3.4.1 Early Mover Advantages

[264] For an excellent literature review see: Peter Magnusson and David J. Boggs, "Order-of-Entry Effects for Service Firms in Developing Markets: An Examination of Multinational Advertising Agencies," *Journal of International Marketing*, 17:2 (2009)23-41

[265] Notice that in the literature the terms 'first mover' or 'early entrant' are not always clear. It can refer to either the very *first* firm or a *group* of firms developing a certain product or service. Following the definition used in this thesis, I look at a group of states rather than the first state developing offensive cyber capabilities. Finally, I use 'first mover' and 'early entrant' interchangeably, whereas some scholars have distinguished between these categories (and added narrower terms such as 'pioneers').

[266] Of course, the timing of cyber weapon development may not always be a matter of strategic choice. Instead, late entry may be the only option for some states considering their lack of (initial) awareness and resources to focus on this issue early.

There are three early mover advantages that are most prominently discussed in the literature on industrial economics: switching costs, pre-emption, and learning by doing.[267] As will become clear, only the latter applies to the development of cyber weapons.

First, firms entering the market early are said to benefit from the buyers' costs of switching.[268] The idea is that "[w]ith switching costs, late entrants must invest extra resources to attract customers away from the first-mover firm".[269] Buyer switching costs may result from investments costs the buyer makes to adapt to the seller's product or learning from the customer, adapting to the product.[270] Also, early entry firms tend to have more time to build their image and acquire customer loyalty.[271] This means that when new firms enter the market, customers tend to be conservative and repeat purchases.[272]

Yet, the attacker-defender dynamics for cyber proliferation - compared to the conventional buyer-seller dynamics - differ substantially. There is an inherent incentive for an actor to *not* align their defence with the attacker's capability. Furthermore, there is an inverse relation between the length of time a piece of malware is 'in the wild' and its effectiveness as it provides the opportunity for the defender to adjust its defences.[273]

A second mechanism which is said to favour firms entering the market early is that of *pre-emption.*[274] This refers to the notion that early entrants can exploit the competitive vacuum in a variety of ways, most prominently in attracting necessary skills early on, pre-empting key product dimensions, and strategically positioning in a geographical space. None of these incentives hold for states' developing cyber weapons. First, generally only nationals can work at a state's cyber command, meaning the competition of skills is largely non-existent between states. Second, cyber weapons are not protected by patents; and states are not barred from absorbing/copying 'product dimensions' of offensive cyber

[267] Marvin B. Lieberman and David B. Montgomery, "First-Mover advantages," *Strategic Management Journal*, 9 (1988)41-58; Dong-Sung Cho, Dong-Jae Kim, and Dong Kee Rhee, "Latecomers Strategies: Evidence from the Semiconductor Industry in Japan and Korea," *Organizational Science*, 9:4 (1998, July-August), p. 498-504;
[268]See Cho et al., "Latecomers Strategies," p. 490
[269] Lieberman and Montgomery, "First-Mover advantages"
[270] Dennis C. Mueller, "First-mover advantage and path dependence", *International Journal of Industrial Organization*, 15:6 (1997) 827-850, p. 831
[271] Al Ries and Jack Trout, "Marketing Warfare," *Journal of Consumer Marketing*, 3:4 (1986) 77-82
[272] The principle of 'brand loyalty' is sometimes considered to be a separate category.
[273] The phrase 'in the wild' is frequently used by security analysts. The phrase originates from an initiative in the 1990s called 'The WildList' by Joe Well, to make a list of all the viruses which have been found spreading (in the real world, and not just research labs).
[274] Cho et al., "Latecomers Strategies," p. 491

capabilities used by other states. Finally, cyberspace is constantly changing. The malleability of cyberspace means that positioning advantages in cyberspace are more difficult to maintain too.[275]

The third and final prominent advantage of early movers is normally referred to as 'learning by doing'.[276] Dong et al. state that "[m]oving earlier than others implies more time to experience the process of value-adding activities to produce and sell the product. Advantages may arise from each identifiable value-adding activity (e.g., research and development, manufacturing, marketing and sales) and learning rates. Technological leadership reflects the early mover's accumulated experience in research and development and additional related activities."[277] Similarly, it is likely that early movers in cyber proliferation currently benefit from having dealt with the (technical, organizational, and strategic) complexities of acting in/through cyberspace for a certain number of years.[278]

3.4.2 Late Mover Advantages

Late mover advantages (or early mover disadvantages) can be categorized in; i) free-rider effects, and ii) technology-shifts and incumbent-inertia. Their application to cyber proliferation do not provide straightforward 'yes' or 'no' answers. Instead, the analysis reveals a number of interesting nuances on how states could benefit from late entry.

The first advantage often discussed in relation to firms' late entry to the market concerns 'information spill-over'. As Cho et al. write, "information spillover lends another advantage to latecomers in such form as significantly reduced R&D costs from diffusion of technologies over time, which could be due to the lower cost of imitation or learning from the mistakes of early movers (skipping trial and error), another kind of free-rider effect."[279]

This issue has been prominently addressed in relation to offensive cyber capability development (normally referred to as 'information security'). The most expressive discussions on this relate to a series of information leakages of U.S. offensive cyber capabilities through the Snowden Files,

[275] The final dimension is potentially the one which may still exist in cyberspace - not least considering US' position and how the internet is built over the original Arpanet
[276] An assumption underlying this barrier of entry is that learning can be kept secret from others.
[277] Cho et al., "Latecomers Strategies,"
[278] For a recent discussion on how Russia has used Ukraine as a 'test lab'; Andy Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar," *Wired*, (2017, June 20), retrieved from: https://www.wired.com/story/russian-hackers-attack-ukraine/
[279] Cho et al., "Latecomers Strategies,"

Wikileaks, and Shadowbrokers leaks.[280] However, free-rider effects due to information spill-overs are conditional upon two factors; i) the *spread* of information, and ii) the ability to *uptake* this information. There are several cases that suggest the second condition - that is, the uptake of information - has not always been straightforward. Iran, for example, is said to have developed its 'wipers' based on U.S.' earlier design of this type of capability. Yet, its initial wiper malware against Saudi Aramco contained at least three coding errors.[281]

The benefits of enhanced levels of information are also said to differ depending on the characteristics of the late entrant. It is said that "[n]umerous giant resource-rich companies have let early movers test the market and then, with positive signals, have dwarfed the earlier entrants by developing incomparable resources."[282] We can hardly say that states without offensive cyber capability, let first movers like the United States and Russia, 'test the waters'. Yet, there may be several minor information advantages when it comes to organizational development. For example, it is unlikely that Germany's establishment of a cyber command would be so encompassing if it was the first actor to establish this type of organization.

Technology shifts are said to be the second possible source for latecomers' advantage. New technology has the greatest potential to disrupt the competitive landscape when it makes the incumbent's acquired competencies obsolete - creating a potentially new level playing field.[283] This vulnerability of early entrants is often enhanced by, what the literature refers to as, 'incumbent inertia', i.e. a firm's inability to respond to environmental change or competitive threats. Lieberman and Montgomery list three root causes for this type of inertia. The firm may be: i) locked-in to a certain set of fixed assets (due to investment costs etc.); ii) reluctant to cannibalize existing product lines; iii) and become organizationally inflexible.[284] Perhaps the most significant technological shifts we will witness in the near future follow from Artificial Intelligence (AI). Yet, there is no reason to assume that states like China and the U.S. would be reluctant or too inflexible to invest in this new technology.

[280] Also, these leakages are particularly significant given the set-up of U.S. hacking capabilities as described above. As said, the U.S. maintains a heavy 'tool-based' rather than 'labour-based' offensive cyber capability set up. In other words, it suggests that certain states are more vulnerable to information spill-overs than others.
[281] Also see the discussion on Shamoon in chapter 4.
[282] Cho et al., "Latecomers Strategies"
[283] Ibid
[284] Ibid

3.4 Conclusion

The purpose of this chapter was to investigate current landscape of cyber proliferation. It helps to provide empirical base to render theoretical explanations of states' behaviour in later chapters. I distinguished between four stages of cyber proliferation; no discernible activity, exploration, pursuit and acquisition of cyber weapons. I argued that no more than forty states have *explored* the development of cyber weapons. In turn, the group of states that is *pursuing* cyber weapon is below thirty, and there are no more than a dozen states across the globe which actually seem to have *acquired* cyber weapons.

In the second part of the chapter I showed that there is significant variation in the ability of states to conduct sophisticated cyber operations, reliance on proxy actors, and the organizational integration of offensive cyber capabilities. Also, although several states are investing a significant amount of money in cyber weapons, the majority of cyber commands across the world have a rather small budget.

The final part of this chapter discussed the effects of 'order of entry' when it comes to cyber proliferation. An assessment of early movers and latecomer advantages helped to assess whether the global process of offensive cyber capability development has a bias towards convergence or divergence. Whereas few of the conventional early mover advantages seem to exist for the development of cyber weapons, the most significant latecomer advantage may come from free-rider effects (through information leakages).

Chapter 4: Supply-Side: What it Takes to Develop Cyber Weapons

4.1 Introduction

"I am informed that within 20 minutes the seven of you could make the internet unusable for the entire nation is that correct?"[285] This was the first question Senator Fred Thompson asked grey-hacker group LOpht when they testified in front of U.S. Congress in May 1998. One of the hackers, Mudge, corrected the Congressman; "actually any one of us can do it in 30 minutes."[286] The Congressman followed up by asking, "what if a foreign government would hire seven individuals like you. What harm could they do to the US? [...] What would the effects be?" Without raising their voices the "hacker think tank from Boston Massachusetts", as the group was officially named, sketched out various scenarios: there is the option to bring down the phone system or the electricity net, take down the financial markets, or jam satellite communication. Overall, the group affirmed that it is "easy to cause major havoc."[287]

Today, policymakers offer remarkably similar warnings about the ease with which to conduct a successful cyber operation with major consequences. In 2009, when a reporter asked former director of the NSA and National Intelligence, Mike McConnell, how easy it was to bring down the power grid, he said that a sophisticated hacker could "sack electric power on the U.S. East Coast, maybe the West Coast, and attempt to cause a cascading effect."[288] The most widely cited statement is from Leon Panetta: that the U.S. is facing the possibility of a "cyber-Pearl Harbor", as "a destructive cyber terrorist attack could paralyze the nation."[289] Overall, there is a strong sense that cyber weapons empower weaker actors; the idea is that just a few hackers with a sufficient supply of Club Mate can wage a cyber war.[290]

---

[285] YouTube, "Hackers Testifying at the United States Senate, May 19, 1998 (L0pht Heavy Industries)," retrieved from: https://www.youtube.com/watch?v=VVJldn_MmMY
[286] Ibid
[287] Ibid
[288] CBS News, "Cyber War: Sabotaging the System," (2009, November 6), Retrieved from: http://www.cbsnews.com/news/cyber-war-sabotaging-the-system-06-11-2009/
[289]Steven Musil, "Pre-emptive cyberattack defense possible, Panetta warns," *CNET* (2012, October 11), Retrieved from: http://www.cnet.com/news/pre-emptive-cyberattack-defense-possible-panetta-warns/
[290] As Kissinger also reflects, "[a] laptop can produce global consequences. A solitary actor with enough computer power is able to access the cyber domain to disable and potentially destroy critical infrastructure form a position of near complete anonymity. Electric grids could be surged and power plants disabled through actions undertaken exclusively outside a nation's physical territory." See: Henry Kissinger, *World Order: Reflections on the Character of Nations and the Course of History*, (London: Penguin Books: 2015), p. 345

But, is it really that easy? What obstacles do actors have to overcome to develop a cyber weapon? Can small states take down critical infrastructure with a cyber attack? If it is not possible today, will it be possible in the future? Experts disagree about the capabilities of actors in cyberspace, let alone agree on their future capability.

To address these questions, this chapter focuses on the supply-side of cyber proliferation. The supply-side looks at the total set of obstacles and possibilities that are available within an environment to develop different types of cyber weapons.[291] The rational for looking at the supply-side is intuitive: states can only develop offensive cyber capabilities if they possess the necessary resources. Stephen Meyer's work on *the Dynamics of Nuclear Proliferation* was a breakthrough study on nuclear proliferation.[292] Previous research primarily concentrated on states which had (almost) acquired the bomb. Such analyses, however, suffered from a selection bias as many states developed their nuclear infrastructure precisely to acquire nuclear weapons.[293] To test the supply-side imperative, Meyer therefore used the concept of 'latent capacity' to denote a state's *potential* nuclear capacity rather than *current* capacity. It has now become common practice to analyse states' latent capacity to avoid unfairly tipping the scales in favour of the supply-side hypothesis. Here, I coin the term 'cyber latency' to describe how quickly a state, starting from different levels of cyber-related expertise, technology and political commitment can develop a cyber weapon if they chose to do so.[294]

The notion underlying the supply-side imperative is that once a state acquires the *latent* capability to develop a cyber weapon, it will be compelled to also develop an operational capability and 'go cyber'.[295] Following this imperative, it can be said that more states will acquire cyber weapons following three developments; i) technological or political advancement within a state allows it to cross the latent cyber capacity threshold and makes the development of cyber weapons feasible; ii) the sophistication required to develop cyber weapons decreases, lowering the overall latency threshold, compelling offensive cyber activity; iii) states are able to acquire (parts of) cyber weapons from other actors, enabling development.

---

[291] Adapted from Most and Harvey Starr, *Inquiry, Logic and International Politics*
[292] Stephen Meyer, *The Dynamics of Nuclear Proliferation*, (Chicago: Chicago University Press: 1984)
[293] Ibid. Jacques E. C. Hymans, "Theories of Nuclear Proliferation"
[294] Also see Sagan's original formulation of the question on nuclear latency, leaving out political commitment. Sagan, "Why Do States Build Nuclear Weapons?"
[295] Both more extreme and more moderate deterministic statements can be formulated following this notion on the timing and inevitability of the decision. The more extreme view is that, the decision to 'go cyber' directly follows the acquirement of latent capability (i.e. both timing and decision are direct and inevitable). A less strong version is that although the decision itself is inevitable, the timing may be probabilistic. The most moderate version is that the greater degree of cyber latency makes it more likely a state develops cyber weapons. Also see: Meyer, *The Dynamics of Nuclear Proliferation*, p. 9-12

The supply-side analysis is conducted in the following steps. Section 4.2 identifies in which (known) cyber campaigns a cyber weapon has been used. I deploy a new dataset called *the Cyber Operations Dataset* which offers information on the date, threat actor, target, intent and sophistication of the main cyber operations since the Morris Worm. In section 4.3 I look at the development costs of the identified cyber weapons on a case-by-case basis. Section 4.4 addresses potential areas of cost reduction with respect to cyber weapons. Section 4.5 looks at the incentives for transferring cyber weapon technology. The final part, section 4.6, concludes.

4.2 Identifying Cyber Weapons: Looking for a Needle in a Haystack

Chapter 2 laid the conceptual groundwork of this thesis and discussed the meaning of a cyber weapon. Cyber weapons were defined as a capability designed to access a computer system or network to damage or harm living or material entities. Yet, to move from a *definition* of cyber weapons to the *identification* of cyber weapons is a meticulous exercise. Numerous incidents occur on a daily basis, yet in few cases the intention of the attacker is to cause harm or damage.

Hence, before we can delve into the costs of each type of cyber weapon, we need to acquire a better overview of the population of cases in which an actor used a cyber weapon. The *Offensive Cyber Operations Dataset*, as discussed in chapter 1, serves to help with this assessment. The dataset includes all cases on which a public report was written by a reputable cyber security firm.[296]

The key benefit of this selection criterion is that a more accurate (although still not perfect) assessment of the attack's sophistication is possible. Instead of relying on statements from policymakers or other actors about the sophistication of attacks, it allows for an analysis of the technical parameters listed in the report.[297] This approach, however, also comes with several limitations.[298]

Figures 4.1- 4.3 summarize the data. The figures classify the cases based on 'date of disclosure' (x-axis) and 'level of sophistication' (y-axis). I use 'date of disclosure' instead of 'date of exploit' because we often do not know when the system was first compromised.[299] Figure 4.1 summarizes the

[296] More information about the dataset can found in Appendix 1.
[297] Here I also differ from Valeriano and Maness' project. The scholars rely on media reports and general statements from various officials (directors of a firm, policy-makers, academics, or other analysis) to code their cases. No method is provided to assess the validity of these statements (nor does the codebook provide any guidance in case there is no consensus about sophistication between, for example, two policymakers/experts). For additional critique on the dataset of Valeriano and Manness see chapter 5.
[298] For a more extensive discussion on the caveats and limitations see Appendix 1.
[299] The average time for APT discovery is 3.5 years. One of the more extreme examples is Equation group. The complex cyber attack platform was disclosed in 2014 but it first known sample originates from 2002. See: Kaspersky Lab, "Equation Group, Questions and Answers," Version 1.5 (2015, February) Retrieved from:

offensive cyber operations between 2010 and 2016. Figure 4.2 does the same for the period between 2001 and mid-2010. And figure 4.3 captures the early cases between 1986 and 2002. All the cases above the x-axis in the figure are considered to be Advanced Persistent Threats (APT). APT is an frequently used term to refer to the most sophisticated type of attacks. According to Kaspersky, "[t]he 'ecosystem' of malware breaks down into known threats (70%), unknown threats (29%) and advanced threats (1%)."[300]

The earliest cases included concerns the Cuckoo's Egg (CUE) and the Morris Worm (MOW). The most recent offensive cyber operations listed are the 'Ukrainian Artillery Units' attack (UAU) and Pointed Dagger Attack (PDA), both discovered in 2016.

The recent spike in the disclosure of APTs cannot go unrecognised. As the figures show, since 2010, the number of APTs discovered by anti-virus firms has inflated.[301] There are a number of reasons which might explain this trend. The first is that actors seem to get increasingly more organized. Whereas in the 1990s, the activities of script kiddies and hobbyists were often headline news and able to guide scholarly debate on the future of cyber attacks, they do increasingly less so. Also, improvements in cyber defence inherently means that attackers have to develop new methods to exploit the target's computer systems. Finally, it should be noticed that is a more intense effort made by cyber security firms to discover and report new vulnerabilities. Cyber firms can gain a real reputational boost if they are the first to unveil a new type of cyber platform.[302]

What the figures do not show is that most cyber attacks directed their efforts against multiple entities instead of focusing on one target. Exceptions include the attack on the German steelworks facility (GSF), Stuxnet (STU), Hacking Scientology (HAS), and My Doom (MYD).

---

https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf, p. 18; The average is calculated using data from: Kaspersky Lab, "Targeted Cyberattacks Logbook." (2016), Retrieved from: https://apt.securelist.com/

[300] The majority of attacks are relatively easy to defend against with traditional tools. The unknown threats can be dealt with too if methods are used going beyond stand anti-virus software - such as heuristics and dynamic whitelisting. Yet, the highly advanced attacks, the 'one percenters', can remain undetected for multiple years due to their sophistication. See: Kaspersky Lab, "Future Risks: Be prepared: Special Report on Mitigation Strategies for Advanced Threats," (2015, May), retrieved from: http://media.kaspersky.com/en/business-security/APT-Report.pdf?icid=en-GL:ent-gallery

[301] Technical investigation of the malware has shown numerous linkages- in terms of the way the code is written or type of vulnerability exploited - between the different incidents. For example, most recent: CozyDuke linked to MiniDuke and Cosmic Duke. Duqu 2.0 linked to MiniFlame, Gauss, Flame, Stuxnet, Duqu. Cloud Atlas linked to Red October. Epic Turla linked to Turla.

[302] And as said, this also means that firms have an incentive to exaggerate some of the threats in order to promote their own detection capabilities. Also see: Robert M Lee and Thomas Rid, "OMG Cyber!," *The RUSI Journal,* 159:5 (2014)4-12

Figure 4.1: Reported Offensive Cyber Operations, over time (2010-2016)

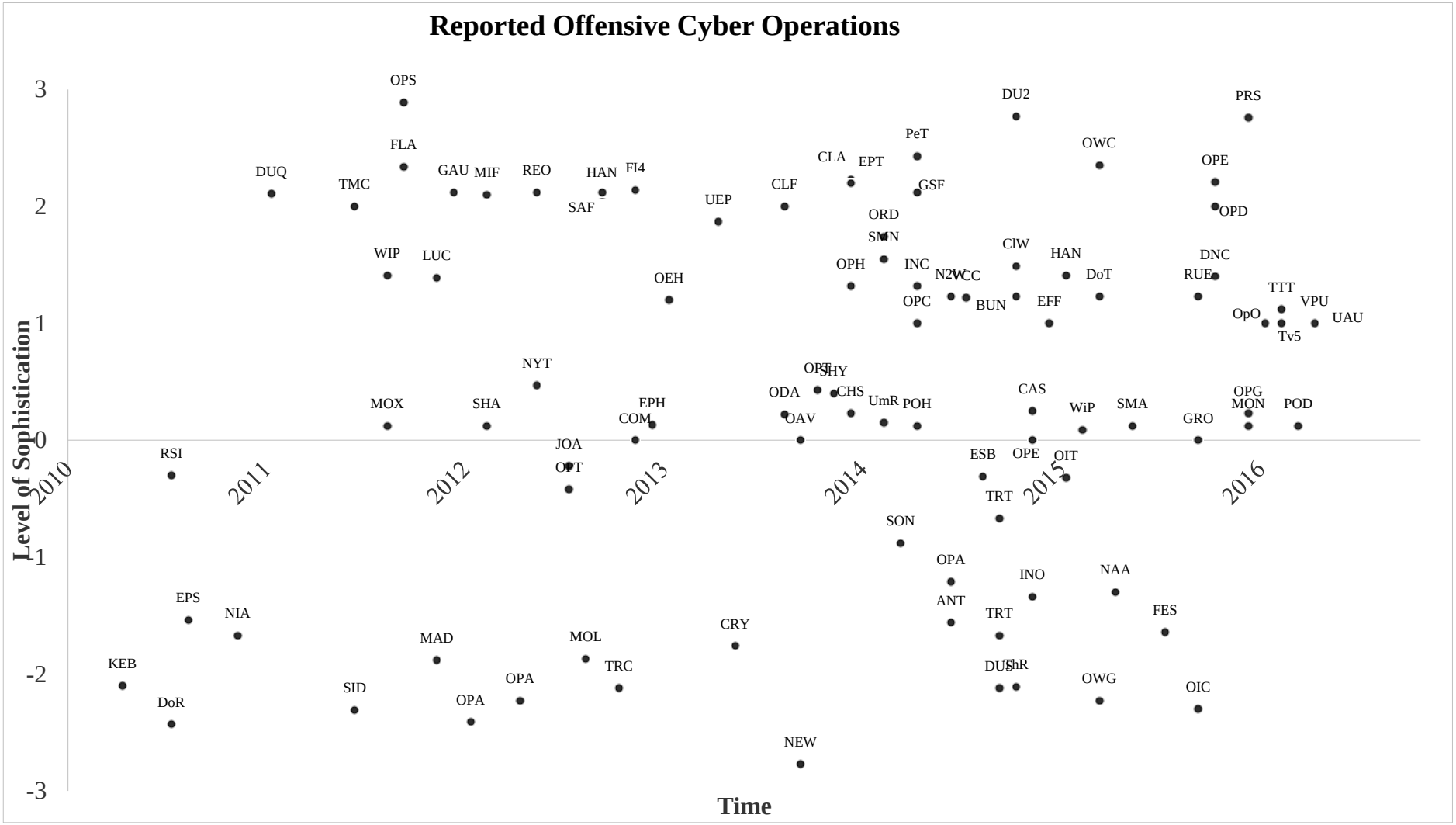


Figure 4.2: Reported Offensive Cyber Operations, over time (2001-2010)

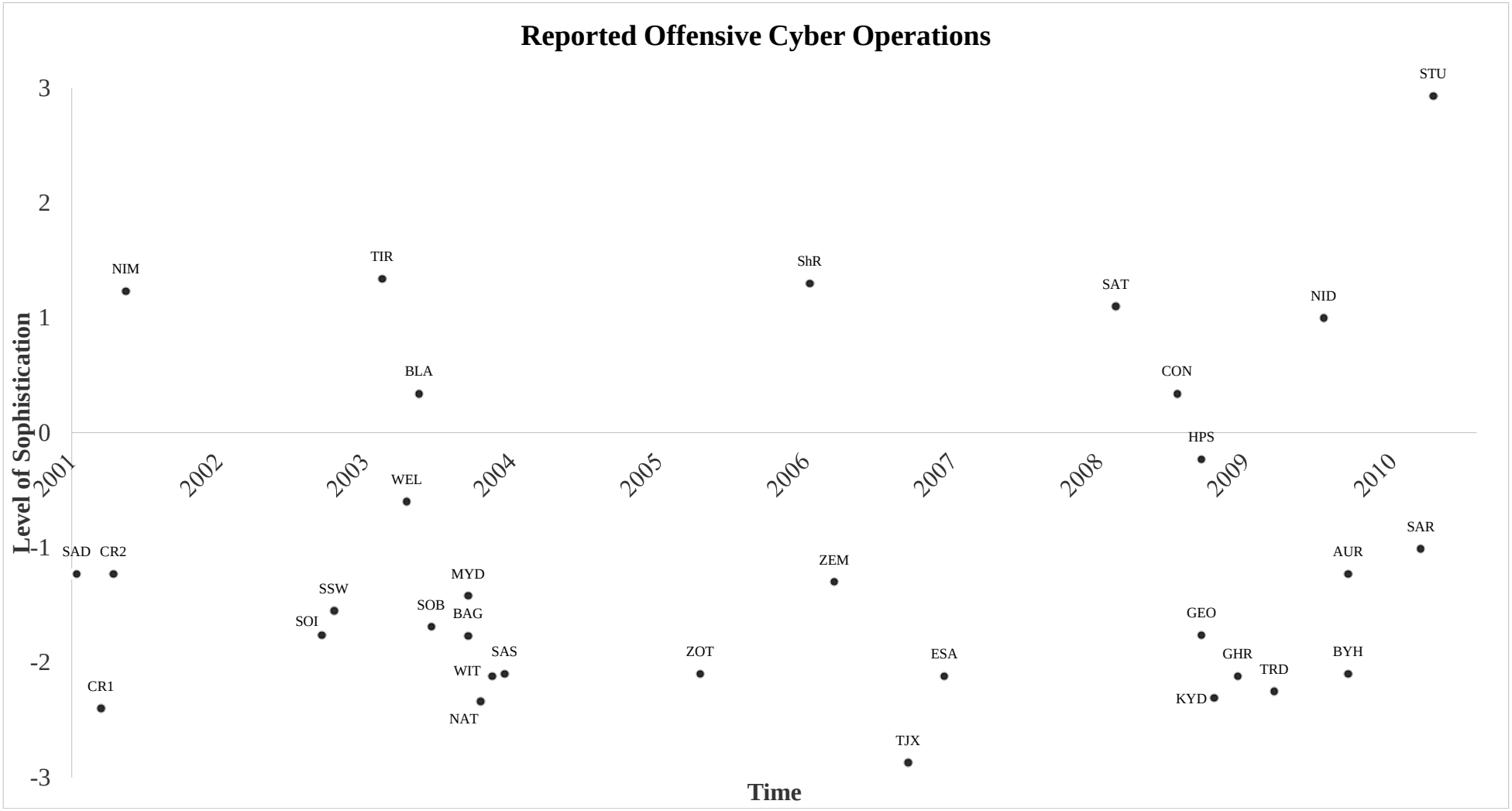
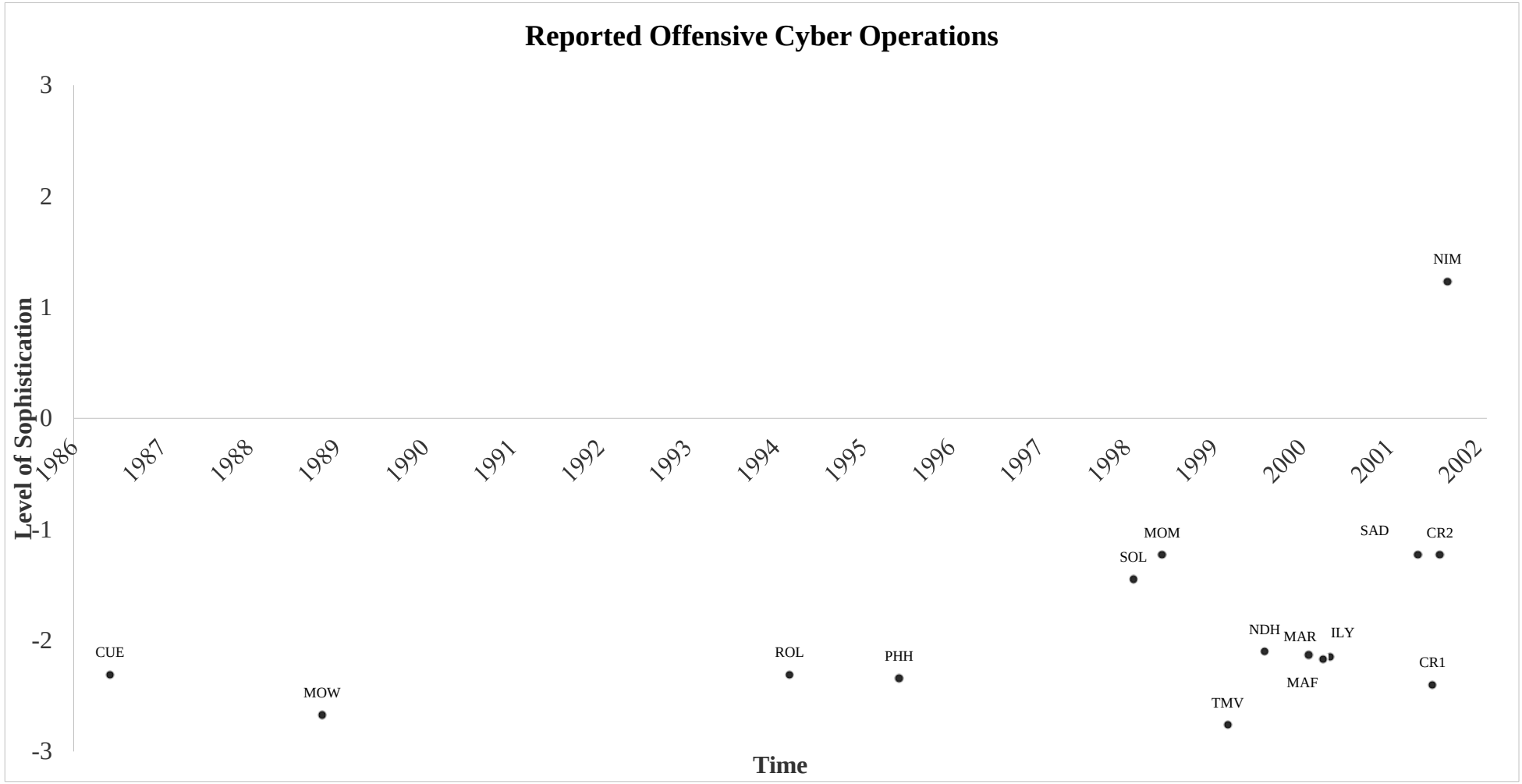


Figure 4.3: Reported Offensive Cyber Operations, over time (1986-2002)



4.3 Case Studies of Cyber Weapons' Development Costs

A key observation following Figure 4.1 - 4.3 is that the use of cyber weapons has been rare relative to the use of espionage capabilities.[303] Most of the cases in which a cyber weapon has been used have already been discussed in relation to their disruptive or destructive impact. However, only a few of these cases have been (systematically) evaluated with respect to the resources required to produce them. To facilitate further discussion on this aspect, table 4.1 provides an overview of the cyber weapons categorized based on their level of sophistication. The categories are based on Bellovin, Landau and Lin's study on the collateral damage of cyber weapons.[304]

Table 4.1: Cyber Weapon Cases based on Level of Sophistication

Type	Classification	Cases
Type I	DDoS attacks	Estonia (2007), Hacking Scientology (2008), Kyrgyzstan (2009), Georgia (2009), Black DDoS (2010), OPI Israel (2012), Operation Adabil (2012)
Type II	Data removals / Wipers	Witty Worm (2004), Narliam (2008), Dozer (2009), Koredos (2010), Shamoon (2012), Groovemonitor (2012), Jokra/Dark Seoul (2013), Destover/Sony (2014), Tv5 monde (2016)
Type III	Physical destruction	Stuxnet (2012), German Steelworks Facility Attack (2014), Ukraine attacks (2015)

4.3.1 DDoS Attacks: Cyber Weapon on the Cheap

Many of the 'Type I' cases have received widespread attention in the media and also triggered new policy initiatives due to their high visibility. Particularly, the events in Estonia, following the government's decision to move a 6-foot-tall bronze statue commemorating the Soviet defeat of Nazi Germany from the city centre to a cemetery located at the outskirts of Tallinn, have led governments

[303] The dataset suffers from an inherent collection bias in that only *reported* events are listed. We do not know how much we do not know; many exploits currently going on are likely still undiscovered. Yet, notice that this bias only reinforces the statement above as a destructive cyber attack is more likely to be discovered compared with a cyber espionage operation.

[304] Steven M. Bellovin, Susan Landau, and Herbert S. Lin, "Limiting the undesired impact of cyber weapons: technical requirements and policy implications," *Journal of Cyber Security*, 3:1 (2017):59-68

and international organizations to review their ability to respond to threats from cyberspace. Some have even denoted these events as a form of "cyber warfare".[305]

The attacks, however, are characterized by a low level of sophistication and led to a minimum amount of damage or harm. OPI Israel, intending to "erase Israel from the internet" and claiming to have caused more than $3 billion in damage, in reality was able to only deface one website for several hours.[306] It has proven difficult for Anonymous, an organization eschewing a hierarchical structure, to cause damage to a country's infrastructure following this type of attack. The Georgian attacks - coinciding with the Russian invasion - led to a degradation of certain websites and caused the National Bank of Georgia to stop offering electronic services for a few days.[307] Yet, the disruption was of a short duration - particularly after international support was provided to effectively counter the surge.[308]

What are the costs of mounting these types of attacks? A commercialization of botnet operators has taken place over the last decade. The costs of buying or hiring a botnet depends mainly on the bandwidth of the attack and its duration.[309] In 2007, Vicente Segura and Javier Lahuerta surveyed forums where these services can be bought.[310] It was found that for U.S. $75, one can hire a DDoS Service for 24 hours with a bandwidth of 100 Mbps. A more serious botnet with a bandwidth of 1000Mbps, will cost U.S. $100 to hire for 24 hours. Finally, hiring a DDoS service for a week at a bandwidth of 4570 Mbps costs in the region of U.S. $5500. Since 2007, the price has been falling for these services.[311] Today, you would pay more than $50 for an hour of 1000Mbps.[312]

---

[305] For example: Jenik Aviram, "Cyberwar in Estonia and the Middle East," *Network Security*, 4 (2009)4-6

[306] Steven Musil, "Anonymous targets Israel in another cyberattack," *CNet*, (2013, April 7), retrieved from: http://www.cnet.com/news/anonymous-targets-israel-in-another-cyberattack/

[307]According to one study, the disruption of the Georgian Central Bank and the government communications tactically benefited the Russian military incursion. See U.S. Cyber Consequences Unit (US-CCU), "Overview by the US-CCU of the Cyber Campaign against Georgia in August 2008," *Special Report, US-CCU*, (2009, August), retrieved from: http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf.

[308] Joshua Davis, "Hackers take down the most wired country in Europe," *Wired*, (2008, August 21), retrieved from: https://www.wired.com/2007/08/ff-estonia/

[309] There are also differences in price when you have to buy the complete botnet including command & control as well as zombies, or whether you merely need 'shells' because you have your own Remote Access Trojan Controller.

[310] Vincente Segura and Javier Laheurta, "Modelling the economic incentives of DDoS attacks: femtocell case study," (paper presented at the Workshop on the Economics of Information Security (WEIS), University College London, England, 24-25 June 2009) retrieved from: http://weis09.infosecon.net/files/113/paper113.pdf

[311] Ibid.

[312] Arbor Networks, "The Risk vs. Cost of Enterprise DDoS Protection How to Calculate the ROI from a DDoS Defense Solution," White Paper (2014), retrieved from: https://enterprise.brighthouse.com/content/dam/bhn/ent/resources/whitepapers/wp-TheRiskvsCostofENTDDoSProtectionWhitePaper.pdf

4.3.2 Data Removals: Getting the most Bang for your Buck

The Witty worm and the other wipers are considered to be 'type II' cases, characterized by a relatively low level of sophistication but having caused a relatively high level of damage. A number of excellent technical accounts exist on Witty, the worm that was so successful in effecting its target population of computer systems. "Twelve thousand machines was the entire and exposed population," as Bruce Schneier writes, "and the Witty worm infected them all in just 45 minutes."[313] This is an impressive feat, especially considering the short time period in which the worm was written. On March 8th 2004, eEye Digital Security discovered an easily exploitable buffer overflow vulnerability in the BlackICE/RealSecurity Products of Internet Security Systems (ISS).[314] Having been informed about it by eEye, ISS released a patch the day after. On the 18th of March, eEye published a detailed report on the vulnerability. Less than 48 hours after publication, the Witty worm started to spread across the internet.[315]

Nicholas Weaver and Dan Ellis have well-documented the cleverness and the nastiness of the malicious code:

> Witty [...] was an architecturally simple worm [it was less than 700 bytes long]. [...]Although simple, the execution was superb. There were no significant bugs […], avoiding common mistakes. The malicious payload, slowly corrupting the drive, causes immediate damage but does not significantly slow the worm's spread, while randomizing the destination port makes the worm more likely to penetrate firewalls. [Also,] the author seeded the worm [to ensure the worm spreads even faster]. Rather than just starting at a single location, the worm started out on over 110 different victims.[316]

Although we still do not know the author of the worm, several things can be said about the required development costs. Given the way the worm was constructed, it must have required at least the following three aspects. First, the author was a highly skilled coder. Weaver and Ellis assume it was just *one* coder, but there is no reason to suggest we can be certain of this - particularly because of the short release time. Second, as Witty was bug-free, the code was likely tested before. Although theoretically it is possible to write a code without errors in one go, it is more likely that the worm was tested before. The testing does not require a significant capability; one only needs a couple of systems to monitor the network traffic on the test systems. Third, the author(s) must have been well-connected

[313] For full technical account see: Nicholas Weaver and Dan Ellis, "Reflections on Witty: Analyzing the Attacker," *Security*, 29:3 (2004) 34-37
[314] The company ISS was acquired by IBM in 2006.
[315] The possibility that the attacker knew about the vulnerability before the report cannot be discarded.
[316] Ibid

to the hacking environment to seed the attack with 110 computer systems. As Weaver and Ellis write, "[t]he use of previously compromised machines requires that the attacker either obtained access to 110 machines using a different tool, already had access to 110 machines, or took control of these machines from a third party. Thus, Witty's author probably possessed some ties to the [hacker community], to gain access to these machines in the short time frame."[317]

There are a number of other cases which have been similar in payload, but they have generally been more targeted than Witty. The incident dubbed Wiper came to light in late April 2012 when the New York Times published a story that a mysterious malware attack was shutting down computer systems at businesses throughout Iran. The attack was confirmed by a spokesman from the Iranian Ministry of Petroleum. He was, however, quick to insist that Wiper caused no permanent damage as a backup of essential and non-essential data was maintained.[318]

The mystery surrounding the attack came from the fact that no one had obtained a sample of the virus to study its code and determine exactly what it did to machines in Iran. The International Telecommunications Union (ITU) asked Kaspersky Lab to investigate the nature of the malware. After several months of research, having obtained mirror images of a number of hard drives that had been hit by the malware, the security firm concluded that: "[t]he malware was so well written that once it was activated, no data survived. So, although we've seen traces of the infection, the malware is still unknown because we have not seen any additional wiping incidents that followed the same pattern as Wiper, and no detections of the malware have appeared in the proactive detection components of our security solutions."[319] The malware contained a carefully designed wiping algorithm to destroy data as effectively as possible. To reduce the chances of discovery, Wiper likely first destroyed the malware components, and only then systematically erased system files causing the systems to crash and be unable to reboot.[320] The identity of the attacker remains a matter of speculation, although possible connections have been found with Duqu and Stuxnet, suggesting the U.S. might be behind it.[321]

---

[317] Ibid, p.36-37
[318] Kim Zetter, "Wiper Malware that Hit Iran left Possible Clues of its Origins," *Wired*, (2012, August 29), retrieved from: https://www.wired.com/2012/08/wiper-possible-origins/; also cited in Rid, *Cyber War Will Not Take Place*
[319] Kaspersky Lab, "What was that Wiper thing?," (2012, August 29), retrieved from: https://securelist.com/blog/incidents/34088/what-was-that-wiper-thing-48/
[320] Ibid
[321] As Kaspersky states "[i]nteresting enough, on some systems we noticed that all PNF files in the INF Windows folder were wiped with a higher priority than other files. Once again, this is a connection to Duqu and Stuxnet, which kept their main body in encrypted ".PNF" files." Ibid

About a year later, General Keith Alexander, director of the National Security Agency (NSA) and commander of U.S. Cyber Command, met up with Sir Iain Robert Lobban, Director of UK's Government Communications Headquarters (GCHQ).[322] The talking points of the meeting prepared by the NSA were leaked by Edward Snowden. The top-secret document states that:

> Iran continues to conduct distributed denial-of-service (DDOS) attack against numerous U.S. financial institutions […]. NSA expects Iran will continue this series of attacks, which it views as successful, while striving for increased effectiveness by adapting its tactics and techniques to circumvent victim mitigation attempts. […] Iran's destructive cyber attack against Saudi Aramco in August 2012, during which data was destroyed on tens of thousands of computers, was the first such attack NSA has observed from this adversary. Iran, having been a victim of a similar cyber attack against its own oil industry in April 2012, has demonstrated a clear ability to learn from the capabilities and actions of others.[323]

The last sentence refers to the Wiper attack. The malicious software, which struck Saudi Aramco, is known as Shamoon, named after a folder name in one of the strings. Shamoon attacked the hard drives of 30,000 workstations owned by the Saudi oil firm. Like Wiper, Shamoon was designed to destroy data. The payload overwrites the segment of a hard drive responsible for rebooting the system as well as the partition table and most files with random data, including a small segment of an image that allegedly shows a burning American flag.[324] Although Shamoon did not cause physical damage to the production facilities of the oil company, the damage was significant. Saudi Aramco reportedly needed weeks - if not months - to recover from the attack, hiring six computer security firms to help with the post-attack clean up and forensic investigation.[325] Later that month, a number of reports were published that Qatari RasGas was hit with the same wiper attack.[326]

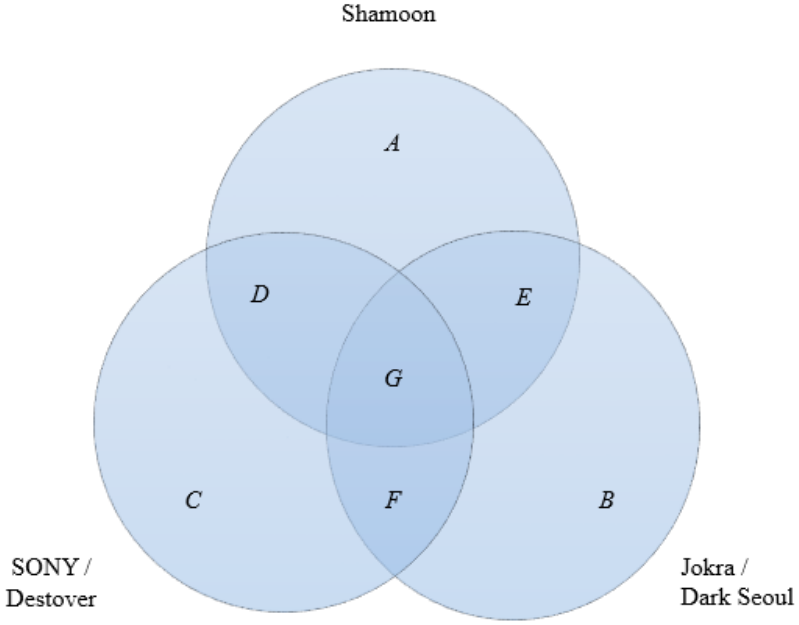
These cases seem to be part of a broad trend of malware with a destructive functionality. Narilam (2008) and Groovemonitor (2012) are similar pieces of malware that have mostly targeted entities in the Arabian Peninsula. Dozer (2009), Koredos (2010), Jokra (2013), and Destover (2014) have been prominent cases in the Korean Peninsula. What all these cases have in common is that they have not

[322] NSA, "Iran - Current Topics, Interaction with GCHQ," (2013 April 12), Retrieved from: https://www.eff.org/files/2015/02/21/20150210-intercept-iran_current_topics_-_interactions_with_gchq.pdf
[323] Ibid
[324] See: Symantec Security Response, "The Shamoon Attacks," *Symantec Official Blog* (2012, August 16), retrieved from: http://www.symantec.com/connect/blogs/shamoon-attacks
[325] See Rid, *Cyber War Will Not Take Place*
[326] There are a number of reports that the computers at RasGas were affected as well. See: Kim Zetter, "Qatari Gas Company Hit with Virus in Wave of Attacks on Energy Companies," *Wired*, (2012, August 30) Retrieved from: http://www.wired.com/2012/08/hack-attack-strikes-rasgas/

been very sophisticated, yet highly effective. No damage to physical production facilities was caused, yet the operational costs due to wiping of disk drivers was considerable.

Numerous intelligence firms have usefully shown the technical linkages between these attacks - generally focusing on Shamoon, Destover/Sony, and Jokra/DarkSeoul. I have summarized these links in the figure below. These reports mainly focus on *how* actors can learn from each other. It is similar to the type of learning of athletes trying to copy techniques of other outstanding sports(wo)men. At a tennis academy a coach might show a series of slow-motion videos of Roger Federer's outstanding single-handed backhand. Players will analyse these videos with as aim to improve their own technique. It is also the type of learning we generally refer to in scholarly discussion as the diffusion of capabilities.

Figure 4.2: Connections between Shamoon, Jokra and Destover



A. *Shamoon's main targets were in the Arab Peninsula (like Narilam and Groovemonitor).*
B. */*
C. *The Destover malware lacked *nix scripts necessary to erase partitions across Linux systems.*
D. *i) The droppers' resource section contained the wiper drivers for both capabilities; ii) both Shamoon and Jokra vaguely encoded political messages were used to overwrite disk data and the master boot record.*
E. *i) Main targets were in South Korea; ii) shared files name; iii) used the same internal web server to display messages on affected computer screens; iv) and used the same colour and messaging schemes.*
F. *i) All were destructive pieces of malware; ii) lacked technical sophistication; iii) did not affect critical infrastructure systems; iv) were politically motivated; v) configured to perform a delayed wipe; vi) used the commercially available RawDisk library from Eldos for disk hardware access; vii) groups claiming credit for intrusion had no prior (hacking) history or real identity.*[327]

[327] Symantec, "Are the 2011 and 2013 South Korean Cyberattacks Related?", (2013, March 29), retrieved from: www.symantec.com/connect/blogs/are-2011-and-2013-south-korean-cyberattacks-related; Choe Shang Hun and John Markoff, "Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea," *The New York Times*, (9 July 2009), retrieved from: www.nytimes.com/2009/07/technology/10cyber.html?_r=0; Symantec, "Four Years of

However, we should notice that these cases might at least partially embody a second type of learning as well: learning *that* something is possible. On 6 May 1954 Roger Bannister was the first person to ever run a mile under four minutes at Iffley Road track in Oxford with a time of 3 minutes and 59.4 seconds (he did so with relatively little training). What is interesting is that once Bannister debunked the widely propagated myth that a four-minute mile was impossible, it changed the mind-set of all the other athletes. This psychological dimension, *the awareness of an achievable target*, meant that it did not take long before many others would run below 4 minutes as well. In fact, Bannister's record lasted just 46 days, after which John Landy ran a time of 3:57.9 in Finland.

4.3.3 Physical Destruction: Crossing the Rubicon [328]

Former NSA and CIA director, Michael Hayden, said in 2012 that someone "crossed the Rubicon", referring to Stuxnet - the worm caused physical damage to Iran's nuclear centrifuges in Natanz.[329] The worm first came to light in June 2010, when Sergey Ulasen, heading an antivirus division of a relatively unknown security firm in Belarus, VirusBlokAda, stumbled upon it when analysing the computer of a customer in Iran.[330] Stuxnet was allegedly the brainchild of the United States and Israel.

DarkSeoul Backscatters Against South Korea Continue on Anniversary of Korean War," (2013, June 26), retrieved from: www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war; Symantec, "W32.Distrack," (2012, August 22), retrieved from: www.symantec.com/security_response/writeup.jsp?docid=2012-081608-0202-99; Novetta, "Operation Blockbuster: Unravelling the Long Thread of the Sony Attack," (2014, December 4), retrieved from: www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf; Dimitry Tarakanov, "Shamoon The Wiper: Further Details," (2012, September 11), retrieved from https://securelist.com/blog/incidents/57784/shamoon-the-wiper-further-details-part-ii/; Kurt Baumgartner, "Sony/Destover: mystery North Korean actor's destructive and past network activity: Comparisons with Shamoon and DarkSeoul," (4 December 2014), retrieved from: https://securelist.com/blog/research/67985/destover/; Jim Finkle, "Exclusive: FBI warns of 'destructive' malware in wake of Sony attack," *Reuters*, (2014, December 2), retrieved from: www.reuters.com/article/us-sony-cybersecurity-malware-idUSKCN0JF3FE20141202; Ryan Sherstobitoff, Itai Liba, and James Walter, "Dissecting Operation Troy: Cyberespionage in South Korea," McAfee, (2013, March 20), retrieved from: www.mcafee.com/it/resources/white-papers/wp-dissecting-operation-troy.pdf

[328] I decided to only focus here on Stuxnet and leave out a discussion on the Ukrainian attacks and the German Steel Mill attacks. On the former, there is however a significant amount of information available about the sophistication and costs of the attacks. On the latter, it remains unclear if the damage was actually caused by a cyber attack. See: Kim Zetter, "Everything We Know About Ukraine's Power Plant Hack," *Wired*, (2016, January 20), Retrieved from: https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/; Kaspersky Lab, "BlackEnergy APT Attacks in Ukraine employ spearphishing with Word documents," *Securelist*, (2016, January 28), retrieved from: https://securelist.com/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/73440/ ; Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, (2016, March 3), retrieved from: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[329] CBS News, "Fmr. CIA head calls Stuxnet virus 'good idea," *60 Minutes*, (2012, March 1), Retrieved from: http://www.cbsnews.com/news/fmr-cia-head-calls-stuxnet-virus-good-idea/

[330] When the firm posted about it a month later, other security firms soon started to inspect the worm as well - all were quick to realize that the code was too sophisticated to be designed by a loosely affiliated group of hackers. Yet, it was Liam Murchu, working for Symantec, who was the first to notice that Stuxnet was much more complex and sophisticated than just a skilled industrial espionage case. See: Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History"

Ralph Langner points out that Stuxnet is actually not one weapon, but two.[331] The earliest version is also referred to as Stuxnet 0.5, and was in development prior to November 2005.[332] This early version is considered to be the most sophisticated of the two, focusing on closing the isolation valves of the Natanz uranium enrichment facility.[333] The later, better-known version followed a different modus operandi as it aimed to change the speeds of the rotors in the centrifuges.

The later Stuxnet was the old version on steroids.[334] As Langner writes, "[a]ll of a sudden, Stuxnet became equipped with the latest and greatest MS Windows exploits and stolen digital certificates as the icing on the cake, allowing the malicious software to pose as legitimate driver software and thus not be rejected by newer versions of the Windows operating system".[335] This worm took advantage of four zero-day vulnerabilities in its exploitation of both the Windows platform and the Siemens systems - two of those zero-days were used to escalate privilege on the compromised systems.[336] It also used various propagation techniques, via infected removable drives, local area network communications, as well as infected Siemens project files. Within these three propagation mechanisms, Stuxnet utilized at least seven different vulnerability exploitation techniques for spreading to new computers in a system.[337] Furthermore, to avoid suspicion, the driver files were digitally signed with two compromised digital certificates.[338]

What means are required to develop a Stuxnet-like capability, the most sophisticated cyber weapon to date? Costin Raiu, former Director of Kaspersky's Global Research and Analysis Team, estimates that it would costs in the region of $100 million to develop Stuxnet.[339] This seems to be an extremely conservative figure considering the costs of additional intelligence gathering, infiltration, and above all for testing. The complexity of the worm means that thorough testing was required to see whether

---

[331] Ralph Langner, "Stuxnet's Secret Twin," *Foreign Policy*, (2013, November 19), retrieved from: http://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/ ; Ralph Langner, "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve," The Langner Group, (November 2013), retrieved from:http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf, p. 5

[332] Geoff McDonald, Liam O Murchu, Stephen Doherty, Eric Chien, "Stuxnet 0.5: The Missing Link," *Symantec*, (2013, February 26), retrieved from: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/stuxnet_0_5_the_missing_link.pdf

[333] Langner, "Stuxnet's Secret Twin"

[334] As Langner notes, it also comes at the cost of being less stealthy. Ibid

[335] Langner, "To Kill a Centrifuge," p. 11

[336] It also used a number of known vulnerabilities - for example, the 'Conficker' vulnerability was used to propagate through unpatched computers.

[337] Eric Byres, Andrew Ginter, Joel Langill, "How Stuxnet Spreads - A Study of Infection Paths in Best Practice Systems," Version 1.0, (2011, February 22), Retrieved from: http://www.abterra.ca/papers/how-stuxnet-spreads.pdf

[338] Falliere et al., "W32.Stuxnet Dossier"

[339] David Gilbert, "Cost of Developing Cyber Weapons Drops from $100M Stuxnet to $10K IceFog*," International Business Times*, (2014, February 6) retrieved from: http://www.ibtimes.co.uk/cost-developing-cyber-weapons-drops-100m-stuxnet-10k-icefrog-1435451

the bug could do what it was intended to do. The U.S. therefore had to produce its own P-1s, perfect replicas of the variant used by the Iranians at Natanz.[340] At first, small-scale tests were conducted borrowing centrifuges stored at the Oak Ridge National Laboratory in Tennessee, once taken from Muammar Qaddafi in late 2003 when he gave up the program.[341] The tests grew in size and sophistication - obtaining parts from various small factories situated all over the world. As Sanger reports, at some point the U.S was "even testing the malware against mock-ups of the next generation of centrifuges the Iranians were expected to deploy, called IR-2s, and successor models, including some the Iranians still are struggling to construct."[342]

Next to the amount of resources poured into Stuxnet, the required institutional infrastructure was at least as significant. The project was likely established under the Bush Jr. administration and continued when President Obama came to office, featuring collaboration with the Israelis. In those years, numerous new institutions were set up - both at the Defence Department and the NSA - to build up the required offensive cyber capacity. Jon Lindsay goes to great length to describe the great deal of planning and support to successfully implement Stuxnet:

> Planners needed expertise in computer science, ICS and nuclear engineering, and covert intelligence operations in order to hack into Natanz.[…] Intelligence preparation for Olympic Games in particular began years before the Stuxnet attack with cyber reconnaissance to map out Natanz's networks. [...]The actual human agents used for insertion may have been affiliated with the Mossad's proxy force in Iran, Mujahedeen-e-Khalq. […]The operation would further need program managers, operational planners, and commanders to oversee planning, financing, and monitoring of the years-long attack.[343]

Lastly, it should be noticed that the attackers prioritized three aspects. First, they were careful to avoid getting caught (especially with the first attack). Second, they went to great lengths to avoid catastrophic damage upon the centrifuge cascades. And third, they tried to minimize collateral damage. As General Michael Hayden, former director of the NSA and CIA, observes, the attack was "incredibly precise". […] "Although it was widely propagated, it was designed to trigger only in very carefully defined, discreet circumstances" - not acknowledging the U.S. was behind the attack, but

[340] As Lindsay also notes, such testing must have involved a fully-functional mock-up IR-1 cascade operating with real uranium hexafluoride because both overpressure and rotor speed manipulations have completely different effects if executed on empty centrifuges. (The Libyan P-1 centrifuges are essentially the same as the IR-1)
[341] Sanger, *Confront and Conceal*, p. 197
[342] Ibid, p. 198
[343] Lindsay, "Stuxnet and the Limits of Cyber Warfare"

stating that it has been launched by a "responsible nation".[344] Inherently, an actor that does not prioritize these issues will be able to conduct this type of attack at a much lower costs.[345]

4.3.4 Knitting the Pieces Together: an Overview of the Main Obstacles

Pulling the empirical data strings together from the empirical discussion above, this section digests the main obstacles to cyber weapon development by way of comparing them to nuclear weapons. Generally, one can identify three obstacles actors have to overcome to develop a certain weapon system. First, weapon development requires *know-how*; the knowledge required to design and acquire the weapon. Second, there are the *material* and *economic* costs. Third, weapon development often requires an *organizational structure*, as various actors have to work together to develop a certain capability. Table 4.2 summarizes the main obstacles to development.

[344] According to David Sanger, Obama became increasingly concerned about the potential collateral damage of Stuxnet. See: Sanger, *Confront and Conceal*, p. 204

[345] Langner stated the following during his three year long investigation: "Stuxnet was particularly costly because of the attackers' self-imposed constraints. Damage was to be disguised as reliability problems. I estimate that well over 50 percent of Stuxnet's development cost went into efforts to hide the attack, with the bulk of that cost dedicated to the overpressure attack which represents the ultimate in disguise - at the cost of having to build a fully-functional mockup IR-1 centrifuge cascade operating with real uranium hexafluoride." Langner, "To Kill a Centrifuge," p. 21

Table 4.2: Main Obstacles to Cyber Weapon Development

	Type I: Unsophisticated	**Type II: Sophisticated**	**Nuclear weapon[346]**
Knowledge	*Essential* • Only generic info required about target • Intelligence gathering not critical. • Targets are interchangeable • One person can have all the knowledge required	*Important* • Very specific information required about target • Intelligence gathering essential • Targets not interchangeable • Understanding ICSs/PLCs • Needs a large group of the most apt and brilliant	*Important* • Only generic info required about target • Intelligence gathering not critical • Targets interchangeable • (Initially) needs a large group of the most apt and brilliant
Economic and Material	*Unimportant* • Food and drinks	*Important* • Labour costs • Intelligence costs • Mirroring ICS testing environment	*Essential* • Plants associated with fissile material production • High cost refinement U-235
Organizational	*Unimportant* • No organizational structure required	*Important* • Coordination intelligence and military • High level of secrecy, not just of design but project itself • Months-long planning	*Important* • Secrecy of design • Interaction with/between agencies

** For each capability, I either denote the obstacle as i) 'essential'; the primary aspect to overcome to develop the capability; ii) 'important'; one of the main aspects to overcome to develop the capability; and iii) 'unimportant'; the aspect is not required for the development of the capability.*

First, unlike nuclear weapons, the knowledge component is the most essential aspect underlying the development of cyber weapons. Part of that knowledge is explicit and transferable in a formal or systematic manner; for example, being able to code in a certain language. The most significant part of this knowledge, however, is tacit - as Michael Polanyi states "we can know more than we can

[346] Gartzke and Jo only discuss three aspects for nuclear weapons; economic, knowledge and material. Yet, as more recent studies have indicated, the organizational component is at least as important. See: Jo and Gartzke, "Determinants of Nuclear Weapons Proliferation"

tell."[347] It concerns knowledge embedded in a hacker's experience or a cyber command's (implicit) operational processes.[348] The case studies above reveal the amount of knowledge required - both explicit and tacit - differs greatly depending on the cyber weapon's level of sophistication. What is perhaps less evident from the case studies, however, concerns the difference in the amount of information required of the target between cyber weapons. Unsophisticated cyber weapons are more generic in their target. The process of usage generally follows the pattern: 'I have this capability; against who/what can I use it?' As a result, it often leads to attacks on relatively easy targets. Highly advanced capabilities tend to follow the reverse process; 'I would like to target this entity, how can I do it?' This makes intelligence gathering activities an essential aspect of sophisticated cyber weapons, whereas for unsophisticated capabilities it matters much less. The difference in intelligence preparation between the two types of cyber weapons can be likened to the difference between someone attacking a stranger on the street with a knife/gun versus a covert attack operation. In the case of the street attack, the offender normally knows (and needs to know) little of the victim's background. He or she can also decide last minute to change target depending on the situation. For the covert operation, however, significant intelligence gathering activities are required to ensure the attack is successful.[349]

Second, the material and economic components are of less importance to the development of cyber weapons compared with nuclear weapons. Even today, acquiring the necessary materials to fuel a nuclear bomb remains difficult.[350] One reason is that isotope U-235, more commonly referred to as weapons-grade uranium, is a highly unstable form that makes up only 0.7 percent of the concentration of uranium ore that is dug up. Also, the uranium needs to be refined to a concentration of at least 80

[347] Michael Polanyi, *The Tacit Dimension,* (London: Routledge: 1967)
[348] Also see Rid, *Cyber War Will Not Take Place,* p. 83-84; Martin Davies, "Knowledge - Explicit, implicit and tacit: Philosophical aspects," in James D. Wright (ed.), *International Encyclopaedia of Social and Behavioral Sciences,* retrieved from: http://www.mkdavies.net/Martin_Davies/Papers_files/KnowledgeExpImpTacit.pdf
[349] Indeed, although there is little public information about the exact way information is gathered for sophisticated cyber operations, it likely follows the typical phases of intelligence gathering, which are: i) selection and discovery; the attackers use publicly available resources to collect details about the target; ii) resource extraction and mining; the attackers dig deeper to collect raw data about the target; iii) resource correlation and information; the attackers spend time to correlate data before processing it iv) and attack modeling; the attackers sketch an outline of the attack by using processed information from the previous phase. See: Par Aditya Sood and Richard Enbody, *Targeted Cyber Attacks: Multi-staged Attacks Driven by Exploits and Malware*, (Elsevier: Waltham: 2014)
[350] Due to increased public information on nuclear weapons, the know-how to develop the technology has not been a major problem over the last decades. The Nth country experiment has proven this. The experiment was conducted by the Lawrence Livermore National Laboratory in May 1964. The lab recruited three early-career physicists, with no experience in (nuclear) weapon development, to "design a nuclear explosive which, if built in small numbers, would give a small nation a significant effect on their foreign relations." The physicists, using only publicly available documents, were able to draft up a credible design for a nuclear bomb within three years of appointment. Similar experiments were conducted in later years - taking even less time. Jim W. Frank, "Summary Report of the Nth Country Experiment," *Lawrence Radiation Laboratory,* (1967, March)

percent U-235 in order to be weapons grade, although upwards of 90 percent is preferable. Although the economic resources required to build a nuclear bomb has fallen, they remain significant as well.[351] For cyber weapons, the material and economic costs do not come even close to these figures. But, for developing sophisticated cyber weapons, it has become clear that a lot of financial and material resources are required as well. Information available about Stuxnet reveals the high costs of establishing an Industrial Control System (ICS) testing environment.

Third, a move along the spectrum of cyber weapons also signifies a shift in the number of people and organization(s) required to develop a cyber weapon. Perhaps the most interesting organizational feature of developing sophisticated cyber weapons is not the amount of institutional capacity required, but its level of secrecy. In the case of the Manhattan Project, the *design* of nuclear weapons was secret during World War II.[352] However, the very fact that the U.S. was developing a nuclear bomb was *not* secret. Notice that in the case of Stuxnet the capability *itself* - the very idea that it was possible to sabotage an industrial control system in the way it did - was kept secret.[353] In fact, this secrecy was a requirement for the cyber weapon to work.

4.4 Drivers of Cost Reduction[354]

Section 4.3 served to provide an overview of the obstacles states *currently* have to overcome to develop a certain type of cyber capability. Yet, as any product, it may become easier or more economical to develop a cyber weapon over time. And, the expectation is that when the overall cyber latency threshold lowers, more states will acquire cyber weapons.

---

[351] According to Frank Barnaby, "[t]he development and production of even modest nuclear forces used to be a costly enterprise. The British and French nuclear forces, for example, cost well over $10 billion. The development of the nuclear warheads was a major part of this cost." When nuclear weapons are produced as a 'by-product' of peaceful nuclear programs - like India - the costs are significantly lower. Frank Barnaby, "How States can "go nuclear," *Annals of the American Academy of Political and Social Science*, 430 (1977):29-43

[352] Yet, Soviet spies were able to gather a great amount of information about the production and design.

[353] The centrifuges used to run the large-scale tests were spread out over several national laboratories of the U.S. Energy Department. Also, there are reports that Stuxnet had been tested at the Israel's Dimona nuclear facility. See: William J. Broad and David E. Sanger, "Israeli Test on Worm Called Crucial in Nuclear Delay," *The New York Times*, (2011), retrieved from: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html ; Isabel Kershner, "Meir Dagan, Israeli Spymaster, Dies at 71; Disrupted Iran's Nuclear program," *The New York Times*, (2016, March 17), retrieved from: http://topics.nytimes.com/top/news/international/countriesandterritories/iran/nuclear_program/index.html?inline=nyt-classifier

[354] This section is adopted from: Max Smeets, "What it Takes to Develop a Cyber Weapon: Nobody Knows"; also see the response of Lin: Herbert Lin, "Oft-Neglected Cost Drivers of Cyber Weapons," *Council on Foreign Relations: Net Politics*, (2016, December 14), retrieved from: https://www.cfr.org/blog/oft-neglected-cost-drivers-cyber-weapons

Although there is a general consensus that conducting offensive cyber operations will be less expensive in the future, thus far, the drivers and barriers to cost reduction have yet to be specified.[355] This invites the question: To what degree will the obstacles outlined above still exist in a few years' time?

As cyber weapons have a significant knowledge component, it suggests that the most critical part of cost reduction comes from 'experience' and 'learning curve' effects.[356] I identify four processes that drive the cost reduction of cyber weapons. First, there is cost reduction through labour efficiency; attackers become more dexterous in that they spend less time learning, experimenting, and making mistakes in writing code. Section 4.3 indicated that the Iranian cyber activities were not necessarily the most sophisticated. Yet, since the Shamoon virus wiped the hard drives of 30,000 workstations at Saudi Aramco, there have been significant improvements in their coding. Whereas Shamoon contained at least four significant coding errors, newer malware seems to be more carefully designed.[357]

Second, there are the processes of standardization and specialization. Some parts of cyber weapons have become increasingly standardized (such as exploit tool kits), leading to an increase in efficiency. The growth of offensive cyber capabilities in militaries allows for greater specialization in cyber weapon production. Chapter 3 noted that the U.S. Cyber Command now has 133 teams in operation, making it easier to dedicate specialized units to specific types of cyber operations—even if these units need to be integrated within a general force structure.[358] According to one report, Russia was able to do the same thing for its cyber campaigns against Ukraine.[359]

Third, product redesign allows attackers to learn to produce cyber weapons more cost effectively. The wiper cases discussed above are illustrative of this process. A recent prominent case has been

[355] Adrienne LaFrance, "How Much Will Today's Internet Outage Cost?," *The Atlantic*, (2016, October 21) retrieved from: http://www.theatlantic.com/technology/archive/2016/10/a-lot/505025/; James Griffiths, "Price of website disabling DDoS attacks fall to US$38 per hour as botnets proliferate in China, Vietnam," *South China Morning Post*, (2015, June 12), retrieved from: http://www.scmp.com/tech/enterprises/article/1820464/price-website-disabling-ddos-attacks-fall-us38-hour-botnets

[356] Marvin B. Lieberman, "The Learning Curve, Diffusion, and Competitive Strategy," *Strategic Management Journal*, 8:5 (1987):441-452; Boston Consulting Group, "Perspective on Experience," *Technical Report* (1972)

[357] Dmitry Tarakanov, "Shamoon The Wiper: Further Details (Part II)," *Securelist,* (2012, September 11) retrieved from: https://securelist.com/blog/incidents/57784/shamoon-the-wiper-further-details-part-ii/

[358] Department of Defense, "All Cyber Mission Force Teams Achieve Initial Operating Capability," *U.S. Cyber Command News Release,* (2016, October 24), retrieved from: http://www.defense.gov/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability; also see chapter 5

[359] Rob Morgus, "WhoDunnit? Russia and Coercion through Cyberspace," *War on the Rocks,* (2016, October 19), retrieved from: http://warontherocks.com/2016/10/whodunnit-russia-and-coercion-through-cyberspace/

WannaCry, which is equipped with NSA exploits leaked the Shadow Brokers hacking group.[360] Actors who seem to have relatively limited resources have in recent years been getting more bang for their buck.

Fourth, there are shared experience effects, which allow lessons from one piece of malware to shed light on other offensive capabilities. Cyber weapons are generally part of a large collection of capabilities—sharing vulnerability, exploits, propagation techniques, and other features. Stuxnet's 'father', for example, is thought to be USB worm Fanny, and Stuxnet has also been linked to espionage platforms like Duqu, Flame, miniFlame, Gauss, and Duqu 2.0.[361]

However, there are also barriers to cost reduction — especially when it comes to sophisticated cyber weapons such as Stuxnet. The defensive measures put in place as a result of advanced persistent threats have forced actors to develop more complex capabilities to remain effective. Although it is still the case that most computer breaches could have been avoided by simple patching, basic measures such as network segmentation, firewall implementation, and the use of secure remote access methods are becoming increasingly common. Furthermore, IT security professionals communicate more regularly with management about cyber threats than they did a decade ago.

At a recent Royal United Services Institute conference, a military cyber commander clearly stated that the main problem for conducting effective operations is "people, people, people."[362] For a government, attracting the brightest minds does not come cheap—especially when a person has the opportunity to work in the private sector for a much higher salary. Historically, foreign intelligence agencies have needed foreign language professionals. Today, they need people able to interpret and write code. However, since coding is a highly transferable skill, these people are able to switch to the private sector easily—making the government's job of retaining them much harder.

Lastly, a cyber weapon program requires continuous production, not just intermittent projects. The malleability of cyberspace gives these weapons a highly transitory nature; they are only effective for a short while.[363] Therefore, the development of cyber weapons must be unceasing and resources must be constantly available. Ideally, cyber weapons would be produced on an assembly line, ensuring that

[360] Eric Geller, "NSA-created cyber tool spawns global attacks — and victims include Russia," *Politico*, (2017, May 12), retrieved from: http://www.politico.com/story/2017/05/12/nsa-hacking-tools-hospital-ransomware-attacks-wannacryptor-238328
[361] Kaspersky Lab, " A Fanny Equation: "I am your father, Stuxnet," *Securelist*, (2015, February 17), Retrieved from: https://securelist.com/blog/research/68787/a-fanny-equation-i-am-your-father-stuxnet/
[362] Senior Military Cyber Commander, "The Second International Cyber Symposium: Cyberspace and the Transformation of 21st Century Warfare," *The Royal United Services Institute (RUSI)* (Church House, Westminster: London), 19-20 October 2016
[363] For a more extensive discussion on this topic see: Smeets, "A Matter of Time"

when one weapon becomes ineffective, the next can be put to use. However, it is hard to estimate the costs of maintaining a cyber capability. Because of the patching dynamic (e.g. the ability to cause harm or damage remains constant for a certain period of time, but rapidly declines the moment a vendor becomes aware of the vulnerability) a better way to model the transitory nature a cyber weapon is similar to the Black-Scholes model of options pricing in finance. A cyber weapon is analogous to what is called an 'American option'. The value of usage could be modelled as a 'Brownian Motion' with random crashes representing the use of the weapon by others.[364]

Having identified the drivers of cost reduction, it indicates that the costs of unsophisticated cyber weapons are most likely to reduce in the future. For sophisticated cyber weapons, the future cost development path is far less evident. As said, to attract the most apt and brilliant will not become easier in the future. Having important material and organizational components too, these capabilities are less susceptible to learning curve effects.

4.5 The Incentives for the Transfer of Cyber Weapon Technology

'Supply' (or opportunity) refers to the "*total* set of environmental constraints and possibilities" for a state to acquire cyber weapons, as the introductory chapter of this study laid out.[365] This means that a comprehensive supply-side analysis is incomplete if it does not take into consideration the activity of other actors as well. A diverse range of actors could potentially make it easier for states to acquire cyber weapons through assisting them in their acquisition efforts. Similarly, other actors may also try to raise the 'cyber latency threshold' through creating additional barriers, such as enforcing sanctions or even sabotaging the development process.

Much has been written on the dynamics of (global) arms trade. The way Khan has helped Pakistan acquire the nuclear bomb is perhaps the most well-known account of how 'environmental possibilities' allowed for nuclear proliferation.[366]

---

[364] The security patching process of software vulnerabilities indicates that these cyberweapons in particular are also qualitatively different from conventional weapons in terms of their short-lived nature to cause harm or damage. Although patches can be distributed in a number of ways, the corrective process which takes place after a software vulnerability is exploited does not only prevent successful exploitation against one system but against any administrator which uploads the patch. See: Smeets, "A Matter of Time," p.10

[365] Most, and Starr, *Inquiry, logic and international politics*, p. 23

[366] As William Hartung writes: "using plans [Khan] developed while working at a nuclear facility in Europe - along with a blank cheque from the Pakistani government of Zulfikar Ali Bhutto - Khan built a vast centrifuge facility at Kahuta, near Islamabad. By the early 1980s the facility was able to enrich significant quantities of uranium. By 1984, Khan claims he completed work on a nuclear bomb. He later boasted about this feat in the context of his country's lack of development saying, 'A country which could not make sewing needles [or] good bicycles [...] was embarking on one of the latest and most difficult technologies'. But he did not do it alone. […] Khan was able to purchase much of what was needed for the

Keith Krause broadly distinguishes between four forms of technological transfer of military capabilities. Subsequent literature has adopted and expanded upon these general categories, which can be fruitfully applied to cyber weapons as well[367]:

- *Form I:* the diffusion of finished systems and the ability to operate weapons technology.
- *Form II:* the diffusion of basic engineering know-how used to reproduce weapons technology, and capacity transfer.
- *Form III:* the diffusion of (scientific) knowledge and technical expertise used to adapt weapons technology.
- *Form IV*: the capacity to innovate at the technological frontier.[368]

As Lindsay and Gartzke observe, the essential element of cyber weapons' success is deception, with its basic tactics being dissimilation (hiding what is there) and simulation (showing what it is not).[369] As the attacker constantly needs to adapt to ensure the effectiveness of a capability, *Form III* and *Form IV* are particularly important for the development of (sophisticated) cyber capabilities.[370]

Several actors can enable the four forms of (technological) transfer, which could be categorized as: advanced cyber powers and private sector actors, and non-state actors.[371] The label 'advanced cyber powers' denotes those states which have in the past developed sophisticated cyber weapons, such as the US, Russia and the UK (see chapter 3). 'Private sector actors' refers here to both privately owned firms (e.g. Microsoft) as well publicly controlled firms (e.g. Huawei). The term 'non-state actors' is used here to label other non-state actors such as script kiddies, criminals, and patriotic hackers.

Pakistani bomb on the open market.[...] Pakistan obtained one or more of almost every component needed to build a centrifuge enrichment plant. [...] Once Pakistan had the bomb and the capacity to enrich uranium, Khan 'reversed the network' he had developed to bring nuclear components and materials into Pakistan, […]". William D. Hartung, "The International Arms Trade," in Paul D. Williams (Ed), *Security Studies: An Introduction*, (Abingdon: Routledge: 2008).

[367] For example, see David Kinsella, "Arms Production in the Third Tier: an Analysis of Opportunity and Willingness", I*nternational Interactions*, 26:3 (2000) 253-286

[368] Keith Krause, *Arms and the State: Patterns of Military Production and Trade*, (Cambridge; Cambridge University Press: 1992), p. 18-25; also see: Kinsella, "Arms Production in the Third Tier: an Analysis of Opportunity and Willingness"

[369] Lindsay and Gartzke consider 'deception' to be a distinct strategy, similar to deterrence in the nuclear era. Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies*, 24:2, (2015) 316-348. As Martin Libicki also states, there is no 'forced entry' when it comes to offensive cyber operations. Martin Libicki, C*onquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007), see p. 31-36; For a discussion on the optimal design of a sophisticated cyber weapon see: Max Smeets, "Organizational Integration of Offensive Cyber Capabilities: A Primer on the Risks and Benefits."

[370] If an actor 'reproduces' cyber weapons, it can only attack those actors which have failed to adopt new security measures, i.e. the 'laggards'. For more information on the patching dynamic see: Smeets, "A Matter of Time"

[371] The export of all these forms could be both direct or indirect, and intentional or unintentional. Previous discussions have already touched upon most of the unintentional aspects; in chapter 3 I talked about the role of leaking capabilities, and in the above section of this chapter I already addressed different from of learning. In this part I therefore primarily focus on the *intentional* forms of transfer.

Table 4.3 provides an overview of the capacity and willingness of these actors to help states develop cyber weapons.[372] First, *capacity* refers to whether the type of actor has the ability to share a specific 'form' with (other) states. Second, *willingness* is about whether the type of actor has an incentive to share this capability with (other) states.

Table 4.3: Actors' Capacity and Willingness to Transfer Cyber Weapon Technology

		Advanced Cyber State	**Private-Sector**	**Non-state/individuals**
Form I	Capacity	V	V	V
	Willingness	X	V	V
Form II	Capacity	V	V	V
	Willingness	X	V	V
Form III	Capacity	V	V/X	X
	Willingness	V/X	V	V
Form IV	Capacity	V	V/X	X
	Willingness	V/X	V	V

First, let us consider the potential transfer of capabilities from 'advanced cyber states' to less advanced actors. Numerous media reports and other articles have been published on defence-related cyber initiatives. Not least, NATO (or affiliated organizations) is said to regularly organize cyber security exercises and strategy development workshops in which states (sometimes also non-members) can participate.[373] The alliance also has more specific initiatives tailored to specific states. For example, in May of 2012, NATO and Georgia developed a cyber defence training program to educate Afghan network and system administrators to build institutional capabilities and public awareness of cyber threats.[374] We also know about a wide range of bilateral state initiatives on cyber capacity building. As part of a defence cooperation agreement, Brazilian personnel take part in workshops and other exercises on cyber defence sponsored by the U.S. Department of Defence.[375]

[372] While for analytical purposes I separate the two types of actors in my discussion below, it should be evident that there has always been an intimate connection between the state and private sector with respect to the export of arms.
[373] During the 2011 NATO-Ukraine International Staff Talks on Cyber Defense, National Security and Defence Council members briefed attendants on the Draft Strategy of Ukraine on Cyber Defence.
[374] NATO, "Afghan Managers Train in Cyber Defence", (2012, May 21), retrieved from: http://www.nato.int/cps/en/natohq/news_86990.htm?selectedLocale=en
[375] Unsurprisingly, the U.S. has bilateral arrangements on cyber defense with multiple other countries. In June 2011, the U.S. also announced a bilateral strategic policy dialogue on cybersecurity with Japan. Marcus Weisberger, "Japan, U.S. to expand missile defense, cyber cooperation", *Defense News*, (2011, June 21). Also see: United Nations Institute for Disarmament Research (UNIDIR), "The Cyber Index International Security Trends and Realities"

More comprehensively, Brazil and Argentina have reportedly pushed a for a 'joint cyber shield' for South America.[376] And Columbia has sent officials to Estonia for cyber training.

However, when it comes to offensive cooperation much less is (publicly) known.[377] For many, the Five Eyes intelligence alliance confirms that offensive cyber cooperation is possible.[378] But, it also illustrates the inherent limitations: indeed, in other areas close cooperation goes beyond a network of five states. The discussion below on the capacity and willingness goes a long way to explain this dynamic.

First, in terms of capacity, advanced cyber states can enable the first three forms of transfer listed above - for example, through the sharing of zero-day exploit, malware samples or testing facilities. The ability of state actors to help others to innovate (*Form IV*) may be possible - for example, through intelligence sharing or the provision/training of experts - although it is inherently more difficult as it also depends on the organizational and cultural dynamics of the state receiving assistance.

Yet, despite their inherent capacity, advanced cyber states do not seem to have strong incentives to engage in this type of activity.[379] Note that for conventional capabilities, a state is said to be inherently more likely to enable the first two forms of technological transfer; that is, deliver finished systems or help with the reproduction of capabilities. The first two forms of transfer can normally strengthen the industrial-defence base at home and lock in alliances, whilst ensuring other states remain dependent. The incentives for transferring cyber weapon technology are different.

As I have previously discussed, the likelihood of a cyber weapon's ineffectiveness after use significantly increases (this is part of so-called 'transitory' dynamic of cyber weapons). This dimension reduces the overall incentives for offensive cyber cooperation, and in particular for sharing zero-day exploits or complete cyber weapons.

---

[376] Shobhan Saxena, "Brazil, Argentina push for joint cyber shield for South America," (November 24, 2013), retrieved from: http://www.thehindu.com/news/international/world/brazil-argentina-push-for-joint-cyber-shield-for-south-america/article5386962.ece

[377] A few public articles exist, but often the exact nature of cooperation remains unknown (or refers to transferring surveillance capabilities). For example, Yanmar, when it established the Defense Services Computer Directorate in 1990, reportedly received assistance from China. Also: ZimNet, "Zim gets deadly Iran Weapons to fight cyber 'internet' protests'" (unknown date), retrieved from: https://zimnews.net/zim-internet-computer-bill-iran-mnangagwa/

[378] Warwick Ashford, "UK and US collaborating on cyber weapons, says Snowden," *Computer Weekly*, (2013, August 2) retrieved from: http://www.computerweekly.com/news/2240202997/UK-and-US-collaborating-on-cyber-weapons-says-Snowden

[379] Indeed, my argument is that the incentives are also weaker compared to the transfer of conventional arms technology.

Consider a situation in which an advanced state (Actor A) sells a conventional military capability - like a tank or aircraft - to an ally (Actor B). In this case, Actor B is usually able to deploy this capability at its own discretion. And, more importantly, the use of the acquired military asset by Actor B against one actor, hardly reduces the effective deployment of the *same* asset by Actor A against a *different* adversary. In contrast, for sharing zero-day exploits - or even complete cyber weapons - we witness a different dynamic; the use of the cyber capability by one actor, greatly reduces the ability of other actors to also use it.[380] This means that mutual benefits only arise when states share views on the i) timing, ii) target iii) and proportionality of the cyber attack. The paradox of cyber weapons is that, although technically they can be (relatively) effortlessly replicated, their transitory nature changes the incentive structure of actors and turns weapons into indivisible goods.[381]

Hence, if any incentives exist, it would be in facilitating other states to develop their *own* offensive capabilities - that is by providing knowledge/expertise to adapt weapons technology (*Form III*), and providing the capacity to innovate (*Form IV)* - as this does not reduce the effectiveness of one's own arsenal. Yet, an advanced cyber power would only consider this type of transfer with a highly select group of other states; i.e. only those actors with which the state has historically strong ties and can trust that these capabilities will not be used against them (at some point in the future).

Finally, attribution dynamics may possibly further complicate the sharing dynamic of cyber weapon technology between states. If a state decides to share part of its hacking infrastructure - such as command and control system and samples of malicious code - and/or provides insights in its modus operandi, it may increase the likelihood for misattribution following the use by another state. Generally, this would be seen as another disincentive to share offensive cyber capability technology. Yet, there are possible advantages: other actors would find it more difficult to disentangle which state - part of the coalition - is responsible for attack, increasing the difficulty of deciding on a response.[382]

[380] These incentives for *not* sharing are not as strong for espionage capabilities, as these are less likely to be discovered following usage.
[381] This dynamic might potentially exist within a state as well, when government institutions, with different organisational missions, are developing separate offensive cyber capability programs.
[382] ´Regin´, a sophisticated piece of malware targeting specific Microsoft Windows-based computers, could be a potential example of this (though not conscious). Experts still debate which state within the 5-eyes network has developed the capability. Australian Times, "Australia implicated in Regin mega cyber-warfare program," (2015, January 30), Retrieved from: http://www.australiantimes.co.uk/australia-implicated-regin-mega-cyber-warfare-program/

Let us now turn our analysis to the private sector and/or other non-state actors as a potential supplier of cyber weapon technology to states.[383] The growing zero-day exploit market signals that this group of actors has a growing capacity to service states which aim to acquire an offensive cyber capabilities.[384] A report from RAND Corporation has provided a comprehensive analysis of the market of zero-day exploits.[385] The report differentiates between markets based on who is informed following zero-day discovery. In white markets the information is sold or given to the vendor. In gray markets, the information is sold to governments or their suppliers.[386] In black markets, the information about the vulnerability is sold to cybercriminals. Prices for exploits are said to range up to $1 million.[387]

In 2015, the email archive of Hacking Team, an Italian company developing and selling spyware to government intelligence and law enforcement agencies around the world, was compromised. The company's activities serves as an interesting case study to better understand the zero-day market. Hacking Team buys zero-day exploits in order to reliably install its spyware on targeted systems.[388]

Vlad Tsyrklevich's excellent study on the spyware-selling company suggests that the market is professional (or 'mundane') in that it follows typical purchasing procedures of testing, delivery, and acceptance (such as warranty and requirement negotiations as well as set agreements on payment). Prices for technical vulnerabilities are shown to differ significantly depending on the relevance and

[383] The discussion of the zero-day market also serves to show that there is a close relationship between the private sector and individual hackers: a non-affiliated hacker often finds a bug or develops an exploitation technique, and a specialized business buys these up to serve as a broker/marketplace.
[384] We commonly distinguish between zero-day bug and a zero-day exploit.
[385] Martin C. Libicki, Lillian Ablon, Tim Web, "The Defender's Dilemma: Charting a Course Toward Cybersecurity," *RAND Publication*, (2015) Retrieved from: http://www.rand.org/content/dam/rand/pubs/research_reports/RR1000/RR1024/RAND_RR1024.pdf
[386] Ibid. A different definition of these markets is used in an earlier RAND report. In the previous report it is stated that: "[w]e separate what we call black markets from gray ones, although such markets may overlap. Black markets are organized and run for the purpose of cybercrime; they deal in exploit kits, botnets, Distributed Denial of Service (DDoS), attack services, and the fruits of crime (e.g., stolen credit card numbers, compromised hosts). Gray markets, by our definition, are limited to the exchanges of vulnerabilities and exploits, the discovery and development of which are not illegal per […] but can nevertheless be troubling because they also complicate the life of system defenders." Lillan Ablon, Martin C. Libicki, and Andrea A. Golay, "Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar," *RAND Corporation*, (2014), retrieved from: http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf, p. 1
[387] In fact, the FBI allegedly paid just under $1 million for the technique to unlock the iPhone used by one of the San Bernadino shooters. See: Mark Hosenball, "FBI paid under $1 million to unlock San Bernardino iPhone," *Reuters*, retrieved from: http://www.reuters.com/article/us-apple-encryption-idUSKCN0XQ032; the market for zero-day exploits seem to continue to grow. Joseph Menn, "Special Report: U.S. cyberwar strategy stokes fear of blowback," Reuters, (2013) Retrieved from: http://www.reuters.com/article/2013/05/10/us-usa-cyberweapons-specialreport-idUSBRE9490EL20130510
[388] The name of their spyware is known as RCS. The company provides both the exploits and RCS to government intelligence and law enforcement agencies around the world.

complexity of exploit.[389] The email leaks also revealed that Hacking Team tried to do business with multiple vendors, including: US-based firms Netragard and Vulnerabilities Brokerage International, French firm VUPEN,[390] and Singaporean firm Coseinc.[391] It was also able to buy from individual exploit developers like Rosario Valotta and Vitaliy Toropov.

Yet, what is perhaps most interesting is the low number of zero-days Hacking Team was actually able to acquire. As Zetter also writes, "[t]hough Hacking Team began seeking zero-days in 2009 and contacted a number of sellers over the years, it appears to have failed to secure zero-days until 2013."[392] In the two years after, it was only able to acquire five zero-day exploits.[393] Furthermore, many suppliers were unwilling to do business with the company, as they were only willing to sell straight to (certain) governments.[394]

Of course the private sector can service more than zero-day exploits. A key stumbling block for cyber commands or other institutions developing military cyber capacity, remains the lack of good people. Various companies - such as Booz Allen Hamilton - employ former intelligence officials, in turn contracted to the governments.[395] Also, the private sector can provide some of the infrastructure required to conduct offensive operations. Thales, for example, has a contract with the Dutch government for a 'cyber range'; a testing facility for capabilities.

4.6 Conclusion

The purpose of this chapter was to assess the supply-side of cyber proliferation. The first part of this chapter identified the main obstacles actors have to overcome to develop a cyber weapon. I argued that the absolute costs of developing unsophisticated cyber weapons are low. Both the material and

[389] Yet, Tsyrklevich also notes that we should be "warned that price comparisons for different exploits should be taken with a grain of salt. Exploit developers have an incentive to state high prices and brokers offer to sell both low-quality and high-quality exploits. If a buyer negotiates poorly or chooses a shoddy exploit, the vendor still benefits. Moreover, it's difficult to compare the reliability and project longevity of vulnerabilities or exploits offered by different developers. Many of the exploits offered by exploit brokers are not sold." Vlad Tsyrklevich, "Hacking Team: a zero-day market case study," (2015, July 22), retrieved from: https://tsyrklevich.net/2015/07/22/hacking-team-0day-market/
[390] In 2015, VUPEN's funders established a new US-based company called Zerodium. See: https://zerodium.com/
[391] Also see the website of the company: https://www.coseinc.com/en/
[392] Zetter largely follows the analysis of Tsyrklevich. See: Kim Zetter, "Hacking Team Leak Shows how Secretive Zero-day exploit sales work," *Wired*, (2015, July 24), retrieved from: https://www.wired.com/2015/07/hacking-team-leak-shows-secretive-zero-day-exploit-sales-work.
[393] Tsyrklevich, "Hacking Team"
[394] Notice that businesses selling these exploits may not be willing to service all states. At least publicly, some state that they only do business with certain actors. See: Adam Segal, "Using Incentives to Shape the Zero-Day Market" *Council on Foreign Relations, Cyber Brief* (2016, September 19), retrieved from: https://www.cfr.org/report/using-incentives-shape-zero-day-market
[395] It remains unclear to what degree they directly helped with the development.

organizational costs for these capabilities are minimal. However, the chapter showed that the material and immaterial resources required to acquire sophisticated cyber weapons are disproportionately higher. Direct access to a dedicated intelligence network is required to obtain sufficient information about the target's computer systems. It was also noticed that the mirroring of an Industrial Control System environment is an obstacle that even well-funded state actors find difficult to overcome. Finally, intelligence and military organizations have to work closely together to develop and use these capabilities while maintaining a high level of secrecy.

The chapter also analysed the drivers of cost reduction to more comprehensively understand the supply-side of cyber proliferation. I identified four processes that drive the cost reduction of cyber weapons: labour efficiency, specialization, product redesign, and shared experience effects. Yet, I also noted that there are some inherent barriers for future cost reduction. Improved defence requires the attacker to develop more complex capabilities to ensure effectiveness. It is also inherently difficult to hire the right technical minds - and because it is a highly transferable skill making it difficult to retain people. Finally, as offensive cyber capabilities are effective for only a short period of time, any cyber weapon program requires continuous production, not just intermittent projects.

The last dimension of the supply-side analysed in this chapter concerned the potential transfer of cyber weapon technology to less advanced states. There are only weak incentives for advanced cyber states to share cyber weapons. If there are any, as I conclude, it would be in facilitating other states to develop their *own* offensive capabilities - that is by providing knowledge/expertise to adapt weapons technology, and by providing the capacity to innovate - as this does not reduce the effectiveness of one's own arsenal. The private sector and/or other non-state actors are also a potential supplier of cyber weapon technology to states. Thus, state acquisition of cyber weapons does not necessarily imply only state *production* of the capability.

What does this imply for states cyber latency? Inherently, as the discussion above reveals, *all* states are able to develop unsophisticated cyber weapons. The costs of simple DDoS attack have a fallen so significantly over the past decade that any actor requires just limited resources to conduct this type of attack. Also, the 'wipers' have shown to be within reach of even less advanced states. Yet, although exact estimates are difficult to provide, the group of states that currently have the technology, facilities, expertise, resources and other capabilities necessary for the development of cyber weapons is much smaller.

Like the small elements of a high-quality Swiss clockwork that work beautifully together to show the time with complete precision, a close connection between numerous actors and processes is necessary to conduct a sophisticated cyber operation like Stuxnet. Today, numerous states still struggle to ensure organizational cooperation with respect to even the most basic tasks related to cyber security.[396] They are still far from crossing the organizational threshold of cyber latency.

[396] For an overview see: United Nations Institute for Disarmament Research (UNIDIR), "The Cyber Index International Security Trends and Realities"

Chapter 5: Demand-Side Predictors: Assessing Three Proliferation Frameworks

5.1 Introduction

The first set of arguments developed in this thesis were drawn from the supply-side; that is, states' opportunity to develop cyber weapons. The previous chapter observed that most cyber weapons used to date are unsophisticated in nature and are relatively easy to acquire for any state. Yet, the barriers states have to overcome to develop sophisticated cyber weapons are disproportionately higher. Although the gap between technical potential to develop sophisticated cyber weapons and military reality is much smaller than what some scholars conceive it to be, the supply-side only goes so far in explaining cyber proliferation. Indeed, there are numerous countries which have the latent capacity to develop cyber capabilities but have not done so.

This chapter therefore looks at the demand-side; that is, the motivations that drive cyber proliferation in the international system.[397] Many works in security studies have been devoted to the demand-side dynamics of arms proliferation, the seminal study of Scott Sagan *Why Do States Build Nuclear Weapons* is among the best; it provides an excellent starting point of analysis.[398] Sagan identifies three 'models', in the informal sense of the term, to explain states' willingness to go for the nuclear option.[399] First, the *international security* framework posits that insecurity explains a state's possession of a (nuclear) weapon. Second, *domestic politics* imperative states that proliferation is driven by competing interests and incentives *within* the state. The final normative framework claims

[397] Excellent reviews of the current literature on the motivations underlying nuclear proliferation have already been provided by other scholars. See: Sagan, "The Causes of Nuclear Weapons Proliferation, "; Hymans, "Theories of Nuclear Proliferation;" Montgomery and Sagan, "The Perils of Predicting Proliferation"

[398] Etel Solingen was the first to derive testable hypotheses on a state's willingness to acquire nuclear weapons. She compared a neorealist framework against her own hypothesis that inward looking, nationalist coalitions are less likely to embrace nuclear regimes compared to their more liberal, outward-looking counterparts as they try to avoid costs such as the denial of access to foreign technology, market, capital and investments in their pursuit of economic reforms. Etel Solingen, "The Political Economy of Nuclear Restraint," *International Security*, 19:2 (1994):126-169. The most significant early contribution concerns: William Epstein, "*The Last Chance: The Unbearable Lightness of the NPT*," (New York: Free Press: 1976); Ibid, p. 136; Sagan, "Why Do States Build Nuclear Weapons?"

[399] Sagan's frameworks closely map on the theoretical approaches laid out by Suchman and Eyre earlier on more general procurement policy. First, the security framework combines the 'strategic-functional' and 'geopolitical' approach of Suchman and Eyre. Second, the domestic politics model is similar to the domestic politics model. Third, Sagan's prestige model closely aligns with the Suchman and Eyre's institutional theory. See: Mark C. Suchman and Dana P. Eyre, "Military Procurement as Rational Myth: Notes on the Social Construction of Weapons Proliferation" , *Sociological Forum*, 7:1 (1992):137-161

that states' movement towards the acquisition of weapons follows from their efforts to match international expectations.[400]

Although previous scholarship on cyber conflict has made passing references to several elements underlying Sagan's proliferation models, they have not been systematically analyzed for cyber proliferation. The central purpose of this chapter is to rigorously assess the application of these models in the explanation of cyber proliferation among states, placing various arguments in a comparative theoretical framework and evaluate them against empirical evidence.

At the outset we should heed an important caveat: none of these frameworks alone provides a silver bullet explanation; that is, none outlines a causal mechanism which explains all cases of cyber proliferation and restraint. Thus, this is not a mono-causal analysis. Hence, the aim here is to assess the explanatory power of each framework separately whilst embracing theoretical eclecticism in fusing their different mechanisms together. Not all factors may matter equally in all cases. However, the acknowledgment that multiple factors may be at play leads to a richer, more powerful analysis. In the end we try to find out which parts of the cyber proliferation puzzle each framework is best able to capture.[401]

Also, it is tempting to assume that the motivations underlying the development of cyber weapons are the same as for building the nuclear bomb. After all, the states which are known to be the first to develop sophisticated offensive cyber capabilities - the United States (U.S.), the United Kingdom (U.K) Russia, China, Israel, and potentially France - also happen to be part of the nuclear club.

Yet, as many scholars have pointed out, cyber weapons have a number of characteristics that differentiate them from nuclear weapons and other kinetic weapons.[402] Also, although the current cyber situation is a close mirror image of the earlier nuclear situation, this is unlikely to endure in the future. Unlike nuclear weapons, there is a significantly larger group - of at least thirty states - which

[400] Subsequent research on nuclear proliferation has built upon Sagan's study, trying to provide a clearer articulation of hypotheses and the plausible mechanisms linking cause and effect.
[401] Sagan draws a similar conclusion in relation to nuclear proliferation frameworks. Sagan, "Why Do States Build Nuclear Weapons?"
[402] According to a study of the National Academy of Sciences (NAS), there are three characteristics which distinguish cyber weapons from conventional weapons. First, "they are easy to use with high degrees of anonymity and with plausible deniability, making them well suited for covert operations and for instigating conflict between other parties." Second, they "are more uncertain in the outcomes they produce, making it difficult to estimate deliberate and collateral damage". Third, they "involve a much larger range of options and possible outcomes, and may operate on time scales ranging from tenths of a second to years, and at spatial scales anywhere from "concentrated in a facility next door" to globally dispersed." See: William A. Owens, Kenneth W. Dam, and Herbert S. Lin (Eds.), "Excerpts from Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities," Committee on Offensive Information Warfare, *National Research Council*, (2009), see S-1, section 1.4 and 2.1

aspire or attempt to develop cyber weapons.[403] Hence, although we can use the same framework for classifying the factors which could potentially drive the dynamics of cyber proliferation, it would be misguided to a priori analogize the underlying motivations of states for acquisition or restraint. Indeed, as Joseph Nye writes, "[h]istorical analogies are always dangerous if taken too literately, and the differences between nuclear and cyber technologies are great."[404]

The chapter successively examines the three theoretical frameworks. The next section (section 5.2) assesses the national security considerations as the cause of cyber proliferation. The subsequent part (section 5.3) analyses how cyber weapons play a role in bureaucratic struggles. Section 5.4 considers the normative elements underlying the development of offensive cyber capabilities.

5.2 The National Security Imperative

5.2.1 Theoretical Framework

Stressing the perils of anarchy, the security imperative emphasizes the role of states' threat perception in explaining cyber proliferation. The framework is rooted in the neorealist tradition of IR.[405] "Scholars in international relations have long given threat perception a central role in theories of war, deterrence, alliances, and conflict resolution," Janice Gross Stein notes.[406] Threat perceptions are subjective, but have 'real' implications.[407] It also seems to be one of most intuitive explanations for cyber proliferation.

Following a large body of scholarship, policy documents and media reports cyber insecurity seems to be a dominant incentive to go, or not to go, 'cyber'.[408] There has always been an oscillation between

[403] Neil McAllister, "Bruce Schneier: 'We're in early years of a cyber arms race'," *The Register*, (2015) pp.1-4
[404] Joseph S. Nye Jr., "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly*, 5:4 (Winter, 2011): 18-33, p. 35
[405] Kenneth Waltz, *A Theory of International Politics*, (New York: McGraw-Hill: 1979); John J. Mearsheimer, *The Tragedy of Great Power Politics*, (New York: W.W. Norton & Company: 2001)
[406] Janice Gross Stein, "Threat Perceptions in International Relations," in Leonie Huddy, David O. Sears, and Jack S. Levy (eds.) *The Oxford Handbook of Political Psychology*, (Oxford: Oxford University Press: 2013).
[407] Cohen opens his article stating that "[t]hreat perception is the decisive intervening variable between action and reaction in international crisis. " Raymond Cohen, "Threat Perception in International Crisis," *Political Science Quarterly*, 1(1978)93-107, p.93; also see: Robert Jervis, *Perception and Misperception in International Politics*, (Princeton: Princeton University Press:1976); Robert Jervis, "War and Misperception, " *Journal of Interdisciplinary History*, 18(1988):675-700; Joseph Nye Jr., "Transformational Leadership and U.S. Grand Strategy," *Foreign Affairs*, 85(2006):139. Barry Buzan, "Will the 'Global War on Terror' Be the New Cold War?," *International Affairs*, 82 (2006):1102-1118.
[408] According to one poll, almost half of U.S. national security leaders believe that cyber warfare is the most serious threat facing the country at the moment. More specifically, Cyberwarfare received 45.1% of the votes, far more than terrorism (26.3%) and "China" with (14.3%). Also, on a daily basis one can find an article in the newspaper discussing

seeing cyberspace as a land of possibility and opportunity, and a space of threats and security.[409] In many early uses of the term, cyberspace reflected a sense of progress and modernity, a new step in history. Mjolnes called cyberspace the new 'land of opportunity' and Aufderheide refers to it as the 'land of knowledge' with the ability to empower every person to pursue its call.[410] Yet, this view of its benefits has increasingly been tempered with the recognition that cyberspace is 'a dangerous world', what Deibert call the "dark side of cyberspace".[411] For most, today, cyberspace implies threats and danger rather than opportunity.[412] Indeed, military officials have frequently referred to cyberspace as the new 'battlespace' and 'warfighting domain'.[413]

This has led to, what might be called, 'reactive proliferation pessimism'.[414] Some scholars and policy analysts believe that one state's pursuit of a sophisticated cyber arsenal sets off an arms race with other (regional) actors.[415] Indeed, the conception is that the adage 'proliferation begets proliferation' not only captures the conventional wisdom for nuclear weapons but cyber weapons too.[416]

Perceived insecurity, more generally, may also be a motive for the development of cyber weapons in accordance with the framework.[417] Some consider offensive cyber capabilities to be a new means to

---

a cyber event . Over 1000 articles were published in the English language newspapers over a three month period with 'cyber security' or 'cybersecurity' in the headline. See: Lexis Nexis newspaper database, results from 5th of February 2016 to 5th of May 2016. DefenseNews, "Poll 2014: Cyberwarfare Is Top Threat Facing US," (2014, January 5), retrieved from: http://www.defensenews.com/article/20140105/DEFREG02/301050011/Poll-Cyberwarfare-Top-Threat-Facing- US

[409] This paragraph relies on Shires and Smeets, "What do we talk about when we talk about 'Cyber'?"; also see Betz and Stevens, *Cyberspace and the State*, p. 10

[410] Patricia Aufderheide, *Communications Policy and the Public Interest: The Telecommunications Act of 1996*, (Guilford Press: New York City:1999), p. 242; Stig F. Mjolsnes, *A Multidisciplinary Introduction to Information Security*, (CRC Press: London: 2011), p. 245

[411] Ronald J. Deibert, "The Growing 'Dark Side' of Cyberspace," *Penn State Journal of Law and International Affairs*, 1:2(2012) 260-274.

[412] Shires and Smeets, "What do we talk about when we talk about 'Cyber'?"

[413] See Edward C. Cardon, "The Future of Army Maneuver - Dominance in the Land and Cyber Domains," T*he Cyber Defense Review*, 1:1 (2016), 15-21

[414] As Sagan writes, "[a]lthough nuclear weapons could also be developed to serve either as deterrents against overwhelming conventional military threats or as coercive tools to compel charges in the status quo, the simple focus on states' responses to emerging nuclear threats is the most common and most parsimonious explanation of nuclear weapons proliferation." Sagan, "Why Do States Build Nuclear Weapons?," p. 57 Also See: Philip Bleek, "Does proliferation beget proliferation? Why nuclear dominoes rarely fall" *PhD Dissertation Georgetown University*, (2010)

[415] Limnéll, "The cyber arms race is accelerating - what are the consequences?"; Damian Paletta, Danny Yadron and Jennifer Valentino-DeVries, "Cyberwar Ignites a New Arms Race," *The Wall Street Journal*, (2015, October 11), retrieved from: https://www.wsj.com/articles/cyberwar-ignites-a-new-arms-race-1444611128; Nick Allen, "Barack Obama warns of Cold War-style 'cyber arms race' with Russia," *The Telegraph*, (2016, September 5), retrieved from: http://www.telegraph.co.uk/news/2016/09/05/barack-obama-warns-of-cold-war-style-cyber-arms-race-with-russia/

[416] This statement was first mentioned by former U.S. Secretary of State George Shultz. See: George Shultz, "Preventing the Proliferation of Nuclear Weapons," *Department of State Bulletin*, 84:2093 (1984), p. 18; Sagan, "Why Do States Build Nuclear Weapons?," p. 57

[417] There is no consensus about the potential destructiveness of cyber weapons . Works supportive of the notion that we are witnessing a cyber revolution concern: David J. Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-power*, (Adelphi Books: Washington DC, 2011); Nicholas Burns and Jonathon Price, *Securing Cyberspace: A New Domain for National Security*, (Aspen, CO: Aspen Institute, 2012); Paul Cornish, David

countervail asymmetry in terms of conventional weaponry.[418] Small and middle powers will naturally seek to develop offensive cyber capabilities with as aim to restore the balance of power and protect their national security interests from external attacks. Like chemical and biological weapons, cyber weapons may be conceived of as the 'poor man's atomic bomb'.[419] Especially for small powers, cyber weapons may offer the best chance in the 21st century to defend themselves against other states - or increase their ability to threaten them.[420]

Taken as a whole, the predominant cause of cyber proliferation under the first framework is insecurity. The premise of the security framework is that states acquire cyber weapons because they perceive themselves to be threatened by other states. Cyber weapons are a way for states to restore the balance of power. Although it is not predefined whether cyber threats or conventional threats are perceived to be the source of this insecurity, the framework's logic is that developing cyber weapons provides a solution. Restraint in developing cyber weapons would be explained as a response to the reduction in threat environment, when 'internal' (or 'external') balancing becomes no longer necessary.

5.2.2 Evidence

Earlier studies provide ample evidence that national security considerations are indeed the predominant driving force for a state to seek cyber weapons.[421] Valeriano and Maness have developed a dataset which aims to capture all cyber incidents and disputes between rival states for the years 2001-2011.[422] Valeriano and Maness look at "[c]yber engagements directed by one state against

---

Livingstone, Clemente, and Yorke, "On Cyber Warfare;" The main sceptics concern: Lindsay, "Stuxnet and the Limits of Cyber Warfare,"; Adam P. Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," *Journal of Strategic Studies*, 35:3(2012); Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies*, 35:1 (2011): 5-32; Thomas Rid, *Cyber War Will Not Take Place*; Martin C. Libicki, *Cyberdeterrence and Cyberwar*, (Santa Monica, CA: RAND: 2009); Martin C. Libicki, C*onquest in Cyberspace: National Security and Information Warfare*, (Cambridge: Cambridge University Press: 2007)

[418] Robert Reardon and Nazli Choucri, "The Role of Cyberspace in International Relations: A View of the Literature," Presented at the 2012 ISA Annual Convention, San Diego, (2012, April 1)

[419] The phrase refers to a study on whether chemical and biological weapons serve as substitutes or complements of nuclear weapons for states. I however do not imply that cyber weapons have to be perfect substitutes of nuclear weapons for the security framework to hold. Michael C. Horowitz and Neil Narang, "Poor Man's Atomic Bomb? Exploring the Relationship between 'Weapons of Mass Destruction'", *Journal of Conflict Resolution*, 00:0 (2013) 1-27; Note that the 'poor man's atomic bomb' could not only refer to security arguments (i.e. a cheap alternative for attack), but also prestige (see framework 3).

[420] Ibid

[421] There are few - if any - states which argue that the general security threat has led to the development of cyber weapons.

[422] Valeriano and Maness dataset is said to be the most comprehensive - and only - dataset to date on rivalry between cyber state. Brandon Valeriano, and Ryan Maness, "The dynamics of cyber conflict between rival antagonists, 2001-2011," *Journal of Peace Research*, 51:3 (2014)347-360.

another" in order to "determine which rival states have been using cyber tactics and where these attacks are directed".[423] It can serve as an indicator for when states are most likely to use cyber proliferation as internal effort to balance against other actors.[424] Key dyadic rival states include: U.S. - China, Israel - Iran, Pakistan - India, South Korea - North Korea, and U.S. - Russia.[425]

Delving into a number of these cases provides some evidence in favour of the reactive proliferation thesis. Some states have reportedly initiated a cyber program as a direct result of their 'dyadic relationship', having previously been victim of large scale cyber-attacks from their 'rival' state. This argument has been most prominently put forward with regards to the military cyber programs of Iran. "Since the Stuxnet attack," Siboni and Korenfeld write, Iran "has been working hard to improve its cyberspace defences on the one hand, while building up cyberspace intelligence gathering and offensive capability on the other."[426] Interestingly, the claim that Iran's program is a direct reaction to earlier incidents is supported by leaked documents from the Western intelligence agencies.[427] To institutionally back up its sparked interest in cyber weapons, in 2010, Iran created the 'Commando for Cyber Defence' which ultimately falls under the jurisdiction of the army's Chief of Staff.[428] And in March 2012, Ayatollah Khamenei, issued a decree to establish the Supreme Council of Cyberspace

[423] Ibid, p. 347

[424] The study is the most extensive to date, though is suffers from some severe limitations as will be discussed below. A 'cyber incident' refers to an 'individual cyber conflict'. The scholars identify 110 cyber incidents within 45 disputes between 2001 and 2011; A follow-on study concludes that "Our findings suggest that these state dyads have indeed been engaged in cyber arms races, as defined by their competitive and above-normal mutual increase in cyber capabilities." See: Brandon Valeriano and Anthony Craig, "Conceptualising Cyber Arms Races," in Nikolaos Pissanidis, Henry Rõigas, Matthijs Veenendaal (Eds.), *8th International Conference on Cyber Conflict Cyber Power* (Tallinn: NATO CCD COE Publications: 2016), p. 141

[425] The main results of the study are the following (number of initiated incidents by the state can be found between brackets): China (20) vs. U.S. (3); Pakistan (7) vs. India (6); North Korea (10) vs. South Korea (1); Israel 7 vs. Iran (4); China (7) vs. Japan (0); South Korea (4) vs. Japan (3); U.S. (6) versus Iran (1); China (5) vs. Taiwan (0); China (4) vs. India (0); Russia (3) vs. Georgia (1); Russia (4) vs. Estonia (0); Russia (3) vs. U.S. (0); North Korea (3) vs. U.S. (0); China (2) vs. Vietnam (0); Lebanon (1) vs. Israel (1); North Korea (1) vs. Japan (0); India (1) vs. Bangladesh (0); Syria (1) vs. U.S. (0); Kuwait (1) vs. Iraq (0); China (1) vs Philippines (0). See: Valeriano, and Maness, "The dynamics of cyber conflict between rival antagonists"

[426] In chapter 4 it was noted that Iran has also been hit by Wiper attacks. Gabi Siboni and Sami Kronenfeld, "Iran and Cyberspace warfare," *Military and Strategic Affairs,* 4:3 (2012)101-117

[427] As an NSA document states, " Iran continues to conduct distributed denial-of-service (DDOS) attacks against numerous U.S. financial institutions, and is currently in the third phase of a series of such attacks that began in August 2012," the document says. "SIGINT indicates that these attacks are in retaliation to Western activities against Iran's nuclear sector and that senior officials in the Iranian government are aware of these attacks." See: Glenn Greenwald, "NSA Claims Iran Learned from Western Cyberattacks," *The Intercept,* retrieved from: https://theintercept.com/2015/02/10/nsa-iran-developing-sophisticated-cyber-attacks-learning-attacks/

[428] Pheonix TS, "The Iranian Cyber Threat ," (2013, September 12), Retrieved from: https://phoenixts.com/blog/the-iranian-cyber-threat-part-1-irans-total-cyber-structure/

which is composed of various senior officials in an effort to plan and implement an integrated cyberspace strategy.[429]

Similarly, South Korea's program is said to be directly geared towards countering North Korea's threatening actions in cyberspace.[430] According to a reporter, the South Korean government has already warned of the growing cyber threat (but initially used the term 'infowar') from North Korea since at least 1994.[431] South Korea's Ministry of National Defence created a Cyber Command in 2010, at a time when the alleged frequency and sophistication of North Korean cyber activity began increasing.[432] A spokesman at South Korea's Ministry of National Defence iterated on numerous occasions that the establishment of the command is part of a direct counterstrategy against North Korean hacking.[433]

There is also empirical evidence of a different form of reactive proliferation. The desire of the PLA's leadership to modernize its military and develop 'cyberwarfare' capabilities since the 1990s is said to be the direct result of American activities in the Gulf. Hence, what triggered the government to explore the development of cyber weapons were not attacks against its own country, but developments seen in another conflict and region. As George Patterson Manson, III writes in more detail:

> the wake-up call for Chinese leaders came in the early 1990s, when military planners in Beijing watched the U.S.-led coalition dismantle Saddam Hussein's army with relative ease, seizing control of the battlefield with superior information systems and 'smart' strike capabilities made possible by the integration of computer network technology and military hardware, enabling complex logistical and combat operations and providing coalition forces with unmatched near real-time intelligence. The war demonstrated to Chinese leaders just how far behind the state-of-the-art their own conventional capabilities had become, and Chinese

[429] Center for Human Rights in Iran, "Khamenei Consolidates Power over Internet Policy in Hard Line Council He Controls," (2015, September 14), retrieved from: https://www.iranhumanrights.org/2015/09/khamenei-internet-policy-iran/

[430] Though it has also been victim of cyber attacks from other countries.

[431] Brian McWilliams, "North Korea's School for hackers," (2003, June 2), *Wired*, retrieved from: https://www.wired.com/2003/06/north-koreas-school-for-hackers/

[432] Zachary Keck, "South Korea Seeks Offensive Cyber Capabilities," *The Diplomat* , (2015, October 11), Retrieved from: the diplomat.com/2014/10/south-korea-seeks-offensive-cyber-capabilities;

[433] As part of the counterstrategy against North Korea, South Korea implemented various measures to protect its intranet. According to a South Korean spokesman: "The intranet used for military manoeuvres can only be accessed by a small number of people. […] Thus, it is very secure and couldn't fall victim to North Korean hacking." Yet, in 2016, various reports noted that the South Korea's Cyber Command was in fact hacked by North Korean hackers. Jennifer Chang, "US, South Korea join forces to prevent cyberattacks by North Korea," PC World / IDG News Service, (2013, April 3), retrieved from: http://www.pcworld.com/article/2032918/us-south-korea-join-forces-to-prevent-cyberattacks-by-north-korea.html; BBC News, "North Korea 'hacks South's military cyber command," (2016, December 6), retrieved from: http://www.bbc.com/news/world-asia-38219009

> strategists were soon referring to Operation Desert Storm by the name z*hongda biange*, the 'great transformation.'[434]

Here the hostile interaction between two rivalry states - depicted in Valeriano and Maness' dataset between the U.S. and China - only becomes of relevance in a later period. Indeed, today's debate is not about whether or not to develop capabilities in response to the other's threatening actions, but whether to retaliate or not.[435]

Much has been written in Western media about Chinese 'aggressive' actions in cyberspace. Yet, as Lindsay writes, "[t]o a Chinese audience, American allegations of cyber threats from China often sound like 'a thief crying stop thief.'"[436] Lindsay cites leaked documents from former contractor Edward Snowden that the NSA infiltrated into the headquarters of Huawei in Shenzhen with as aim to exploit the routers and switches.[437] A similar point is made by Chinese PLA scholar Ye Zheng, citing NSA's PRISM information-collection program and Quantum Program - also disclosed by Snowden - to show how the U.S. threat is perceived by other countries, including China.[438]

Despite its differences, in all the above cases states' cyber proliferation is triggered by offensive cyber activities from another state. So how could the early cases of proliferation, especially the US' pioneering development of offensive capabilities, be explained through the notion of 'reactive proliferation'? There is evidence to suggest that the U.S. is an example of a case where actors do not respond to *actual* developments, but to the *fear* of what other actors might be able to do. U.S. Cyber Command historian (and former CIA historian) Michael Warner writes that U.S. inclination around

---

[434] George Patterson Manson III, "Cyberwar: The United States and China Prepare For the Next Generation of Conflict," *Comparative Strategy*, 30:2(2011)121-133, p. 121; also see: Gurmeet Kanwal, "China's Emerging Cyber War Doctrine," *Journal of Defence Studies*, 3:3(2009)14-22

[435] It seems that the U.S. is still lacking a viable strategy in terms of how to respond against the attack. As an article from the New York Times states, "officials have struggles to choose among options that range from largely symbolic responses to more significant actions unless the U.S. finds a way to respond to the attacks, they are bound to escalate." The discussion became especially prominent following the Office of Personnel Management hack. See: David Sanger, "U.S. Decides to Retaliate Against China's Hacking," *The New York Times*, (2015, July 31), retrieved from: https://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html?_r=0; Jack Goldsmith, "The United States' Feckless Cyber Deterrence Policy," *Lawfare*, (2015, August 1), retrieved from: https://www.lawfareblog.com/united-states-feckless-cyber-deterrence-policy; Adam Segal, "Retaliating Against China's Great Firewall," *Council on Foreign Relations: Net Politics*, (2015, August 3), retrieved from: https://www.cfr.org/blog-post/retaliating-against-chinas-great-firewall;

[436] Jon Lindsay, "Espionage and Cybercrime" in Jon R. Lindsay, Tai Ming Cheung, Derek S. Reveron (Eds.), *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, (Oxford: Oxford University Press: 2015)

[437] Ibid, p. 3

[438] PLA-scholar Zheng also provides another much telling statement: "[w]hile it is common, even expected, that countries carry out intelligence activities, taking advantage of information and network technology to openly implement a wide range of monitoring, such as PRISM and the 'Quantum' program, is very rare. The United States sets a bad example." Ye Zheng, "From Cyberwarfare to Cybersecurity in the Asia-Pacific and Beyond," in Jon R. Lindsay, Tai Ming Cheung, Derek S. Reveron (Eds.), *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, (Oxford: Oxford University Press: 2015), Also see: Nicholas Weaver, "A Close Look at the NSA's most powerful internet attack tool," *Wired*, (2014, March 13), Retrieved from: https://www.wired.com/2014/03/quantum/

the development of offensive cyber capabilities evolved in four phases.[439] In the 1960s, the U.S. government realized that "[c]omputers can spill sensitive data and must be guarded".[440] The decade after in the 1970s, there was a growing awareness that "[c]omputers can be attacked and data stolen." In the 1980s and 1990s the government realized that "[w]e can build computer attacks into military arsenals."[441] Yet, in the 1990s the government also realized that "[o]thers might do that to us - and perhaps already are."[442] Pulitzer Prize-winning reporter Fred Kaplan in *Dark Territory* draws a similar conclusion reviewing the U.S. history of 'cyberwar', even though he more directly connects the moment of 'awareness' to Russian activities.[443] As he states, "[i]t took a while, but as more of these vulnerabilities were discovered, and as more evidence emerged that Soviet spies were exploiting them, a disturbing thought smacked a few analysts inside NSA: Anything we're doing to them they can do to us."[444] In other words, it can be said that the U.S. own early *offensive* activities led to a new interpretation of its defences.

There are however considerable grounds to question the explanatory power of this national insecurity narrative of cyber proliferation. In a review of Ernest May's book *Lessons of the Past,* Arthur Schlesinger writes that "[t]he past is an enormous grab bag with a prize for everybody. The issue of history as rationalization somewhat diminishes the force of the argument that history is per se a powerful determinant of policy."[445] This statement is particularly relevant for the cyber realm; given the number of (small) cyber attacks which occur on a daily basis, it is easy to point to one incident as the catalyst for a state to develop an offensive cyber capability.

Also, the large-N data about states' reactive cyber interactions is far less convincing than what many scholars conceive it to be. As said, the 'dynamics of cyber conflict dataset' developed by Valeriano and Maness is the largest and most-cited and statistical analysis on 'states cyber rivalry'.[446] Yet, few sources provided in the study's codebook actually provide evidence (or cite an expert or policy-

[439] Warner, "Cybersecurity: A Pre-history,"
[440] As Warner also notes, [i]n 1967, DSB asks for report on computer security. The Defense Science Board in October 1967 asked Ware to lead a study group examining the problem. Its then-classified report, published by the RAND Corporation in early 1970, warned there would be no engineering solution to the problem of computer security." Ibid, p. 784
[441] Ibid, p. 782
[442] Ibid, p. 782
[443] Fred Kaplan, *Dark Territory*
[444] Kaplan, *Dark Territory*, p.17
[445] This issue echoes the debate on the use of historical analogies in decision making. For some, decision makers can resort to analogies to help them deal with the present and in this way learn from history. Others, like Schlesinger, are more sceptical in Yuen Foong Khong, *Analogies at War: Korea, Munich, Dien Bien Phu and the Vietnam Decisions of 1965,* (1992: Princeton University Press, Princeton, New Jersey)
[446] Valeriano and Maness, "The dynamics of cyber conflict between rival antagonists"

maker) that a state actor or state-sponsored actor was behind the attack. [447] The scholars, for example, list twelve 'cyber incidents' between India and Pakistan. Yet, in *none* of these incidents a state-actor was likely behind the attack. It mostly concerned acts of hacktivism from groups giving themselves names like 'India Cyber Force' or 'Pakistan Cyber Army' (PCA). These groups do not need to have any state connection (hence, they should also not be called 'proxy actors') and are often not even from these countries. For example, the Pakistan Cyber Army and the Muslim Liberation Army, both cited by Maness and Valeriano, have numerous members in Saudi-Arabia, the United States and Europe.[448] If I would start the *Iceland Hacking Army* with my Dutch nationality and rent a Russian-operated botnet for a few hours (see chapter 4) from a library in Oxford, UK to attack a website in Greenland, it would be coded in the *Dyadic Cyber Incident and Dispute Dataset*.[449] These coding errors lead to a significant bias in favour of the security imperative; it overestimates state rivalries and arms race dynamics and it dismisses the agency of other non-actors.

Finally, even with the dataset being biased towards overestimating the number of incidents from state-actors, the number of coded retaliatory actions remains extremely low.[450] Of the nineteen main cyber disputes among rival states listed between 2001 and 2011, in *twelve* cases 'rival A' state has repeatedly conducted cyber operations but there was *no* cyber response of 'rival B'.[451] Furthermore, in those cases where a retaliatory action did take place, we witnessed a highly asymmetric, minimal response rather than tit-for-tat behaviour. Although this observation on its own is insufficient to reject

[447] Overall, the coding seems to be conducted in both an undiligent and biased manner. For example, consider the following cyber incidents listed in the dataset: i) 'US banks hacked'; this only remains speculation it was state-led operation, ii) 'Twitter hack'; a message from the attackers calling themselves 'Iranian Cyber Army' is used as the only source. There is no other evidence which suggests that actually a government entity is behind the attack; iii) 'Iran network infiltration', 'Operation Newscaster', 'Operation Ababil', 'Saffron Rose' and 'NMCI hack'; the report(s) cited for these incident only state that it is an operation "undertaken by a coordinated and determined group"; iv) 'Commerce theft' and 'White House theft'; for both incidents it remains unclear who was behind the attack; v) 'Senator Nelson theft'; the cited article only states that it had been traced back to China, but does not explicitly attribute it to the government; vi) 'Commerce disabled'; the source only states that these were "targeted attacks originating from China", again not attributing it to the government; vii) 'Commerce Sec hack'; the source only mentions that malware was found a device of then Commerce Secretary Carlos Gutierrez and several other officials following a trade mission to China. Finally, in various other cases, we know from other sources that a state actor was in fact behind the attack, but these sources are not cited in the dataset (for example, Stuxnet 0.5 and Duqu).

[448] In a number of these cases, the actors do not even seem to have a political motivation. An example is the incident 'Worm Infiltrates Pakistan govt'. The source cited by Maness and Valeriano notes that the hack was likely not politically motivated given the messages. Instead, they were "childish squabbles [...] fought on the computers of incident computer users, uninterested in the disagreement."

[449] How this case would exactly be coded is unclear from Valeriano and Maness' codebook. The only reason this specific case would be excluded is because there is no historic rivalry between Greenland and Iceland (the dataset is narrowed to states which are rivals). Narrowing the analysis in this manner is another problem of the dataset After all, an important dimension of cyber conflict is that it may open up new forms of rivalry we have not witnessed before. The scholars are unable to test this, although they make a number of claims about it. See for example: Maness and Valeriano, "The dynamics of cyber conflict between rival antagonists," p. 348

[450] Although this is not a perfect indicator of reactive proliferation, it suggests that reactive proliferation has been much rarer than historically perceived.

[451] Ibid

the security imperative, it is another indicator that reactive proliferation has historically been far rarer than many reports purport it to be.

Estonia is a most-likely case for the security imperative.[452] Since the collapse of the Soviet Union, Estonia has felt threatened by its neighbour; the country is fearful that its sovereignty is not recognized by Russia which has a strategic interest in dominating the Baltic Sea and the Black Sea regions. [453] The confrontational course came to its head in 2007 when Russia conducted a large-scale DDoS attack against the country, which is one of the most digitally advanced (and reliant) in the world.[454] (also see chapter 4). The attacks have been intensively studied by policy analysts and scholars, and have triggered a range of actions. Estonia formed its first ever Cyber Security Strategy Committee in the aftermath of the attacks and published its first Cyber Security Strategy in 2008. In addition, a year after the attacks the NATO Cooperative Cyber Defence Centre of Excellence was established in Tallinn. Estonia also has a voluntary organization aimed at protecting its cyberspace, called the Estonian Defence League's Cyber Unit.[455] Yet, following the attacks, it did *not* respond to Russia with retaliatory cyber activity, nor did the government initiate a cyber command or other program to develop offensive cyber capabilities.

There are two potential, related explanations for the weak security imperative. First, as Hymans notes in a review on nuclear proliferation, the 'hard' realist point or view is that "in international anarchy the 'absolute weapon' is so obviously beneficial for states that only supply-side factors […] hold them back. As Adam Liff notes, despite calls of cyber weapons being a tool for empowerment, "cyberwarfare is not a new 'absolute weapon' [:] Although Stuxnet manifests cyberwarfare's potential to become a useful brute force measure, no examples of irrefutably effective coercive [computer network attacks (CNA)] exist."[456]

Second, there is a near-consensus view among scholars that cyber weapons fail to provide an effective deterrence. The theory of nuclear deterrence rested upon the conviction that a credible threat of

[452] Harry Eckstein, "Case Studies in Political Science," in Alexander L. George and Andrew Bennet, *Case Studies and Theory Development in the Social Sciences* (Cambridge, MA: MIT Press: 2004)
[453] Estonia also has a large Russian speaking population. Moscow states it aims to defend this group regardless of their citizenship. Official bilateral relations between the two countries have been close to non-existent.
[454] As Kadri Liik writes, "[t]he actual roots go much deeper back in time, and in order to understand those, one must look to the disputes between the two countries that started soon after Estonia's restoration of independence." Kadri Liik, "The 'Bronze Year' of Estonia-Russia relations," International Centre for Defence Studies, (2007), retrieved from: https://www.icds.ee/fileadmin/media/icds.ee/failid/Kadri_Liik_Bronze_Year.pdf
[455] Kadri Kaska, Anna-Maria Osula, Jan Stinissen, *The Cyber Defence Unit of the Estonian Defence League Legal, Policy and Organisational Analysis*, (NATO Cooperative Cyber Defence Centre of Excellence Publications: Tallinn: 2013)
[456] Ibid, p. 426

retaliation - and possible mutually assured destruction (MAD) - would forestall an enemy attack. This notion underlying deterrence - that a second strike capability provides the best possible form of security - provides the ultimate argument about why proliferation begets proliferation. Numerous scholars observed, however, that it is much more difficult to achieve cyber deterrence.[457] This means the incentives to 'go cyber' when a rival state has developed offensive cyber capabilities are less significant - even when statements of policymakers might sometimes suggest otherwise.

Overall, the importance of the national security imperative is largely overblown. Many analysts overstate the degree of reactive proliferation and consequently overestimate the significance of the national security imperative. At most, cyber proliferation by rivals makes states modestly more motivated to proliferate. This weak stimulus seems to be insufficient to push most states over the hurdles of establishing a program to develop sophisticated cyber weapons - especially small powers lacking large defence budgets.

5.3 The Domestic Politics Imperative

5.3.1 Theoretical Framework

Many proponents of the neorealist school of thought recognize that it is unable to provide a fine-grained analysis of foreign policy behaviour. In fact, Waltz explicitly attempts to 'black box' states to provide a structural theory of international systems.[458] Decision making approaches in IR challenge the premise that to conceptualize states as unitary actors.[459]

[457] In this discussion a few mechanisms and concepts are collapsed in one, as failure of cyber deterrence has at least two different meanings in the literature; i) the difficulty of deterring cyber attacks and ii) the difficulty of using cyber weapons to deter other actors.

[458] Waltz uses the analogy of markets and firms. See; Waltz, *A Theory of International Politics;* a critique of conflating different levels of analysis is originally provided in*: Kenneth* Waltz*, Kenneth, Man, the State and War* (New York: Columbia University Press, 1959).

[459] These studies are far from uniform on how and which domestic pressures and constraints (such as political parties, public opinion, elite maintenance, or interests groups) play a central role in shaping the behaviour of states. In line with earlier arms proliferation research, this study primarily focuses on the role of interest groups. It would be difficult to justify a focus on public opinion as a key domestic driver since opinion polls show that the public is rather disinterested in cybersecurity matters and has relatively little knowledge about it. The media also seems to play a limited role in shaping cyber policy. Journalists often rely on reports from cyber security firms and have a limited familiarity with technical concepts. See: Kenneth Olmstead and Aaron Smith, "What the Public Knows About Cybersecurity," *Pew Research Center*, (2017, March 22), retrieved from: http://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/

Following a burgeoning literature, the domestic politics framework gauges the domestic considerations which could potentially influence cyber proliferation.[460] The starting observation of the domestic politics imperative is that the state is not a monolithic entity but rather a loose constellation of allied organizations. Individuals and organizations compete for resources and interests *within* a state.[461] As Joseph Nye Jr. states, "[n]ew technologies raise new issues in civil-military relations. Different parts of complex institutions like governments learn different lessons at different paces, and new technologies set off competition among bureaucracies."[462]

The private sector is said to play a critical role in cyber security activities.[463] Studies have also shown that the expansion of the arms-producing companies into the cybersecurity market is a clear trend in the top of the arms production pyramid.[464] It has led some to suggest that there is the emergence of a 'cyber-industrial complex'.[465] As Jerry Brito and Tate Watkins write, "a cyber-industrial complex is emerging, much like the military-industrial complex of the Cold War. This complex may serve to not only *supply* cybersecurity solutions to the federal government, but to *drum up demand* for them as well."[466]

---

[460] The framework here builds upon Moravcsik's work; it fuses 'commercial liberalism' (market incentives are the source state preferences) and 'republican liberalism' (domestic political institutions affect state preferences) to explain cyber proliferation. Note that the ideational version of liberalism, as proposed by Morvcsik, is more closely aligned with the third framework of cyber proliferation. Andrew Moravcsik, "Taking Preferences Seriously: A Liberal Theory of International Politics," *International Organization*, 51:4(1997) 513-553;

[461] As Sagan writes, "[r]ealists recognize that domestic political actors have parochial interests, of course, but argue that such interests have only a marginal influence on crucial national security issues. […] Security threats are [...] not the central cause of weapons decisions according to this model: they are merely windows of opportunity through which parochial interests can jump. Sagan, "Why Do States Build Nuclear Weapons?," p. 65

[462] Nye Jr., "Nuclear Lessons for Cyber Security?," p. 26

[463] These do not just include defense contracts, but possibly also communications and technologies, trade organizations, and other interests. Perhaps the most-often raised issue is that the public and private sector should work together in defending critical infrastructure against potential cyber-attacks. James P. Farwell, "Industry's Vital Role in National Cyber Security," *Strategic Studies Quarterly* (2012): 10-41. Also see: Melissa Hathaway, "Leadership and Responsibility for Cybersecurity", *Georgetown Journal of International Affairs*, (2012):71-80; Sue Eckert, "Protecting Critical Infrastructure: The Role of the Private Sector," University of Pittsburg (2006), retrieved from: http://www.ridgway.pitt.edu/Portals/1/pdfs/Publications/Eckert.pdf; Kenneth Neil Cukier and Viktor Mayer Schoenberger, and Lewis M. Branscomb, "Ensuring (and Insuring?) Critical Information Infrastructure Protection," *Working Paper, John F. Kennedy School of Government, Harvard University*, (2005, October 11).

[464] Vincent Boulanin, "Cybersecurity and the arms industry," *SIPRI Yearbook 2013: Armaments, disarmament and international security* (Oxford: Oxford University Press: 2013), pp. 218-226;

[465] The Economist, "Hiring Digital 007s: A new cyber-industrial complex is rising," (2013, June 13), retrieved from: http://www.economist.com/news/business/21579465-new-cyber-industrial-complex-rising-should-you-worry-hiring-digital-007s; Peter W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know?* (Oxford University Press: New York: 2014), p. 162; Chris Strohm, "Lockheed to Boeing Building Security-Industrial Complex," *Bloomberg Business*, (2013, June 10), Retrieved from: https://www.bloomberg.com/news/articles/2013-06-10/lockheed-to-boeing-building-security-industrial-complex

[466] Emphasis added. Jerry Brito and Tate Watkins, "The Cybersecurity-Industrial Complex," *Reason*, 43:4 (2011):1-39, p.1

Competing interests and incentives, affecting demand, may not just exist between the government and private sector, but also *within* the government.[467] As David Baldwin notes in his classic article, security inherently comes at a cost.[468] It is just one of the many important policy objectives competing for scarce resources and subject to the law of diminishing returns.[469] Not only do governments have to make policy trade-offs *between* security and other values - such as health and industrial productivity - also *within* security - such as between cyber security and counterterrorism.[470] Intelligence services might benefit from a stronger focus on offensive cyber operations, whereas conventional military services might find their share in 'modern warfare' declining.

In sum, from the perspective of the domestic politics framework, cyber proliferation is driven by competing interests and incentives *within* the state. An essential feature of the framework is that actors - both private and public - are unable to entirely rise above their institutional perspectives and focus on the public good.[471]

5.3.2 Evidence

With a flourishing cyber security industry, large conventional arms industry, well-respected professional military constituency, and historically significant intelligence apparatus, the United States is undoubtedly a most-likely case for the domestic politics imperative. Various actors within the state seem to have a vested interest developing cyber weapons.

In the introduction of his book *Dark Territory,* Kaplan writes that he aims to uncover the history of cyber warfare in the United States, as the subtitle also suggests *A Secret History of Cyber War*.[472] Although it largely fails to achieve this aim, the work does offer an excellent overview of the turf

[467] The domestic politics framework of the demand side analysis is primarily aligned with studies on interest groups. However, the literature on bureaucratic politics - specifically on organizational routines and standard operational procedures - may also provide valuable insights. It could aid our understanding to what degree the *design* of a cyber weapon is merely the product of rational actors or whether also other factors play a role.
[468] David Baldwin, "The Concept of Security," *Review of International Studies*, 23 (1997)5-26
[469] Ibid
[470] Catalysed by the Snowden revelations, various scholars, policy-makers and media officials have assessed the *quid pro quo* between security and privacy (i.e. between security and other values). Yet, the trade-offs between cyber security and counterterrorism (i.e. within security) has not been studied enough from a theoretical perspective. It could be argued that pressure placed by governments on companies to weaken their encryption codes has allowed governments to more easily gather information on potential terrorists. Yet, in turn, by making information systems (especially end-user applications) weaker than they could be, it increases the vulnerability of computer networks. In other words, the far-reaching policies of internet surveillance after 9/11 do not make countries more secure *in general*; it makes countries more secure against a *particular* kind of threat.
[471] Graham T. Allison and Philip Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis*, (Pearson Education:1999)
[472] Kaplan, *Dark Territory*

battles fought over who should be responsible for cyber warfare.[473] More specifically, a better title of Kaplan's book would be 'Dark Territory: A History of how the NSA rose to Power'. Having its roots in the First World War, the NSA was officially established in 1952 to intercept foreign communications.[474] As Kaplan's account shows, the NSA gradually wielded more power; by establishing bases around the world throughout the Cold War;[475] taking sole control of computer based intelligence in the early 1980s;[476] receiving the authority to establish security standards for all telecommunications and computers following NSDD-145;[477] making itself indispensable in counter-command and control warfare;[478] becoming superior in Tailored Access Operations (TAO);[479] receiving almost unlimited financial resources (especially following NSPD-54, in which the bulk of the $17.3 billion went to the NSA);[480] being recognized as the authority ultimately in control of defending networks (as Buckshot Yankee demonstrated);[481] becoming effectively the 'brother' organization of the newly established U.S. Cyber Command (not least because of the dual-hat role); and playing a key role in developing the most sophisticated cyber weapon discovered to date (Stuxnet).[482] "On October 31, 2010," as Kaplan concludes, "U.S. Cyber Command raised its flag at Fort Meade, with General Alexander at the helm while, simultaneously, entering his sixth year as director of an NSA that was teeming with unprecedented political, bureaucratic, and computational power."[483] What the domestic politics model highlights above all, in the case of the US, is how the intelligence apparatus has a vested interest in expanding its powers - moving ever more closely to playing a key role in the development of cyber weapons.[484]

Of course, the integration of offensive cyber capabilities - with the intelligence apparatus expanding its role and taking the lead - provides certain obvious benefits. Not least because there is little

[473] The author does delve into the any of the actual offensive operations. Also see: Ben Buchanan, "A not-so Secret History of Cyber War," *War on the Rocks*, (2016, June 30), retrieved from: https://warontherocks.com/2016/06/a-not-so-secret-history-of-cyber-war/

[474] Its two main directorates were 'Signals Intelligence' and 'Information Security'. It was later called 'Information Assurance'.

[475] Kaplan, *Dark Territory*, p.12

[476] Ibid, p. 27

[477] Ibid, p. 27

[478] Ibid, p. 33 and p. 135. And later the establishment of the Office of Tailored Access Operations (TAO).

[479] Ibid, p. 135-137

[480] Ibid, p. 178-179

[481] As Kaplan notes, "[i]n 2011, When Robert Gates realized that the Department of Homeland Security would never be able to protect the nation's critical infrastructure from a cyber attack (and after his plan for a partnership between DHS and the NSA went up in smoke), he gave that responsibility to Cyber Command as well." Ibid, p. 280

[482] Ibid, p. 217, 184-185; I have avoided using the term 'parent' organization here as one could point to the fact the Cyber Command is a sub-unified command of StratCom and thus regard StratCom as a 'parent.'

[483] Ibid, p. 189

[484] Also notice that the Cyber Command was established at a time when DoD was facing significant budget cuts - from $721 billion in 2010, to $717 billion in 2011, down to $681 billion in 2012 and $610 billion in 2013.

difference between - what in intelligence jargon is called - Computer Network Exploitation (CNE) and Computer Network Attack (CNA).[485] In fact, as former NSA and CIA director Michael Hayden states:

> Reconnaissance should come first in the cyber domain too. How else would you knowwhat to hit, how, when - without collateral damage? But here's the difference. In the cyber domain the reconnaissance is usually a more difficult task than the follow-on operation. It is tougher to penetrate a network and live on it undetected while extracting large volumes of data from it than it is to, digitally speaking, kick in the front door and fry a circuit or two. […] Let me go further. An attack on a network to degrade it or destroy information in it is generally a lesser included case of the technology and operational art needed to spy on that same network.[486]

There may be other benefits too. Not only can organizational integration of offensive cyber capabilities (OIOCC) lead to interaction efficiency of intelligence and military activities, it can also increase the opportunity for knowledge transfer, minimize mission overlap and improve resource allocation.[487] But all these benefits come at the risk of - what can be labelled as - 'cyber mission creep'; when initial intelligence activities through cyberspace go beyond their core mission and lead to the development and use of cyber weapons.[488]

---

[485] The NSA distinguishes between three types of computer networks operations (CNO): i) computer network defense (CND); how to keep your own networks secure, ii) computer network exploitation (CNE), how to steal data from other parties; iii) Computer network attack (CNA); how to destroy data, networks or other physical objects. Also see chapter 2 for discussion on differences in cyber weapon's payload.

[486] Hayden also states: "I can think of no other family of weapons so anchored in the espionage services for their development (except perhaps armed drones)." Hayden, *Playing the Edge*, p. 137

[487] First, as I have written elsewhere, "the interdependence between the intelligence collection activity and the military activity is essential as a great amount of preparation is required to understand the targeted systems. OI facilitates this interaction, making it the most obvious benefit." Second, as I mentioned in chapter 4, the required knowledge component for developing offensive cyber capabilities comes in two form, tacit and explicit. "The tacit knowledge required to conduct offensive cyber activities cannot be formally communicated. Forms of OIOCC, however, allow for the opportunity to also transfer this type of knowledge," according to Smeets. Finally, "OIOCC allows for a more efficient allocation of resources, because the same processes or tasks are not replicated unnecessarily. In any organisation, some overlap in tasks is inevitable; yet OIOCC leads to enhancement resource allocation on three levels. […]First, it can put people to better use. [...] Second, 'capital' can be used more efficiently.[…] Third, and related, OIOCC makes it easier to leverage previous activities and accomplishments". For a more extensive discussion see: Smeets, "Organizational Integration of Offensive Cyber Capabilities: A Primer on the Benefits and Risks"

[488] OIOCC can also intensify the cyber security dilemma and potential cost ineffectiveness in the long run. This inherent temptation is also apparent in Hayden's writing: "The final category of action under computer network operations was computer network attack, or CNA. This was action designed to disrupt an adversary's network or, in its most extreme form, take over the network in order to use it to create some level of physical destruction. NSA still had no authority to do that'; it was limited to defending American information and stealing other people's. But we knew that defense, exploitation, and attack were technologically and operationally indistinguishable even though they were separated in legal authority, funding streams, and congressional oversight - all the result of putting new (digital) wine into old (eighteenth-century, actually) bottles. To us, that made as much sense as America having three air forces - one for reconnaissance, another for fighters, and a third for bombers - when it was really *all* about control of the air." Hayden, *Playing the Edge*, p. 142; For a more extensive discussion see; Smeets, "Organizational Integration of Offensive Cyber Capabilities".

Bruce Schneier already wrote about NSA's potential for mass surveillance mission creep.[489] "Once the NSA's ubiquitous surveillance of all Americans is complete - location data, physical mail, financial transactions, and who knows what else - why limit its use to cases of terrorism?," Schneier asks.[490] In later writing, he notes that there is already evidence that the vast "NSA surveillance apparatus is used for other, lesser, crimes" as other agencies are asking to use NSA data.[491] The point here is that mission creep does not just move down - to lesser 'crimes' - but also moves up - to more severe 'crimes'/attacks.[492]

What is notably left out in Kaplan's account is the role of the private sector in potentially steering demand towards the development of cyber weapons.[493] There is of course widespread recognition that, parallel to the growing prominence of cybersecurity as an issue, there is a growing industry trying to make money from it. The global market size of cyber security products and services is ever expanding (between 5 to 10 percent a year), and the U.S. market makes up a substantial portion of it.[494] In a recent report, the U.S. Defence Secretary Ashton Carter states that almost $7 billion will be allocated towards the development of cyber capabilities as part of a $528.7 billion budget request to fund the DoD in 2017.[495] The plan is to invest a total of $35 billion over the coming five years into cybersecurity.[496]

[489] Bruce Schneier, "Counterterrorism Mission Creep," *Schneier on Security,* (2013, July 19), Retrieved from: https://www.schneier.com/blog/archives/2013/07/counterterroris_1.html
[490] Ibid
[491] Bruce Schneier, "NSA Surveillance and Mission Creep," *Schneier on Security,*(2013, August 6) Retrieved from: https://www.schneier.com/blog/archives/2013/08/nsa_surveillanc.html; also see: Cory Doctorow, "Feds admit they used secret anti-terror mass surveillance tool to catch an undocumented waiter," *BoingBoing,* (2017, May 19), Retrieved from: http://boingboing.net/2017/05/19/swatting-jaywalkers-with-tacti.html
[492] The recent Shadowbrokers allegedly show that there is now evidence of this activity too. See: Lorenzo Frenceschi-Bicchierai, "The New Shadow Brokers Leak Connects the NSA to the Stuxnet Cyber Weapon Used on Iran," *Motherboard,* (2017, April 17), Retrieved from: https://motherboard.vice.com/en_us/article/shadow-brokers-nsa-stuxnet-iran
[493] As it was observed at the annual State of the Field Conference of Cybersecurity studies in 2016, scholarship has generally failed to discuss the role of the private sector in relation to offensive cyber activity. See: Karl Grindal and Jason Healey, "Hand out: Cyber Conflict History," State of the Field of Cybersecurity Studies: Columbia University, (2016, June 15-17)
[494] Brito and Watkins, "The Cybersecurity-Industrial complex"; Singer and Friedman, *Cybersecurity and Cyberwar*; Alec Ross, "Want job security? Try online security," *Wired,* (2016, April 25), retrieved from: http://www.wired.co.uk/article/job-security-cybersecurity-alec-ross
[495] Jeff Stone, "Meet the Cyber-Industrial Complex: Private contractors may get $7B windfall from Pentagon's Cyberwar on ISIS," IB Times, (2016, July 3), retrieved from: http://www.ibtimes.com/meet-cyber-industrial-complex-private-contractors-may-get-7b-windfall-pentagons-2329652
[496] This budget concerns both offensive and defensive capability. Ibid; also see: Lee and Rid, "OMG Cyber!"

There are three principal mechanisms through which the private sector influences the willingness to develop cyber weapons in the United States.[497] First, the private sector - as 'securitizing actor' - influences the threat perception of policy-makers.[498] As Robert Lee and Thomas Rid write, "cyber is piping hot [… following] several scary precedents being set over the course of the last year. […] In the US, all of this nurtures hype; and the Washington Beltway forms the ideal Petri dish in which to cultivate the alarmism - several parties think that overstating 'cyber' is in their own best interest."[499] The second mechanism is that of lobbying. As James Ball of the Washington Post writes, "in 2001, only four firms listed cybersecurity as an issue on which they were lobbying. […] By 2006, this had risen to 129 and in 2011 [… to] 1489 companies."[500] Third, the private industry can influence the demand for cyber weapons through direct counselling and advice - either formally or informally. The Economist notes that there is a continuing drain of senior government officials moving to the private sector.[501]

Despite the growing influence of the private sector, most 'cyber dollars' in the U.S. are still made on the defence rather than offense side of things. Indeed, the bulk of the most recent $35 billion proposal is said to be primarily used for defence.[502] This means the industry is incentivized to focus on defensive rather than offensive as the market for these capabilities is much bigger and more profitable

[497] Other than the industry pushing up demand, there are of course other risks. First, it might have an affect information security. As an article from The Economist notes "Mr Snowden's leak will raise questions about just how watertight firms such as Booz Allen Hamilton can keep their operations." Private sector involvement might also affect the sophistication of cyber weapons. As Singer and Friedman write, the cybersecurity complex "not only creates a kind of feeding frenzy among defense contractors, but also propels the development of more refined techniques of monitoring exploitations, and attack." See: The Economist, "Hiring digital 007s,"

[498] As Buzan et al. note, an issue becomes 'securitized' when it is presented by a securitizing actor and accepted by an audience as an existential threat to survival - i.e. "if we do not tackle this problem, everything else will be irrelevant." Notice, however, that Dunn Cavelty in one of the most comprehensive accounts of U.S. cyber securitization concludes that, overall, the securitization efforts have failed; cyber has *not* been securitized. See: Dunn Cavelty, *Cyber-Security and Threat Politics US Efforts to Secure in the Information Age*

[499] Lee and "OMG Cyber!"

[500] According to one indicator, the companies most actively lobbying on cyber issues over the past decade concern: Oracle Corp, Intel Corp, Comcast Corp, Microsoft Corp, AT&T Inc., National Cable & Telecommunications, Verizon Communications, Google Inc, Boeing Co, EMCR Corp, and Sap AG; In total, 1073 client(s) reported lobbying on specific issues containing the word 'cyber' in filings covering the period 2006 to the present, with additional reports included in prior years. Ranking is based on the number of mentions of the word 'cyber' in lobbying reports. See Open Secrets, "Lobbying Database," retrieved from: https://www.opensecrets.org/lobby/lookup.php; James Ball, "Good news for lobbyists: Cyber dollars," The Washington Post, (2012, November 13), retrieved from: https://www.washingtonpost.com/postlive/good-news-for-lobbyists-cyber-dollars/2012/11/12/158a361e-29f9-11e2-b4e0-346287b7e56c_story.html?utm_term=.507e1e4df797; Friedman and Singer, *Cybersecurity and Cyberwar*

[501] The Economist, "Hiring digital 007s"

[502] See Libicki's statement in: Stone, "Meet The Cyber-Industrial Complex". Also some argue that, when it comes to offensive capabilities, the core development of cyber weapons generally comes from *within* the secretive halls of government.

(as companies can sell to both government and private sector).[503] Governments also try to restrict the export of offensive cyber capabilities – although these initiatives remains fraught with problems.[504]

The Dutch road to 'going cyber' is another interesting case for the domestic security imperative. Like many other Western countries, the defence budget in the Netherlands dwindled for the past decades. In 2013-2014, the budget of the Dutch military reached an historic low (even lower than after the Wall Street Crash of 1929), when defence spending accounted for only just above one percent of gross national product.[505] At a time when the political leadership was wary of military spending - one prominent politician (Alexander Pechtold, D66) even wrote in a confidential email that the soldiers should just shout 'pang pang' when they shoot during military exercises given the shortage of practice ammunition - few new military initiatives were established at the Ministry of Defence in recent years - particularly on the offensive side.[506] The only two projects which stand out in the Dutch context are i) the F-35 Joint Strike Fighter (JSF) program and ii) the establishment of the Cyber Command.[507]

Scott-Smith and Smeets have reconstructed the decision-making dynamics of the highly controversial Dutch commitment to the JSF project since the late 1990s.[508] They concluded that:

> [s]ince the beginning, the Dutch commitment to the JSF has been driven by a coalition of military, governmental, and industrial interests that have sought to keep the project on track in the face of increasing parliamentary opposition and budget cuts. [Royal Netherlands Air force] (RNAF) wants to secure cutting-edge US military technology in order to remain in the

[503] As was noted in the previous chapter, this does not mean there is no provision of supply from the private sector. Instead, the argument is that drumming up demand for it is less of a priority.
[504] Herr and Rosenzweig, "Cyber Weapons and Export Control;" Paul Stockton and Michele Golabek-Goldman, "Curbing the Market for Cyber Weapons," *Yale Law & Policy Review*, 32:1 (2013)239-266; David Loundy, "Is Your T-Shirt a Lethal Weapon?" *America Online*, (1996, May) retrieved from: http://www.loundy.com/Roadside_T-Shirt.html
[505] From 2016 onwards, defence spending has gone up. The budgets over the years are difficult to compare as the government has changed its definition of 'defense spending' over the years. For example, in recent years the defense budget also included spending the costal guard and 'international safety' of foreign development aid to make it seem as if spending was not at a historical low. Krijn Schramade, "Defensiebudget historish laag," (2016, September 30),*FTM*, Retrieved from: https://www.ftm.nl/artikelen/defensiebudget-historisch-laag; Ministry of Defense, "Opniew extra geld voor Defensie in 2016", *Defensiekrant*, (2015, January 18), Retrieved from: https://magazines.defensie.nl/defensiekrant/2015/18/01-prinsjesdag; Peter Striek, "'Meer geld? Defensie krijgt juist nog veel minder geld"' *De Volkskrant*, (2014, September 26), retrieved from: http://www.volkskrant.nl/binnenland/-meer-geld-defensie-krijgt-juist-nog-veel-minder-geld~a3755100/
[506] De Telegraaf, "Militair moet zelf pang-pang roepen," (2015, August 1) retrieved from: http://www.telegraaf.nl/binnenland/24330771/__Soldaat_moet__pang__roepen__.html; RTL Nieuws, "Hennis: grappen over 'pang pang' vernietigend," (2015, August 14), retrieved from: https://www.rtlnieuws.nl/nieuws/binnenland/hennis-grappen-over-pang-pang-vernietigend
[507] The JSF programme is a program intended to replace a wide range of existing fighter, strike, and ground attack aircraft for a number of Western countries. See: U.S. Government, "The F-35 Lightning II", Retrieved from: http://www.jsf.mil/; a possible third programme would concern the use of four medium-altitude long-endurance unmanned aerial vehicles (MALE UAV). See: Kees Homan, "Ambitieniveau defensie op droevig dieptepunt", *Reformatorisch Dagblad*, (2013, September 21)
[508] Giles Scott-Smith and Max Smeets, "Noblesse oblige: The transatlantic security dynamic and Dutch involvement in the Joint Strike Fighter program," *International Journal*, (2012-2013)49-69

> front of rank of NATO forces. The Dutch defence ministry came to support this position as part of its aim to maintain a flexible multi- task military, despite declining resources. The Dutch aerospace industry was attracted by the possibility of major contracts and combing with the US high-tech sector at a time when the business climate was poor. The broader context for these positions has been set by the traditionally close relations between the Netherlands and the United States, where the transatlantic outlook for Dutch security policy fits closely with US interests in maintaining the Netherlands as a useful ally.[509]

It is tempting to assume that analogous special interest dynamics were at play for the establishment of the Dutch Cyber Taskforce in 2012 and subsequently the Cyber Command in 2014.[510] Even though there are some similarities, an analysis reveals significant differences too.

The domestic situation and interests are able to explain some peculiar decisions of the Dutch government that other imperatives cannot explain. An important starting observation is that, at a time when new computer skills are essential and largely non-existent in the military, the Cyber Command does not hire any people outside of the military, but only retrains people from other units to become proficient in hacking.[511] Also, unlike most other countries, the Cyber Command is located in the Army branch of the military, a unit not historically known for its computer savviness.[512]

The proverb 'a drowning man will clutch at a straw' seems to hold here. A state's interest in offensive cyber capabilities is a way for military organizations to avoid further budget cuts and ensure job security.[513] For the Netherlands, the establishment of the cyber command is also a way to reallocate redundant military personnel to cyber-related jobs. At the same time, the focus on offensive cyber operations sits well with those leaders and politicians in the Netherlands who (still) favour the downsizing of military forces after the Cold War as there is the perception cyber operations can be conducted with smaller units.

Private sector actors are involved in the establishment and operation of the military cyber command. What is publicly known is that Fox-IT trains the military in hacking techniques and Thales set up a

[509] Ibid, p.50
[510] There have been various conflicting statements as to when the cyber command would exactly be operational.
[511] Jeanine A. Hennis-Plasschaert, "Antwoorden op feitelijke vragen van de vaste commissie voor Defensie over de begrotingsstaten van het Ministerie van Defensie (X) voor het jaar 2017," Dutch House of Representatives, BS2016025082, (2016)
[512] Hans Folmer, "Defense Cyber Commando: Een nieuwe loot aan de defensie boom", *Operationeel: Intercom*, 45:1 (2016)22-28
[513] The money directly invested in the Dutch cyber command does not affect the general defense budget Hennis-Plasschaert, "Antwoorden op feitelijke vragen van de vaste commissie voor Defensie over de begrotingsstaten van het Ministerie van Defensie (X) voor het jaar 2017," p. 21

cyber range.[514] The level of industry involvement is, however, massively different compared with the JSF program. In the late 1990s, as Scott-Smith and Smeets note, the Dutch aerospace industry pooled their resources to push for the JSF: "the Netherlands Defence Manufacturers Association (NIID) established the Netherlands Industrial Fighter Replacement Platform (NIFARP) to ensure that Dutch companies would profit from the largest government order in history."[515] Although various public-private initiatives to enhance Dutch cyber security have been established, a platform - similar to the 'Dutch aerospace cluster' - to push for the development of *offensive* cyber capabilities was never formed in the Netherlands.[516]

An overview of the potential profit margin largely explains why Dutch private interests have thus far not made a concentrated effort to drum up demand for offensive capabilities. The Dutch command currently consists of 80 personnel, with an expectation to move it up to 200 in the near future.[517] The allocated budget was 50 million, with a structural budget of 21 million a year.[518] Fox-IT trained in the first program just fourteen officials.[519] By contrast, the report from Booz Allen Hamilton estimated that the JSF project would create between 4,800 and 5,200 jobs over the long term.[520] With

[514] The third group of 'cyber professionals' has recently started. FoxIT, "Ministerie van Defensie en Fox-IT sluiten Raamovereenkomst," (2017) Retrieved from: https://www.fox-it.com/nl/over-fox-it/corporate-nieuws/news/derde-leergang-cyberopleidingsprogramma-cop-iii-start/; Ministry of Defense, "Voortgangsrapportage uitvoering Defensie Cyber Strategie," *Dutch House of Representatives*, (2016, March 15), p. 6; Thales, "Thales to build "Cyber Range" , a Cybersecurity Training and Testing Facility for the Dutch Defence Cyber Command," (2016, May 18), retrieved from: https://www.thalesgroup.com/sites/default/files/asset/document/pr_thales_to_build_cyber_range_a_cybersecurity_training_and_testing_facility_for_the_dutch_defence_cyber_command.pdf

[515] Scott-Smith and Smeets, "Noblesse Oblige," p.51

[516] This does not mean that the private sector does not supply offensive cyber capabilities to the Dutch government. In fact, based on an article citing the head of the Dutch Cyber Command, there is evidence that the government is relying on these tools from the private sector. See: Jaco Alberts and Harry Lensink, "Te Land, ter zee en op het web; Profiel van ons cyberleger," *Vrij Nederland*, (2014, March 29)

[517] Several reports indicate that the total of 200 personnel members consists of 150 reserves. Niels Rigter, "Cybercommando nu al overvraagd," *De Telegraaf*, (2017, February 16), retrieved from: http://www.telegraaf.nl/binnenland/27637681/__Commando_nu_al_overvraagd__.html; De Telegraaf, "Cyberspecialist belangrijk wapen; Slimme virussen verlammen de vijand," (2015, April 15), retrieved from: https://www.pressreader.com/netherlands/de-telegraaf/20150415/281672548470641

[518] Raymond Boere, "Leger zoekt 150 whizzkids voor Cyber Commando," *Het Algemeen Dagblad*, (2013, November 2), retrieved from: http://www.ad.nl/binnenland/leger-zoekt-150-whizzkids-voor-cyber-commando~a2e242d5/?vwoParameters=vwo-abbo; Jeanine Hennis- Plasschaert, "Antwoorden op feitelijke vragen van de vaste commissie voor Defensie over de begrotingsstaten van het Ministerie van Defense (X) voor het jaar 2017," *Dutch House of Representatives,* (2016, November 6)

[519] Een Vandaag, "Wat gebeurt er bij het Defensie Cyber Commando?," (2014, September), Retrieved from: http://www.eenvandaag.nl/binnenland/54190/wat_gebeurt_er_bij_het_defensie_cyber_commando_; See chapter 3 for a similar discussion of other commands.

[520] Though the Booz Allen Hamilton may have an incentive to overestimate the revenue from the project, the figures remain vastly different. Early investment of the Dutch government included 150 million guilders in subsidies to help the prototype and technological development of the JSF-project, and an additional 320 million guilders for the Airbus program. See: Annemarie Jorritsma-Lebbink, "Verhoging budget subsidieregeling demonstratie-en ontwikkelingsprojecten Joint Strike Fighter (JSF) - Nederlandse luchtvaartcluster," Dutch House of Representatives, (1999, September 13), retrieved from: www.parlement.com; Ministry of Economic Affairs, "Subsidieregeling

such a low numbers, and with a dire 'cyber security need' in the private sector, it makes much more sense for companies to focus attention on this group for business.

To conclude, the second framework reveals how, at times, domestic interests both enable and propel the development of cyber weapons. The close link between 'network exploitation' and 'network attack', means that the intelligence services have an inherently important role to play. The domestic politics imperative may not only reveal why the military has an interest in the development of these capabilities, as the Dutch case has shown, it can also provide a fruitful explanation for some of the organizational decision-making (i.e. *how* capabilities are developed and *who* is responsible).[521]

5.4 The Normative Imperative: Cyber Symbolism

5.4.1 Theoretical Framework

Although the previous two theoretical frameworks differ in the locus of decision making, both see proliferation as the result of a rational decision making process. In contrast, the third 'model', grounded in social or 'constructivist' theories of international relations, suggests that status or normative imperatives impel or constrain cyber proliferation.

The term 'constructivism was coined by Nicholas Onuf', to emphasize the socially constructed nature of our world. [522] As Martha Finnemore notes "[t]he fact that we live in an international society means that what we want and, in some ways, who we are are shaped by the social norms, rules, understandings, and relationships we have with others. These social realities are as influential as material realities in determining behavior."[523]

---

demonstratie-en technologie-ontwikkelingsprojecten Joint Strike Fighter - Nederlandse luchtvaartcluster,"(1998, December 14), retrieved from: http://wetten.overheid.nl/BWBR0010265/2002-11-16

[521] This is also a more general critique on Graham Allison's second model on standard operating procedures. The model can explain some of the mistakes made by the Soviet Union in placing missiles in Cuba (such as the limited camouflage and easy-to-identify Soviet trucks) it has more difficulty explaining why Krushev placed the missiles in Cuba and Kennedy decided for the blockade. See: Allison and Zelikow, *Essence of Decision*

[522] In a speech at the University of Helsinki 25 years later, Onuf states that the book "had little impact at the time, beyond introducing the term constructivism to IR. Twenty-five years ago, my elders and contemporaries in the field had little enough interest in rules. Nor, for that matter, in norms, which are rules by another name. I cannot say the situation has changed very much since then, even if many self-described constructivists talk incessantly about norms with no sense of what makes them normative." See: Nicholas Onuf, *World of Our Making: Rules and Rule in International Relations*, (Columbia: University of South Carolina Press: 1989); Nicholas Onuf, "Rule and Rules in International Relations," Erik Castrén Institute of International Law and Human Rights University of Helsinki, (2014, April 24), retrieved from: http://www.helsinki.fi/eci/Events/Nicholas%20Onuf_Rule%20and%20Rules%20%204-2-14.pdf

[523] There is significant variation between constructivist approaches. Most constructivists scholars do not argue that it is not 'ideas all the way down', but that material forces still matter too. Alexander Wendt states that "[t]he claim is not that ideas are more important than power and interest, or that they are autonomous from power and interest. The claim is rather that power and interest have the effects they do in virtue of the ideas that make them up. Power and interest

There are two intertwined propositions which come out of the constructivist scholarship.[524] First, there is an emphasize on the role of norms as states adjust their behaviour to international expectations. Proliferation behaviour, following this perspective, tends to be driven by rules of appropriate or exemplary behaviour.[525] Thus, if there is a norm against proliferation, it can restrain actors from obtaining cyber weapons.

Second, actors' identity may influence states' decision to proliferate.[526] Actors often seek to conform to expectations about their role and membership in international society. The obtainment of a cyber weapon - through the symbolism underlying it - may exert a bolstering effect on a states' role or image within society. In other words, as Dana Eyre and Mark Suchman write, this approach of proliferation "stresses not the autonomous decision-making activity of independent nation-states, but rather the metonymical iconography of the global cultural order."[527]

In its most extreme form, cyber weapons could be conceived as a new symbol of regional or international status.[528] Whereas nuclear weapons were sought to represent or enhance prestige in the 20th century, the idea would be that cyber weapons do this for the 21st century.[529] In less extreme

---

explanations presuppose ideas, and to that extent are not rivals to ideational explanations at all." The relationship between ideas and material forces is also prominently discussed in the works of other scholars, including Hopf, Ruggie, Tannewald, and Katzenstein. See: Martha Finnemore, *National Interests in International Society* (Ithaca: Cornell University Press: 1996); Alexander Wendt, "Anarchy is What States Make of It: The Social Construction of Power Politics," *International Organization*, 46:2 (1992)391-425; Alexander Wendt, *Social Theory of International Politics* (Cambridge: Cambridge University Press: 1999); Ted Hopf, *Social Construction of International Politics: Identities & Foreign Policies, Moscow, 1955 and 1999*, (Ithaca, NY: Cornell University Press: 2002); John Gerard Ruggie, "What Makes the World Hang Together? Neo-utilitarianism and the Social Constructivist Challenge," *International Organization*, 52:4 (1998) 855-885; Peter Katzenstein, *The Culture of National Security, Norms and Identity*, (New York: Columbia University Press: 1996); Nina Tannewald, "Stigmatizing the Bomb: Origins of the Nuclear Taboo," *International Security*, 30:1 (2005) 5-49.

[524] For a discussion on the relationship between norms, culture and identity see: Maxym Alexandrov, "The Concept of State Identity in International Relations: A Theoretical Analysis," *Journal of International Development and Cooperation*, 10:1(2003)33-46

[525] See March and Olsen on the distinction between the logic of consequence and the logic of appropriateness. James G. March and Johan P. Olsen, "*Democratic Governance,"* (New York: Free Press: 1995)

[526] For a discussion on identity formulation see: Wendt, *Social Theory of International Politics*; and Peter Katzenstein, *Cultural Norms and National Security: Police and Military in Postwar Japan*, (Ithaca: Cornell University Press: 1996)

[527] Suchman and Eyre refer to this approach as the 'institutional perspective'. See: Suchman and. Eyre, "Military Procurement as Rational Myth"

[528] Also see: Nichole Ball, "Third World arms control: a Third World responsibility," in Thomas Ohlson (ed.), *Arms Transfer Limitations and Third World Security*, (Oxford: Oxford University Press: 1988)

[529] Leonard Beaton and John Maddox, *The spread of nuclear weapons*, (New York: Praeger: 1962); Lewis A. Dunn and Herman Kahn, *Trends in nuclear proliferation, 1975-1995*, (Croton-on Hudson: Hudson Institute: 1976); Ted Greenwood, Harold A. Feiveson, and Theodore B. Taylor, *Nuclear proliferation: Motivations, capabilities, and strategies for control*, (New York: McGraw-Hill: 1977); George H. Quester, *Offensive and defense in the international system*, (New York: John Wiley: 1977)

terms, cyber weapons may now be viewed as an inherent part of a state's role as 'independent' or 'modern' state, when the acquisition of these capabilities has become a common standard of a state's legitimacy. [530]

This means the sociological approach expects states to develop cyber weapons not because of rational learning, competitive dynamics and/or the need for survival. Instead states have a tendency to mimic each other. The resemblance in modern states actions and organization is referred to as 'institutional isomorphism'.[531] DiMaggio and Powell identify three mechanisms through which institutional isomorphism can occur: i) 'coercive isomorphism' results from pressures exerted by other organizations and/or societal expectations about the legitimacy of certain behaviour; ii) 'mimetic isomorphism' results from standard responses in times of uncertainty and ambiguity; iii) and 'normative isomorphism' stems from professionalization.[532]

The dominant inference pattern of the final framework is that, states' movement towards the development of cyber weapons follows from their efforts to match expectations about their role and identity in the international community. International life is embodied by international norms and regimes which guides and justifies state behaviour.

5.4.2 Evidence

Maurer's study of the United Nations implies that 'politico-military' norms to govern cyberspace are slowly emerging at the international level.[533] Maurer distinguishes between five phases process tracing how the issue has evolved over the past two decades within the United Nations (UN) environment - with Russia playing a key initiating role in this process and the U.S. as most important counterweight.[534] In the first phase (1998-2004) it was primarily Russia which drafted resolutions to

[530] As Eyre and Suchman state, "[w]hile the impact of neighboring-arsenal size on procurement may reflect strategic considerations […], the impact of regional arsenals, controlling for neighboring arsenals, almost certainly reflects the social construction of a regional standard of legitimacy. To illustrate, if Mozambique buys aircraft because neighboring South Africa has the, it is at least arguably responding to a strategic threat: if Mozambique buys aircraft because remote Senegal and Nigeria have them, it is probably responding to an emerging norm regarding what it takes to be a 'modern African nation.'" Suchman and Eyre, "Military Procurement as Rational Myth," p. 152

[531] Paul J. DiMaggio and Walter W. Powell, "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields," *American Sociological Review*, 48: 2 (1983)147-160

[532] Ibid

[533] In an excellent early study on this topic, Maurer concludes: that "[t]he activities at the United Nations show clear signs of nascent cyber norms slowly emerging. Key evidence in support of this assessment is the number General Assembly resolutions adopted over time in various committees, the annexed elements, the increasing number of co-sponsors, and the requests for bureaucracies to become involved in the issue and deliver technical assistance particularly after 2005."Tim Maurer, "Cyber Norm Emergence at the United Nations: An Analysis of the UN's Activities Regarding Cyber-security?," *Discussion Paper*, (September 2011), p. 47

[534] Tim Maurer, "Cybersecurity in a Complex Environment: Transatlantic Divergences and Diplomatic Achievements", (2016) retrieved from:

address the issue of cyber arms control. Their first initiative was launched at the UN General Assembly in 1998 with a resolution calling on states to develop "international principles" for "new information technologies" that would help "maintain international stability and security" and combat what it called "information terrorism".[535] Russia introduced similarly worded resolutions in subsequent years although the word 'cyber' never appeared in any of the resolutions.[536] The second phase (2005-2008) was one of 'contentious politics', as Maurer describes it.[537] Russian efforts gain more traction among its allies (Russia is no longer sole sponsor of resolutions) and in 2005 the draft resolution of Russia goes to a vote, with the U.S. being the only country voting against it. After the Obama administration moved into office, there was a move away from 'contestation' to 'engagement' (2008-2013).[538] In January 2010, Hillary Clinton, laid out US' position on the unlawfulness of cyber attacks, arguing that: "[c]ountries or individuals that engage in cyber-attacks should face consequences and international condemnation."[539] Phase 4 commences in 2013, when substantive discussions evolve and we witnesses a few initial agreements about the cyber threat. Not least, a consensus emerged that International Law, in particular the UN Charter, is applicable to the ICT environment.[540] The 2015 report from the Governmental Group of Experts (GGE) also published a consensus report outlining a set of specific norms, most principally about the critical infrastructure attacks.[541] A new phase is said to have recently started with the UN aiming to broaden and deepen its legitimacy with respect to these initial agreements.

---

http://www.dgvn.de/fileadmin/publications/PDFs/Zeitschrift_VN/VN_2016/Heft_2_2016/Maurer_Cyberraum_VN_2_16_engl_web.pdf; Tim Maurer and Jason Healey, "What It'll Take to Forge Peace in Cyberspace," (2017, March 20), *Christian Science Monitor*, retrieved from: http://carnegieendowment.org/2017/03/20/what-it-ll-take-to-forge-peace-in-cyberspace-pub-68351

[535] Cited in Maurer, "Cyber Norm Emergence at the United Nations"

[536] As Gjelten also notes "[t]he resolutions appealed to lots of authoritarian regimes - that info could affect stability." Tom Gjelten, "Shadow Wars, Debating Cyber 'Disarmament,'" *World Affairs*, 173:4 (2010)33-42;

[537] Maurer, "Cybersecurity in a Complex Environment"

[538] For an excellent discussion on the pulling and hauling between the American and Russian government about the establishment of cyber norms see: Arimatsu, "A Treaty for Governing Cyber-Weapons"

[539] As Gjelten notes, another public hint of the revised U.S. position came from Army General Keith Alexander, director of the NSA and U.S. Cyber Command. "When asked at a news conference in June 2010 about the Russian proposal, Alexander said, 'I do think we have to establish the rules, and what Russia has put forward is, perhaps, the starting point for international debate.'" See: Gjelten, "Shadow Wars," p. 40

[540] What this applicability means in practice is most prominently addressed in the Tallinn Manual, a non-binding study of academics on how international law applies to cyber conflict
Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, (New York: Cambridge University Press: 2013)

[541] It was agreed on that "[a] State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operations of critical infrastructure to provide services to the public." Elaine Korzak, "The 2015 GGE Report: What Next for Norms in Cyberspace?," *Lawfare,* (2015, September 23), retrieved from: https://www.lawfareblog.com/2015-gge-report-what-next-norms-cyberspace

The progress at the UN level laid out above is encouraging. No norm guiding state's behaviour emerges, cascades and internalizes overnight.[542] It inevitably takes time for states to learn, adjust and cooperate. Also, the discussions at the global level run in parallel to initiatives from other actors. We have seen a number proposals at the regional level to promote the development of norms in cyberspace - with the ASEAN Regional Forum and the OSCE - amongst more like-minded states.[543] And the private sector has been involved too. For example, Microsoft published a white paper just before the Global Conference on Cyberspace (GCSS) in 2015 proposing six norms to reduce conflict in cyberspace.[544]

A critical breakdown of the current initiatives however reveals that these efforts have so far not been conducive to limiting the spread of cyber weapons.[545] Indeed, as Joseph Nye Jr. concludes, when it comes to 'cyber war' and 'sabotage', states and non-state actors have not yet widely accepted and adhered to a set of norms.[546]

When a state develops WMD it knows it likely has to absorb a substantial amount of additional political and economic costs. It risks undercutting alliances and trading relations with other states. For a state which relies on its good relation with other (more powerful) states this might strongly impinge on the motivation to acquire these capabilities. There is no such 'cyber taboo'; states which develop cyber weapons are not perceived with abhorrence.[547] When a state reveals it pursues cyber weapons it faces hardly any political or moral pressure from the international community - either

[542] Martha Finnemore and Kathryn Sikkink, "International norm dynamics and political change," *International Organization* 52 (1998): 887-917.
[543] For an excellent basic overview of how the ASEAN Regional Forum and the OSCE have been used as regional platforms to discuss various cyber see: Dan Ward and Robert Morgus, "Professor Cy Burr's Graphic Guide to: International Cyber Norms," *New America: Cyber Security Initiative* (2016, November), Retrieved from: https://na-production.s3.amazonaws.com/documents/CyberNorms11.14.pdf
[544] Angela McKay, Paul Nicholas, Jan Neutze and Kevin Sullivan, "International Cybersecurity Norms: Reducing Conflict in an Internet-dependent World," (2014, December), *Microsoft WhitePaper*, retrieved from: https://blogs.microsoft.com/cybertrust/2014/12/03/proposed-cybersecurity-norms/. It was part of part of the EastWest Institute's 2014 Global Cyberspace Cooperation Summit in Berlin.
[545] As becomes clear from the discussion above, only two norms have the potential to cascade in the near future: i) states should not conduct cyber attacks on critical infrastructures; ii) states should consider how best cooperate to exchange information and assist in prosecuting terrorist and criminal use of information and communications technologies.
[546] Joseph Nye Jr. maps out seven issues of cyber governance using regime theory: DNS/standards, crime, war/sabotage, espionage, privacy, content control, and human rights. Similar to Nye, Tim Stevens argues that it is unlikely "a 'cyber taboo' analogous to nuclear and chemical weapons taboos will be constructed" even though U.S. has tried to establish cyber norms as part of their international engagement strategy. At most, a norm emerges about 'acceptable' use, serving to demonstrate 'red lines' of cyber operations. Joseph S. Nye, "The Regime Complex for Managing Global Cyber Activities," *Global Commission on Internet Governance Paper Series*, 1 (2014), retrieved from: https://www.cigionline.org/publications/regime-complex-managing-global-cyber-activities Tim Stevens, "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace," *Contemporary Security Policy*, 33: 1 (2012): 148-170
[547] For a discussion on the nuclear taboo see: Tannewald, "Stigmatizing the Bomb"

directly or indirectly - to not 'go cyber'. It is therefore hardly surprising that there are no known examples of states having started to explore or pursue cyber proliferation, but backed down because of current international norms.

Lacking a 'cyber treaty' or 'cyber taboo', it would seem that the road is open for cyber weapons to be used as a source of prestige.[548] Yet, status driven motives are much *less* favourable to explain the variation in cyber weapon development than one may initially expect. This is due to three, intertwined reasons. The first two dimensions have already been discussed in the previous chapters. First, as was laid out in chapter 2, cyberspace has a largely non-material ontology.[549] It makes it hard to publicly showcase or 'parade' them. Second, it was also already noted that cyber weapons have limited attributive ability following usage. Normally, the 'attribution problem' is said to provide advantages to the attacker. As Gjelten states, "[i]n conventional warfare, an aggressor can quickly be identified, and the responsibility for war crimes or treaty violations can be determined, but an attack on a computer network can be almost impossible to attribute."[550] But it can be a disadvantage too when states want to signal they have a certain offensive capability.[551]

Third, whereas conventional weapons are generally characterised by their 'multiple use-ability' or 'permanent' nature, cyberweapons are unique in that they are 'transitory' in nature, that is, they have a short-lived or temporary ability to effectively cause harm or damage to living or material entities.[552] The nuclear bombs developed at the height of the Cold War could still vanish cities in one blow. Also, the Kalashnikovs mass-produced in the early 1950s could still kill people. Even some of the earliest weapons used in conflict - including the socket axe, the chariot, the spear and the sickle-sword - could be lethal today. In contrast, the cyberweapons produced today are unlikely to have any impact in a few years' - or even less - time. Cyber weapons' temporary ability to access a computer system or network is primarily due to the malleability of cyberspace affecting the life-cycle of a vulnerability and effectiveness of a cyber weapons (see chapter 2 for components of a cyber weapon).[553] This

[548] In the nuclear case, there are two normative mechanisms going in opposing directions; one the one hand, the symbolism framework explained restrained, because nuclear capabilities were viewed with abhorrence; and on the other hand, the framework explained proliferation, as these capabilities give actors a certain amount of prestige. To reconcile these two mechanisms, it was noted that the 'role' or 'identity' of the state should be considered.
[549] This point also came back in early discussions at the UN level. As Gjelten notes: "[t]he idea of cyber arms limitation was complicated by the fact that cyber "weapons" are often software programs that, unlike missiles or tanks, cannot be seen or counted," See: Gjelten, "Shadow Wars"
[550] Gjelten, "Shadow Wars", p. 38
[551] For a more detailed discussion on this issue see chapter 6.
[552] For a more extensive discussion on this topic see: Smeets, "A Matter of Time"; Also see chapter 4.
[553] Bruce Schneier, "Crypto-Gram", *Schneier on Security,* (2000, September 15), retrieved from: https://www.schneier.com/crypto-gram/archives/2000/0915.html

dynamic inherently changes the incentives structure of states to showcase their capabilities.[554] The life cycle of vulnerabilities is subject to three delays; i) the awareness delay, ii) the patching delay and iii) the adaptation delay. The moment actors reveal their capability, it inevitably increases the likelihood a vendor learns about the vulnerability and will assign a high level of priority of developing a patch (i.e. reducing the awareness and patching delay). Overall, as document from the EWI also concludes, "[m]ilitary forces will have distinct interests in keeping cyber weapons secret. […] Those nations that are developing the most advanced weapons have a strong interest in being able to protect the intelligence surrounding such capabilities."[555]

What this leads to is that states are more inclined to talk boastingly about their *intentions* instead of developing *actual* cyber weapons in an effort to deter and enhance their status in the international system.[556] Bouwmeester, Folmer, and Ducheine for instance state about the United States: "[s]howing their offensive cyber aims obviously is a part of the U.S. battle of the narrative. Since most offensive cyber weapons - by their nature - can only be used once before the rest of the world will have an adequate answer to these weapons, the U.S. DoD is very willing to openly share their offensive intentions without compromising in detail their tactics, techniques and procedures."[557] To reveal their intentions to 'go cyber' states can poser with a publication of a national strategy and/or the public establishment of institutions like a cyber command.

First, most states have published a National Cyber Security Strategy.[558] These strategies, written in multiple languages, serve as much a domestic and international function.[559] The country perhaps most

[554] There are a number of other technical and political factors which affect the short-lived nature of offensive cyber capabilities. Smeets, "A Matter of Time"

[555] EastWest Institute, "Working Towards Rules for Governing Cyber Conflict Rendering the Geneva and Hague Conventions in Cyberspace," (2011),retrieved from: https://www.eastwest.ngo/sites/default/files/ideas-files/US-Russia%20(1).pdf,

[556] One additional reason why the aspect of prestige seems to play a lesser role in the development of cyber weapons concerns the fact that it is not yet clear whether states possessing offensive cyber capability are given greater weight in certain aspects of foreign policy. It is certainly not the case that cyber weapons are a direct ticket to the 'head table' at international forums.

[557] Hans Bouwmeester, Hans Folmer and Paul Ducheine, "Cyber Security and Policy Responses," in Paul Ducheine, Frans Osinga, Joseph Soeters (eds.), *Cyber Warfare: Critical Perspectives,* (The Hague: Asser Press: 2012), p. 29

[558] The National Cyber Security Strategies of the NATO member states can be found at the website of the NATO Cooperative Cyber Defence Centre of Excellence: https://ccdcoe.org/strategies-policies.html

[559] Also, few strategies reflect upon the specific nature of attacks, actors and/or threats nor do they indicate how the cyber perils are likely to evolve over the course of the next few years. States which do describe the nature of threats emerging in the cyberspace in their NCSS rarely go beyond a mere superficial discussion of the cyber threat and sharply disagree amongst each other. A typical report merely states that the threat emerging in cyberspace come from "several sources" and the consequence can be "severe" (for example, see Hungary's strategy). Norway considers espionage and sabotage to be a growing threat - but discusses this issue in just one paragraph. Countries like Italy and Spain classify the main threats associated with cyber space but shy away from discussing the likelihood and impact of the listed threats. States which do offer a public assessment of the cyber threat - for example, the United Kingdom, United States, the Netherlands and Switzerland - are exceptions which prove the rule. Viktor Orbán, *National Cyber Security Strategy of Hungary*, (2013) retrieved from: https://ccdcoe.org/strategies-policies.html2

forthright about offensive capability development in their strategy is the United Kingdom. The 'National Cyber Security Strategy 2016-2021' of the UK states that "[t]he Government will measure [their] success in establishing offensive cyber capabilities by assessing progress towards the following outcomes: i) the UK is a world leader in offensive cyber capability; and ii) the UK has established a pipeline of skills and expertise to develop and deploy our sovereign offensive cyber capabilities."[560] More generally, comparing the national cyber security strategies we can observe some form of 'policy isomorphism'[561]: European states are required to develop a NCSS (coercive isomorphism); cyber security is still seen as ambiguous problem with unclear solutions (mimetic isomorphism); but there is a growing professionalization of strategy writing as states update their earlier publications and organize workshops to share best practices (normative isomorphism).[562]

Second, initiatives to establish a formal institution dealing with 'cyber warfare' receive widespread media coverage.[563] In the Netherlands, over 150 Dutch news articles were written over the past four years highlighting the establishment of the Dutch Cyber Command. It was widely publicized as a place where "whizzkids" and "highly talented hackers" were working.[564] Indeed, in line with this argument, the irony is that many states which are known to have deployed sophisticated offensive cyber capabilities - as chapter 3 indicates, for example, Russia, China, and France - are the most secretive about their program. These are the countries which also need it the least, as it is widely acknowledged that they have these capabilities.

In chapter 3 one of the key findings was that numerous states are at the 'exploration' or 'pursuit' stage of cyber proliferation; they have a military program to develop offensive cyber capabilities but we

[560] Philip Hammond, "National Cyber Security Strategy 2016 to 2021," (2016, November) retrieved from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

[561] Instead of 'institutional isomorphism' - although it may turn into that. DiMaggio and Powell, "The Iron Cage Revisited"

[562] Di Maggio and Powell "interpret professionalization as the collective struggle of members of an occupation to define the conditions and methods of their work, to control 'the production of producers', and to establish a cognitive base and legitimation for their occupational autonomy." See: DiMaggio and Powell, "The Iron Cage Revisited," p. 152

[563] Germany is a possible exception, remaining highly sceptical about attracting talent and 'hyping up' the program. One potential explanation might be its ongoing struggle with the past; not used to brag about its military capabilities. See: Christian Thiels, "Mit Nerds in den Krieg," *Tagesschau*, (2016, April 26), retrieved from: https://www.tagesschau.de/inland/cyber-bundeswehr-101.html; Burkhard Ewert, "Marschbefehl in den Cyberkrieg," *Deutschlandfunk*, (2017, April 8), retrieved from: http://www.deutschlandfunk.de/neues-bundeswehrkommando-marschbefehl-in-den-cyberkrieg.720.de.html?dram:article_id=383346; Ulrike Scheffer, "Bundeswehr startet Kommando gegen Cyberattacken," *Der Tagesspiegel*, (2017, April 4), Retrieved from: http://www.tagesspiegel.de/politik/verteidigung-bundeswehr-startet-kommando-gegen-cyberattacken/19608528.html

[564] See for example: Michael Persson, "Cybersoldaten klaargestoomd voor de aanval," *De Volkskrant*, (2014, September 26), retrieved from: http://www.volkskrant.nl/binnenland/cybersoldaten-klaargestoomd-voor-de-aanval~a3755316/; Boere, "Leger zoekt 150 whizzkids voor Cyber Commando". I conducted a search of all newspaper article using LexisNexis. In total, I retrieved 129 newsarticles with the word 'cyber commando' or 'Cyber Defensie Commando' written in Dutch since 1990

have not yet observed a (public) incident in which they have deployed any capability. Even small states, lacking the capacity to develop highly sophisticated cyber weapons, have a cyber command or equivalent program.[565] The prestige dynamics laid out above can partially explain this observation. Overall, for modern states not the *possession* of cyber weapons but *visible initiatives* revealing the intention to develop cyber weapons serve a primary iconographic function.

5.5 Conclusion

The purpose of this chapter was to analyse the motivations underlying states' cyber proliferation. To conduct this demand-side analysis, I deployed three classic theoretical frameworks in a comparative fashion to explain why states 'go cyber'. The first framework suggested that the predominant cause for cyber proliferation is perceived insecurity. Although the imperative seems to provide an intuitive explanation for why states develop cyber weapons, the chapter concluded that it does a poor job explaining most variation. Estonia is unable to compete with its main geopolitical rival Russia in the conventional domain of conflict. It has a skilled labour force and is highly digitalized - making limited proliferation (i.e. developing unsophisticated cyber weapons) an option. Yet, as was shown, they do not intend to use cyber weapons as a way to balance or as a 'poor man's bomb'. The framework also has difficulties explaining *when* a state proliferates. It was noted that South Korea, for example, only recently established a military program to develop offensive cyber capabilities but said to have been threatened by its northern neighboring country since 1994. The chapter has shown that we have be extremely cautious to accept the conventional wisdom that states develop cyber weapons for national security reasons. At most, the cyber arms thesis provides a weak incentive for states to proliferate.

The domestic politics framework instead posited that cyber proliferation is driven by competing interests and incentives *within* the state. An analysis opening up the black box of decision-making in the U.S. has shown how at times domestic interests, particularly intelligence services, enable the development of cyber weapons. Former UN Secretary-General Dag Hammarskjöld once said, "[p]eacekeeping is not a job for soldiers, but only a soldier can do it." It is not too far of a stretch to state that, the current perception is that 'CNA is not a job for the intelligence services, but only the intelligence services can do it.' The focus on developing cyber weapons also provides a number of benefits to militaries of states facing defence budget cuts. For the Netherlands, the domestic politics imperative helps us understand why the cyber command is part of the army and the command only recruits officials from within the military. Even though the growing prominence of the cyber security

[565] Also see chapter 3

industry is hard to ignore, the chapter has also clarified that a number of factors which limit industry's incentive in drumming up demand for offensive cyber capabilities.

The third framework assessed the normative processes underlying cyber proliferation. Scholars have suggested that weapons are often acquired because it provides an important normative symbol of a state's modernity and identity. It became clear that a diverse range of actors have now called for the establishment of new cyber norms and regimes. Yet, lacking the demonstration effect of a 'cyber Pearl Harbor', cyber weapons are currently not regarded with abhorrence in the same manner as weapons of mass destruction. Even though there is no 'cyber taboo' to halt the spread of cyber weapons, I also concluded that status driven motives seem to be less favourable to explain the variation in cyber weapon development given its element of surprise, limited attributive ability, and immateriality. Overall, states are more inclined to poser with a publication of a national cyber security strategy and/or the public establishment of institutions like a cyber command instead of developing *actual* cyber weapons. Indeed,

Thus, similar to Sagan's classic study on nuclear proliferation, this chapter presented a multi-causal argument for cyber proliferation. But, whereas for Sagan still "the largest number of past and even current active proliferant cases are best explained by the security model", the explanatory value of this framework is more limited for cyber proliferation.[566] Indeed, the 'domestic politics' and 'normative' framework do not just explain a few, residual cases but are at the heart of the cyber proliferation puzzle. In addition, the *nature* of the causal mechanisms is different for cyber proliferation. The iconographic value of cyber proliferation lies not in the showcase or use of cyber weapons, but in policy and institutions which embody a state's intentions to develop them. Perhaps it is not 'all mouth and no trousers,' policymakers and experts often confuse *apparent* proliferation with *actual* proliferation.

[566] Sagan, "Why do States Build Nuclear Weapons?," p. 85

Chapter 6: A Strategic Utility Analysis of Cyber Weapons

6.1 Introduction

The previous chapter was concerned with the demand-side factors of the cyber proliferation puzzle. A key observation was that the national security imperative - even though it is a straightforward and intuitive framework - is unconvincing in light of current evidence. I noted that the result may not be surprising given that the cyber weapon is not an 'absolute weapon', nor is there an evident relationship between actors' build-up of a cyber weapon arsenal and their own security given the limits of cyber deterrence.[567]

This leads us to consider an important question: if the value of cyber weapons is not 'obviously beneficial' and 'existential', what purpose *do* they serve? There is a sense that state leaders and policy makers themselves do not have a strong conception of its strategic advantages and limitations.[568] Henry Kissinger in *World Order* makes a parallel claim when the writes "internet technology has outstripped strategy or doctrine - at least for the time being. In the new era, capabilities exist for which there is as yet no common interpretation - or even understanding. Few if any limits exist among those wielding them to define either explicit or tacit restraints."[569] Hence, this chapter extends the demand-side analysis and evaluates the strategic utility of cyber weapons - which also helps to understand why states develop cyber weapons in the future, following strategic adaptation.

6.2 From Destructive Effect to Strategic Utility

The post-2000 literature's primary focus is on the disruptive or destructive effects of cyber weapons. The academic debate on the potential for cyber war is at the spill of this literature, and notably

[567] For an original conception of the term 'absolute weapon' see: Bernard Brodie (ed.), *The Absolute Weapon: Atomic Power and World Order*, (New York: Brace and Company: 1946); Gregg Herken, "The Not-Quite-Absolute Weapon: Deterrence and the Legacy of Bernard Brodie," *Journal of Strategic Studies*, 9:4 (1986)15-24; Roman Kolkowicz (ed.), *Dilemmas of Nuclear Strategy* (London: Frank Cass & Co.: 1987);

[568] See discussion in next section of this chapter.

[569] Henry Kissinger, *World Order: Reflections on the Character of Nations and the Course of History* (London: Penguin Books Limited, 2015), p. 334

illustrative.[570] An often-cited quote from Thomas Rid's article *Cyber War will not Take Place* reads "No cyber offense has ever injured a person. No cyber attack has ever damaged a building."[571] The statement has been debated repetitively and at-length, from both theoretical and empirical perspectives.[572]

John Stone, a scholar of Clausewitz, writes in a theory-driven response to Rid's article that cyber attacks could constitute acts of war.[573] According to Stone, "it depends on the meaning and relationship of the terms 'force', 'violence', and 'lethality': Acts of war involve the application of force in order to produce violent effects. These violent effects need not be lethal in character: they can break things, rather than kill people, and still fall under the rubric of war."[574] From an empirical perspective, scholars have criticised Rid that many of the attacks cited were in fact much more violent. Perhaps not the direct effects but the indirect effects of the DDoS attacks on Estonia, one scholar argues, were consequential.[575] Similarly, others have argued that Stuxnet was more than just an act of sabotage.[576]

Parallel to these academic discussions, the focus in the policy-space has primarily revolved around the likelihood a cyber attack can cripple a domestic society or economy. In the United States, an important event which propelled government attention to a potential cyber-attack on critical infrastructure was the Oklahoma City bombing of 1995.[577] In response to the tragedy the President's

[570] Having said that, a number of 'classic' articles in the field offered various strategic insights. This debate re-emerged in the 2010 (hence, the term 'recent' was added). See: Arquilla and Ronfeldt, "Cyberwar is Coming!". Stephen M. Walt, "Is the Cyber Threat Overblown?," *Foreign Policy*, (March 30, 2010), retrieved from: http://walt.foreignpolicy.com/posts/2010/03/30/is_the_cyber_threat_overblown : Clarke and Knake, "Cyber war"; Rid, *Cyber War Will Not Take Place*; Thomas Rid, "Cyberwar and Peace: Hacking Can Reduce Real-World Violence," *Foreign Affairs*, (2013, November/December), retrieved from: https://ridt.co/d/rid-foreign-affairs-cyberwar.pdf

[571] However, Rid is often misrepresented in this respect. Although the focus of subsequent scholarship has primarily been on the (potential) scale of violence, Rid lays out three of Clausewitz criteria: i) violent, ii) instrumental and iii) political. He considers the latter to be potentially the most important.

[572] For direct discussions on this quote see for example: Gary McGraw, "Cyber War is Inevitable (Unless We Build Security In)"*Journal of Strategic Studies*, 36:1 (2013)109-119; Isabelle Duyvesteyn, "Between doomsday and dismissal Cyber war, the parameters of war, and collective defense," (2012) retrieved from: https://www.atlcom.nl/ap_archive/pdf/AP%202014%20nr.%207/Duyvesteyn.pdf; Shruti Tulpule, "Are we headed towards Web War I?," *International Journal of Law and Legal Jurisprudence Studies*, 1:7 (2014)

[573] John Stone, "Cyber War Will Take Place!," *Journal of Strategic Studies*, 36:1 (2013) 101-108

[574] Ibid, p. 107

[575] CBS News, "Stuxnet: Computer Worm Opens New Era of Warfare," *60 Minutes*, Transcript (2012, March 4); Christian Czosseck, Rain Ottis and Anna-Maria Talihärm, "Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security," *Journal of Cyber Warfare and Terrorism*, 1:1 (2011)57-64

[576] This has also let to a new field of scholarly work on the laws of cyber conflict. When does a cyber attack hit the threshold of war? The most prominent work on this concerns the Tallin Manual project. Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare.

[577] On April 19, 1995 a terrorist attack took place at the Alfred P. Murrah Federal Building in downtown Oklahoma City, killing 168 people and injuring many others. See: Sheryll Shariat, Sue Mallonee, and Shelli Stephens-Stidham, "Summary Of Reportable Injuries In Oklahoma," (1998, December) retrieved from: http://web.archive.org/web/20080110063748/http://www.health.state.ok.us/PROGRAM/injury/Summary/bomb/OKCbomb.htm

Commission on Critical Infrastructure Protection (PCCIP) was formed by the Clinton administration.[578] The commission released its report to President Clinton in October 1997, examining both the physical and cyber threats to the nation.[579] Although the commission did not "discover[…] an immediate threat sufficient to warrant a fear of imminent national crisis,"[580] it did find reasons to implement new measures, especially in the area of cyber security. As a product of the Commission's report, President Clinton released Presidential Decision Directive 63 (PDD-63) in May 1998.[581] PDD-63 called for a range of actions intended to improve the nation's ability to protect "critical infrastructure" from physical and cyber-attacks.[582] Several key documents have followed the PCCIP report: the 2003 National Strategy to Secure Cyberspace,[583] the 2008 Comprehensive National Cybersecurity Initiative,[584] the Cyberspace Policy Review when the Obama administration began its tenure,[585] and most recently the 2016 Cybersecurity National Action Plan.[586] Although they differ in emphasis on how the government should prioritize efforts, they are strikingly similar in that they centre attention around critical infrastructure protection.[587] Other countries have followed suit, all providing detailed outlines of what is and is not part of critical infrastructure, and what the consequences would be if attacked.[588]

Even though these discussions have yielded valuable insights and increased policy-awareness, they do not deepen our understanding of the value of cyber weapons. The level of harm or damage means

[578] Ralph Bendrath, "The Cyberwar Debate;" Bendrath, "The American Cyber-Angst and the Real World"
[579] President's Commission on Critical Infrastructures, "Infrastructure Protection, Critical Foundations: Protecting America's: The Report of the President's Commission on Critical Infrastructure Protection," (1997, October 13), Retrieved from: https://www.fas.org/sgp/library/pccip.pdf
[580] Ibid, p.x
[581] The White House, "The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive," *White Paper*, 63 (1998, May 22), retrieved from: www.fas.org/irp/offdocs/paper598.htm
[582] According to Kaplan, "[t]he surprise twist came about because key members of the Critical Infrastructure Working Group and the subsequent presidential commission had come from the NSA and Navy's super-secret black programs and were thus well aware of this new aspect of the world." Kaplan, *Dark Territory*, p. 40
[583] The White House, "The National Strategy to Secure Cyberspace," (February, 2003), retrieved from: www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf
[584] The White House, "The Comprehensive National Cybersecurity Initiative," (2014, February), retrieved from: http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative
[585] The White House, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure" (2009), retrieved from: https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf
[586] The White House, "FACT SHEET: Cybersecurity National Action Plan," (2016, February) Retrieved from: http://sitsd.mt.gov/Portals/77/docs/MT-ISAC/2016/2016%2002%2018/CNAP.pdf?ver=2016-02-16-093003-710
[587] That is, there is a primary focus on the physical level of cyberspace (see chapter 3). I have argued elsewhere that this discourse may change following the DNC hack. See: Max Smeets, "Diplomacy in Cyberspace," Workshop Diplomatic Studies, London, Senate House, (2016)
[588] For an overview of the initiatives worldwide see: Myriam Dunn, "A Comparative Analysis of Cybersecurity Initiatives Worldwide," *International Telecommunications Union*, WSIS, Thematic Meeting on Cybersecurity, Geneva,(2005, June/July) , retrieved from: https://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_InitiativesWorldwide.pdf

little if not placed in its relevant strategic context. Indeed, there is certainly no perfect correlation between the strategic utility of a military capability and its ability to cause harm or damage. "Most of us are capable of seriously injuring others, but for the most part we fail to exercise our capabilities because there is no positive reason to strike", Gartzke writes.[589] Our goal should therefore be to better connect the threat and use of cyber weapons with policy. In Clausewitzian terms, we need to better connect for which aim(s), 'cyber' provides the appropriate means.

In other words, earlier scholarship has distracted us from the more important issue at hand: namely, what is the strategic utility of a cyber weapon? There is no single method to measure the strategic utility of cyber weapons. 'Strategic utility' can mean at least two different things. First, it can refer to whether a cyber weapon can provide value in support of a national strategy. The assessment of 'utility' then is highly dependent on defining what the strategy is. Following this perspective, a possible measure the utility of cyber weapons is how it contributes to the pursuit of deterrence. Yet, it remains unclear to what degree deterrence - or any other strategy for that matter - is in fact the correct strategy to pursue. Hence, by this measure stick, we may come to the conclusion that cyber weapons have (no) strategic utility.

Second, the term 'strategic utility' could also refer to a cyber weapon's ability to produce an outcome of conflict itself, or even more broadly state competition. Here, we would use a different set of measures for utility. We should discuss how a cyber weapon helps to avoid and/or affect the strategic outcome of a conflict. [590] It is this second form of strategic utility which I propose to lay out in this chapter.

According to Gartzke, "'[c]yber war' is not likely to serve as the final arbiter of competition in an anarchical world and so should not be considered in isolation from more traditional forms of political violence." Although I agree with Gartkze that cyber weapons should not be conceived as the most authoritative asset, the point of this chapter is that an analysis of cyber weapons strategic utility is nevertheless valuable; if we use 'final arbitration' as a criterion for analysis, almost no capabilities would pass the test. Hence, my approach is more closely aligned with Colin Gray's review the military asset's strategic utility. In the final part of his book *Explorations of Strategy* Gray writes the following about special operations: "[I] will avoid the trap of immoderate and unrealistic tests of strategic value.

[589] This notion adds to Gartzke's argument that cyberwar is a myth. See: Gartzke, "The Myth of Cyberwar," p. 52; also Betz and Stevens, *Cyberspace and the State*

[590] I adopt the definition used by Colin Gray with two alterations. Gray focuses on "how a military directly contributes to the strategic outcome of a war". The effects do not have to be direct and apply strategy to a broader context than 'war', I therefore refer to the term 'conflict' instead. Colin S. Gray, *Explorations in Strategy*, (Westport: Praeger Publishers: 1996)

More specifically, the test of independent decisive effect on the course of a war is a criterion that special operations would fail in most instances. Since navies, arms, and air forces also fail the 'test' of independent decisive effect, one should not hold the special operations community to a higher standard."[591]

When we realize that cyber weapons should not be considered per se, but with reference to both its direct and indirect impact upon conflict, it reveals an intricate relationship between mission excellence and strategic success. A well-written piece of code might provide great tactical value but does not guarantee strategic utility. Similarly, a failed usage of a cyber weapon might provide strategic gains. An example of this seemingly counterintuitive logic might be Shamoon. The malware, described in more detailed in chapter 4, contained multiple coding errors and was badly executed. Yet, with reference to Iran's broader conflict situation and posture in the region, it might have had a 'positive' contribution too. Not least, Iran showed it was unwilling to immediately back down following others usage of a capability itself had hardly developed at the time. The deployment showed military perseverance and perhaps even enhanced its political standing relative to other states.

This study's call for a strategic scrutiny is certainly not a pioneering statement.[592] Former CIA and NSA director Michael Hayden notes in his book that "[n]o one has yet begun to write the On Thermonuclear War [Herman Kahn's classic 1959 text on nuclear strategic concepts] for cyber conflict."[593] Similarly, Jim Ellis writes that the current strategic thinking on cyber conflict is "like the Rio Grande [river in North America], a mile wide and an inch deep."[594] Of course, the discussion in this chapter is unable to completely fill this large gap in strategic thinking. Yet, my hope is to at least address the relevant matter in relation to my thesis whilst engaging with the sparse literature which has provided valuable strategic insights.

In the remainder of this chapter, I make a distinction between two principle ways in which a cyber weapon may provide a beneficial impact on a state's ability to influence and avoid conflict.[595] The first part will look at the strategic value of cyber weapons' (potential) *possession*. The second part will assess the strategic value of cyber weapons when *used* by an actor.

---

[591] Ibid
[592] Also see: Kello, "The Meaning of the Cyber Revolution"
[593] Hayden, *Playing to the Edge*
[594] Cited in: Patrick Cirenza,"The flawed analogy between nuclear and cyber deterrence," *Bulletin of the Atomic Scientists*, (2016, February 22), Retrieved from: http://thebulletin.org/flawed-analogy-between-nuclear-and-cyber-deterrence9179
[595] Many of the claims made in this chapter apply to cyber operations more generally (i.e. also use of espionage capabilities). Yet, considering the focus of my thesis, I have narrowed the nature of discussion here.

6.3 Cyber Bargaining: Strategic Utility in (Potential) Possession

Following the bargaining and coercive diplomacy literature, it is said that the (potential) possession of a weapon can sometimes be used in negotiating a concession or inducement. The aim of this section is to answer the following question: can cyber weapons be used in negotiations to influence the outcome of a conflict? The term 'negotiation' denotes both explicit interaction as well as implicit interaction, i.e. via tacit communication.[596]

It might seem counter-intuitive to assess the strategic value of cyber weapons short of actual usage considering the large number of cyber attacks which take place on a daily basis. Indeed, governments and companies frequently talk about their struggles to keep up with all the cyber incidents and develop an effective defence mechanism.[597] Why should we even bother about the effects of cyber capabilities short of actual use?

Viewing utility only in light of what happens *after* a cyber capability has been used, however, would lead to a significant bias in our thinking about the cyber proliferation. Cyber conflict is best understood as a 'next step' only after bargaining fails to deter and/or compel.[598] Whether the mere possession of cyber weapons can be used to leverage outcomes can go a long way explaining whether the usage of cyber capabilities is necessary or not. Collectively, the inclusion of the literature on bargaining and coercive diplomacy therefore allows us to uncover less observable forms of strategic utility. It prevents us from misconstruing the value of cyber weapons: what happens pre-usage of cyber weapons is just as important as the use of cyber weapons.

I assess the following three propositions on bargaining in relation to cyber proliferation:

- Cyber Bargaining Proposition I: The ability of a state to develop a cyber weapon (i.e. cyber latency) can lead to coercive bargaining advantages.
- Cyber Bargaining Proposition II: The prospect of a state giving up its offensive cyber capability can lead to coercive bargaining advantages.
- Cyber Bargaining Proposition III: The threat of a state using a cyber weapon can lead to coercive bargaining advantages.

[596] Tacit communication refers to the type of communication that is invisible, unspoken, inferred, or implied.
[597] For example, see: Phil Stewart, Diane Bartz, Jim Wolf and Jeff Mason, "Special report: Government in cyber fight but can't keep up," Reuters, (2011, June 17) retrieved from: http://www.reuters.com/article/us-usa-cybersecurity-idUSTRE75F4YG20110617
[598] For a similar argument on the role of air power see: Wallace J. Thies, "Compellence Failure or Coercive Success? The Case of NATO and Yugoslavia," *Comparative Strategy*, 22:3 (2003)243-267

The three bargaining propositions are not always clearly distinguished in the literature on coercive diplomacy. I will address each of the propositions separately below, often drawing out a comparison to nuclear capabilities since it has received the most prominent attention in earlier scholarly work.

Cyber Bargaining Proposition I: The ability of a state to develop a cyber weapon (i.e. cyber latency) can be used as a tool of diplomatic persuasion/coercion.

We can recount numerous historical cases when states' nuclear latency was used to bargain for concessions from other countries.[599] Italy used its potential ability to develop nuclear weapons to back demands during the NATO negotiations in the 1950s and 1960s.[600] West Germany demanded various concessions from both the Soviet Union and the U.S. in exchange for its Non-Proliferation Treaty (NPT) signature.[601] In the same period, Japan signalled that it would only forgo the nuclear option in return for military assistance and territorial reversion of Western Pacific Islands (Okinawa).[602] In the early 1990s, officials from Pyongyang requested to abandon the nuclear weapons program in exchange for a laundry list of concessions.[603] And in the early 2000s, Libyan leader Muammar al-Qaddafi offered to give up its nuclear program, obtained via the Kahn network, in return for sanctions relief. [604]

Tristan Volpe constructed a 'theory of proliferation persuasion' to explain when states hedging with advanced nuclear technology are least and most likely to be successful.[605] His main argument is that states are locked into a bargaining dilemma: "the more [a state] threatens to proliferate, the harder it

[599] For an excellent review see: Tristan A Volpe, "Proliferation Persuasion: Coercive Bargaining with Nuclear Technology," *PhD Dissertation*, George Washington University, (2015, May), retrieved from: https://e-reports-ext.llnl.gov/pdf/788895.pdf

[600] Leopoldo Nuti, "'Me Too, Please': Italy and the Politics of Nuclear Weapons, 1945-1975," *Diplomacy and Statecraft*, 4:1(1993)114-148, p.136

[601] George H. Quester, *The Politics of Nuclear Proliferation*, (Baltimore: Johns Hopkins University Press, 1973), p. 167-187.

[602] John E. Endicott, *Japan's Nuclear Option*, (New York: Praeger, 1975), p. 114.

[603] Jonathan D. Pollack, *No Exit: North Korea, Nuclear Weapons, and International Security*, (Abingdon: Routledge, 2011)

[604] It remains unclear exactly how close the Libyan government was to acquiring a nuclear weapon. Gadhdafi said in mid-2006 that it was near to accomplishing the development, but U.S. officials discounted this claim (arguing that Libya had enough uranium but not enough technical expertise). See: Robert G. Joseph, *Countering WMD: The Libyan Experience* (Fairfax, Virginia: National Institute Press, 2009); William H. Tobey, "A Message from Tripoli: How Libya Gave Up Its WMD," *Bulletin of the Atomic Scientists*, Online Analysis, (2014, December)

[605] Advanced nuclear technology refers to the stage when a country first acquires enrichment and/or reprocessing (ENR) technology. Volpe's argument is not that other scholars of nuclear proliferation provided invalid explanations on why states forgo nuclear weapons. Instead, he argues that they have so far overlooked the importance of coercive bargaining. Volpe, "Proliferation Persuasion"

becomes to reassure others that compliance will be rewarded with nuclear restraint."[606] This means that, contrary to the conventional wisdom about the role of power in world politics, "bargaining success depends on the willingness and ability of the challenger to resolve a commitment problem. Less nuclear latency provides an optimal means of compellence because it becomes increasingly costly for the challenger to restrain itself close to the bomb [emphasis added]".[607]

Whereas the nuclear literature is rife with historical examples described above, we have not yet witnessed a case of a government waiting to acquire cyber weapons (i.e. paused its program to develop cyber weapons) with as aim to bargain for concessions from allies or adversaries. More specifically, as far as I am aware, there has been no public case of a state making an explicit demand for concessions to another state, backed by a threat to develop cyber weapons if the target does not comply.

On the surface, it is unclear why cyber latency cannot be used for political gain. After all, cyber weapons are widely perceived to be 'equalizers' among states. As former U.S. President Barack Obama writes in a commentary of the Wall Street Journal in 2012; "[i]n a future conflict, an adversary unable to match our military supremacy on the battlefield might seek to exploit our computer vulnerabilities here at home."[608] In a review of the 'cyber international relations' literature between 2001-2010, Reardon and Choucri found that "all of the authors [with one scholar being the exception] see cyberspace as a potential tool of empowerment."[609] This suggests that proliferation of these capabilities would pose higher costs on other states. Adversaries (and allies) thus suffer from a loss in relative power when the other state acquires cyber weapons. Hence, rather than to absorb these costs, there are incentives for states to restraint others from acquiring cyber weapons which opens up an opportunity for the type of coercive diplomacy described above.

Yet, delving into the logic of how a state uses its ability to produce nuclear weapons as a form of bargaining leverage, highlights why we have not witnessed these demands for cyber programs to date - and unlikely to witness them in the future. The first and most obvious reason is derived from the potential to set demands. The challenger's ability to signal its decision to forego cyber weapons, as Volpe's study indicates, depends on the target's compliance with a clear set of demands. Yet, as

[606] Ibid, p.9
[607] Ibid, p.9
[608] Barack Obama, "Taking the Cyberattack Threat Seriously," *Wall Street Journal, (*2012, July 19) retrieved from: https://www.wsj.com/articles/SB10000872396390444330904577535492693044650
[609] Reardon and Choucri, "The Role of Cyberspace in International Relations," p. 9; Evgeny Morozov, "The Internet," *Foreign Policy,* 179 (2010), 40-44; For a critical perspective on whether weaker actors can use 'cyber warfare' to counter advantages of stronger adversaries see: Lindsay, "Stuxnet and the Limits of Cyber Warfare"

earlier noted, cyber weapons are not a new 'absolute weapon'. Hence, the clear demands it can set are much lower, less noticeable.

Second, and more importantly, the 'bargaining chip' can only be placed on the table if a state is able to leverage milestones in capability development to compel certain concessions. Also, as Thomas Schelling notes, coercive diplomacy needs to be backed up by "a convincing, self-biding, promise" to exercise restraint once the target capitulates.[610] For nuclear weapons, the critical milestone to be leveraged is that of ENR technology.[611] This means that normally the main goal of a nuclear arms control deal is to create mechanisms in which the status-quo power can detect, punish, and prevent future progress towards the bomb and particularly the dismantling of this type of technology.

As was described in chapter 4, for sophisticated cyber weapons, the key milestone for latency concerns intelligence gathering.[612] It is extremely difficult for a state to share this milestone publicly without impending on its effectiveness. And even if this would be possible, to make an assurance of restraint is even harder. Restraint is normally the process of physically rolling back the required infrastructure. When Muammar al-Qaddafi in December 2003 agreed after months of negotiations to disclose and dismantle its weapons of mass destruction program, it had to allow international inspectors unconditional access to its facilities to monitor and verify compliance.[613] As Libya agreed to the requirements of the Additional Protocol of the NPT it also permitted the establishment of mechanisms to monitor its export-import locations.[614] Iran, today, is subject to similar (if not more intense) efforts to close all potential pathways constructing for nuclear weapons.[615] It is currently the

[610] Thomas C. Schelling, *Strategy of Conflic*t, (Cambridge, Mass.: Harvard University Press: 1960), p. 43; Thomas C. Schelling, *Arms and Influence* (New Haven, Conn.: Yale University Press: 1966), p. 76
[611] Matthew Fuhrmann and Benjamin Tkach, "Almost nuclear: Introducing the Nuclear Latency dataset," *Conflict Management and Peace Science*, 32:4 (2015) 443-461, p. 444
[612] As mentioned in chapter 4, this especially applies to sophisticated cyber weapons.
[613] Already in early October 2003, the U.S. and the UK seized a large amount of centrifuge parts for uranium enrichment heading towards Tripoli as part of the Proliferation Security Initiative. See: Nuclear Threat Initiative, "Libya Nuclear Chronology," (2011, February), retrieved from: http://www.nti.org/media/pdfs/libya_nuclear.pdf?_=1316466791; Rubert Cornwell, "Intercepted Shipment was a Key to Libya Deal," *Financial Times Global News Wire*, (2004, January), retrieved from: http://www.independent.co.uk/news/world/politics/intercepted-shipment-was-key-to-libya-deal-72546.html
[614] Nuclear Threat Initiative, "Libya Nuclear Chronology"; International Atomic Energy Agency, "Additional Protocol. What is the Additional Protocol?," retrieved from: https://www.iaea.org/safeguards/safeguards-legal-framework/additional-protocol
[615] For an excellent report on the Iran nuclear deal see: International Crisis Group, "Implementing the Iran Nuclear Deal: A Status Report," *Middle East Report*, 173, (2017, January 16), retrieved from: https://www.crisisgroup.org/middle-east-north-africa/gulf-and-arabian-peninsula/iran/173-implementing-iran-nuclear-deal-status-report

most monitored nuclear program in the world, with the IAEA using a live, online enrichment monitoring system and surveilling of the nuclear fuel chain in real time.[616]

A similar type of handover is not possible for a cyber weapons program. Indeed, it is hard to apprehend what it means to forgo a capability in this context. Should a state make a list of all the information and lines of code it has started to acquire and put it on a USB flash drive? How can we check if a state disclosed all its zero-day exploits? As Vincent Boulanin also concludes, "cyberweapons can be reproduced and stored at minimal cost. Furthermore, arms control treaties require verification mechanisms, but it is beyond dispute that no state would allow a third party to scan its governmental computer systems and networks for this purpose."[617] Overall, with capability more embedded in humans than in technology, restraint of this kind is inherently more difficult. The stages when a state has a non-latent, latent, and actual capability are also more difficult to verify - as discussions in Chapter 3 and Chapter 4 have shown as well.

Cyber Bargaining Proposition II: The prospect of a state giving up its offensive cyber capability can lead to coercive bargaining advantages.

The same mechanisms described above also affect the dynamics for the second type of coercive diplomacy: that is, why it is difficult for a state to use cyber weapons as a bargaining device to potentially give up once a state has obtained them. It is subject to similar conditions; the state needs to prove it has an offensive cyber capability, it can forgo this capability, and that it cannot or does not develop a new capability in the foreseeable future. All these conditions are difficult to maintain.

First, 'proving' you have a specific type of cyber capability to threaten others is difficult. This is partially because of the immaterial ontology of cyber weapons.[618] In the words of Thomas Rid, 'you can't parade a code on the streets of Moscow.'[619] It is also the result of the malleability of cyberspace. The premise of cyber weapons being highly transitory in nature is that once you expose a capability,

[616] Ibid, p. 3

[617] Boulanin provides a number of additional reasons why 'cyber arms control' is difficult, next to the technical complexity of monitoring 'stockpiles' of cyber weapons. This includes; definitional problems with cyber weapon, rapid change of malicious capabilities, attribution problems, and strategic usage. According to Litwak and King, the reason cyber arms control is difficult is because "unlike the nuclear weapons under the control of states, cyberspace (along with the oceans, air, and outer space) is part of the world's shared spaces [...] that is integral to globalization and a domain in which non-state actors can increasingly exercise power and influence rivaling that of states." Yet, the analogical reasoning of Litwak and King is flawed. The scholars compare nuclear weapons with cyberspace, rather than with cyber weapons (which can be under the control of states). See: Robert S. Litwak and Meg King, "Arms Control in Cyberspace?" (2015, November 2), retrieved from; https://www.wilsoncenter.org/publication/arms-control-cyberspace; Vincent Boulanin, "Arms production goes cyber: a challenge for arms control," *SIPRI Publication*, (2013, May 30), retrieved from: https://www.sipri.org/node/361

[618] See chapter 2 for a more comprehensive discussion.

[619] Rid, *Cyber War Will not Take Place*

the adversary could relatively easily adapt its systems to avert intrusion.[620] The exposure of a zero-day means that its effectiveness is practically lost.[621] The problems with the second and third conditions were already addressed above: even if a program can be dismantled, monitoring and verifying potential cheating after a state has given up its capability is virtually impossible.[622]

Cyber Bargaining Proposition III: The threat of a state using a cyber weapon can lead to coercive bargaining advantages.

This leaves us with the third, and perhaps most compelling question: once a state has developed cyber weapons which can cause significant harm or damage, can the threat of usage lead to coercive advantages?

Given that it is difficult to prove you have a specific type of offensive cyber capability pre-deployment, the starting observation for this proposition is that the best state actors can do is, what scholars call, 'cheap talk'.[623] Cheap talk entails the costless verbal communication to potential other actors.[624] Verbal threats or promises, void of costs on the sender, are less likely to change behaviour of the defender. Yet, literature has shown that it does *not* mean they are inherently empty or inconsequential.[625] There are certain conditions when cheap talk might still be able to work.

The two main conditions which affect the effectiveness of cheap talk concern reputation and audience costs.[626] Considering these two conditions in relation to the threat of conducting a cyber attack reveals some compelling dynamics which have so far remained largely unrecognised.

---

[620] Smeets, "A Matter of Time"
[621] There may still be a patching and adaptation delay. Ibid, p. 11
[622] Also, for cyber capabilities it is even more difficult to distinguish between a civilian and military program.
[623] Travis Sharp argues that "cyber operations lack persuasiveness because they are less physically destructive than kinetic military force, meaning the target will interpret them as cheap talk." Yet, cheap talk is not about the destructiveness of the attack, but the ability to verify claims. See: Travis Sharp, "Theorizing cyber coercion: the 2014 North Korean operation against Sony," *Journal of Strategic Studies*, (2017)1-29
[624] Farrell and Rabin state that cheap talk is "costless, nonbinding, nonverifiable messages that may affect the listener's beliefs." In turn, Thyne distinguishes cheap talk from cheap signals, which concern "day-to-day communications that are apt to exhibit a high degree of volatility over time". Joseph Farrell and Matthew Rabin, "Cheap Talk," *Journal of Economic Perspectives*, 10:3 (1996):103-118, p. 104; Clayon L. Thyne, "Cheap Signals with Costly Consequences: The Effect of Interstate Relations on Civil War," *Journal of Conflict Resolution*, 50:6 (2006)937-961, p. 941
[625] For models where cheap talk can influence behavior see: Vincent P. Crawford, "Lying for Strategic Advantage: Rational and Boundedly Rational Misrepresentation of Intentions," *The American Economic Review*, (2003, March)133-149; Vincent P. Crawford and Joel Sobel, Strategic Information Transmission, *Econometrica*, 50:6(1982)1431-1451; Joseph Farrell and Robert Gibbons, "Cheap Talk with Two Audiences," *The American Economic Review*, 79:5 (1989)1214-1223
[626] The argument is actually that it makes cheap talk more costly, and hence, ironically, you may no longer want to call it cheap talk. Kydd has shown that cheap talk can also be effective when there is sufficient overlap in interest between the two actors. Andrew Kydd, "Which Side Are You On? Bias, Credibility, and Mediation," *American Journal of Political Science*, 47:4 (2003)597-611

I will first consider the role of reputation with respect to cheap talk. A reputation for resolve, Thomas Schelling notes, is "one of the few things worth fighting over".[627] Numerous studies have contended that reputation affects the credibility of the policy-leaders' statements and alters their bargaining position.[628] The main underlying mechanism is well-described by Alexandra Guisinger and Alastair Smith: "[c]redibility arises from the expectation of future continued gains from retaining an honest record. Diplomatic statements are believed only if a country's or leader's credibility is unmarred. Leaders keep their word so that they are believed in later crises."[629]

The focus of these studies on signalling is for the most part on how leaders' reputation can more credibly convey their intentions or interests. As Guisinger and Smith also state, "[t]he problem for both the threatened and threatened countries during a crisis is that they lack information about each other's interests".[630] Yet, we know from the classic threat perception and balance of threat literature that a threat assessment of actors - and their potential willingness to resolve - is not just about actors' intentions but should at least also consider their capability.[631] After all, an actor with bad intentions but limited capability is not perceived to be a real threat. An actor with significant capabilities to harm you, but has no intention do so is not a threat either.

The bias in the literature is hardly surprising, though it has important consequences for understanding the role of reputation in relation to the strategic bargaining value of cyber weapons. The vast amount of literature on bargaining and reputation is written against the backdrop of the nuclear arms race during the Cold War - a time in which the capability component of the 'threat equation' was undisputed. The atomic bombing of Hiroshima and Nagasaki had dramatically demonstrated the destructive impact of nuclear weapons to the world. There was also little secrecy as to who was able to deploy this capability, and that potentially any area in the world could be hit.[632] This meant that the primary unknown variable in the equation concerned the actors' willingness to attack.

Yet, for the threat of using cyber weapons - as the discussion above has made apparent on the limited ability to showcase capabilities - there is both uncertainty over the intend *and* the ability to use an

[627] Schelling, *Arms and Influence*, p. 124
[628] Several scholars have discussed the ways in which domestic institutions or reputational issues can make cheap talk more costly. Alexandra Guisinger and Alastair Smith, "Honest threats: The interaction of reputation and political institutions in international crises," *Journal of Conflict Resolution*, 46, (2002)175-200; Anne Sartori, "The Might of the Pen: A Reputational Theory of Communication in International Disputes," *International Organization*, 56 (2002)121-50; Kristopher Ramsay, "Politics at the Water's Edge: Crisis Bargaining and Electoral Competition," *Journal of Conflict Resolution*, 48, (2004)459-86.
[629] Guisinger and Smith, "Honest threats," p.175
[630] Ibid, p. 176
[631] Stephen Walt, *The Origin of Alliances*, (Ithaca, NY: Cornell University Press: 1987)
[632] Also see chapter 3 for a longer discussion on this topic.

offensive cyber capability.[633] As David Gompert and Martin Libicki note: "offensive capabilities can only be inferred from anodyne policy statements or from claims made by others about the extent and authorship of this or that cyber-espionage intrusion."[634] This has led to a number of paradoxical dynamics and bargaining position outcomes. To illustrate this point consider the following two examples.

First, the release of the classified NSA documents by Edward Snowden has been described as the most embarrassing episode in the history of the secretive U.S. intelligence agency. It revealed how the NSA maintained a mass-surveillance program over its own citizens, accessed data from companies, intercepted data from global communications networks, and stored information of millions of people. Yet, it also exposed the impressive arsenal of the agency. Not least, from the Snowden disclosures, the Washington Post reported that the U.S. government mounted at least 231 offensive cyber operations in 2011.[635] As Gompert and Libicki note, in this way, the leaks have ironically "helped it to broadcast how deeply the NSA can supposedly burrow into the systems of others."[636]

A similarly interesting case concerns the French revelation about their espionage capabilities. In 2014, researchers at Kaspersky Lab published a series of reports on various espionage tools associated with an advanced threat actor they called 'Animal Farm'.[637] The 'Farm' includes several Trojans, which Kaspersky grouped together into six families**:** Bunny**,** Dino**,** Barbar, NBot**,** Tafacalou, and Casper.[638] For a long time the French government was believed to be behind the development of the sophisticated capabilities within the intelligence community. A classified presentation from the Canadian government, also disclosed as part of the Snowden revelations, confirmed this suspicion.[639] The French government for a long time denied that they were behind the development of the malware. Yet, in June 2016 during a guest lecture at a French engineering school, Bernard Barbier, the former

[633] One corollary argument may from the rationalist perspective is that cyber conflict is more likely to occur than conventional conflict. See James D. Fearon, "Rationalist Explanations for War," *International Organization*, 49:3 (1995)379-414
[634] David C. Gompert and Martin Libicki, "Waging Cyber War the American Way," *Survival*, 57:4 (2015)7-28, p. 21
[635] Barton Gellman and Ellen Nakashima, "U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show," *The Washington Post*, (2013, August 30), Retrieved from: https://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html
[636] Gompert and Libicki, "Waging Cyber War the American Way"; also see: Martin Libicki, *Cyberspace in Peace and War*, (Annapolis, Naval Institute Press: 2016), p. 198
[637] Kaspersky Lab, "Animals in the APT Farm," *Securelist*, (2015, March 6), retrieved from: https://securelist.com/blog/research/69114/animals-in-the-apt-farm/;
[638] Ibid
[639] Pierluigi Paganini, "Dino Malware that targeting Iran belong to Animal Farm's arsenal," *Security Affairs*, (2015, July 1), retrieved from: http://securityaffairs.co/wordpress/38204/cyber-crime/dino-malware-animal-farm.html

technical head of the French DGSE (General Directorate of External Security) admitted the development and deployment of the capability. [640] In the talk he also said that he assembled a hacking team as early as 1992.[641] According to Bruce Schneier, the former head "talked about a lot of things he probably shouldn't have."[642] Yet, we could also view it in a different light: it is a post-hoc confirmation of capabilities in order to potentially enhance the French government's reputation in this new area of conflict.[643]

Post-hoc revelations about an actor's capability - either intentionally or non-intentionally - can add to the credibility of the actor's cheap talk on the ability to conduct a cyber operation. In that sense, it is a bit like a game of Texas Hold'em poker; when someone reveals his or her excellent hand after raising post-flop and all the other players fold.[644] If you reveal your hand it can add to the player's credibility for the next play - not only towards the person you played against (and folded post-flop) but also to the other people at the table who were not part of this hand and folded pre-flop (but were observing).

Yet, this dynamic is even stronger in the case of cyber weapons. The principles of Bayesian inference reveal why this is the case. First, let us take a poker scenario in which you show a strong hand at t=0. When you get new cards the next turn, in t=1, the other players at the table know that the probability you once again will get a strong hand has not changed.[645] At most, the person's beliefs are updated that you only raise/play with a good hand. In contrast, imagine a situation in which a state admits the usage of a sophisticated cyber weapon against another actor during a crises in t=0.[646] In the following period, t=1, the other threatened actors are likely to update their beliefs differently. The revelation

[640] Youtube, "Espionnage et cybersécurité, Bernard Barbier reçu par Symposium CentraleSupélec," (2016, September 5), retrieved from: https://www.youtube.com/watch?v=s8gCaySejr4
[641] Ibid.
[642] Bruce Schneier, "Talk by the Former Head of French SIGINT," (2016, September 7) Retrieved from: https://www.schneier.com/blog/archives/2016/09/talk_by_the_for.html
[643] This occurs at a time when French government is forced to increase military spending on other issues, particularly terrorism, and other actors started to publicly announce their aim to develop offensive cyber capabilities. Other excerpts of the lecture confirm this view: "I received the order from Mr. Sarkozy's successor to go to shout at the Americans. It was on April 12, 2013 and it was really a great moment in my professional career. We were convinced it was them. At the end of the meeting, Keith Alexander [director of the NSA from 2005 to 2014] was not happy. While we were in the bus, he told me he was disappointed because he never thought they would have been caught. He added: 'You are pretty good.' As allies, we didn't spy on them. The fact that the Americans broke this rule took us by surprise"; See: Youtube, "Espionnage et cybersécurité"; Alex Grisby, "Shouting at Americans: A Peek Into French Signals Intelligence," *Council on Foreign Relations: NetPolitics*, (2016, September 15), retrieved from: http://blogs.cfr.org/cyber/2016/09/15/shouting-at-americans-a-peek-into-french-signals-intelligence/
[644] For the rules of Texas Hold'em poker see: Blakesware "A Guide to Texas Hold'em Poker," retrieved from: http://www.how-to-hold-a-party.com/downloads/HowToPlayPoker.pdf
[645] Only irrational opponents who think luck is on the side of the other play or the deck is stacked in against them, will update their beliefs in this manner.
[646] A scenario with a similar outcome is when the actor reveals it has a sophisticated cyber weapon as a 'backup' during a crises.

does not only increase the likelihood that the actor is honest about its capability in case of crises, it also increases the probability that the actor has a strong capability in t=1.[647]

The second issue which can affect the effectiveness of cheap talk concern 'audience costs'. Involving the domestic or international audience during a crisis is supposed to make backing down more difficult, and cheap talk more credible. The logic is most famously spelled out by James Fearon in his article *Domestic Political Audiences and the Escalation of International Disputes*.[648] Fearon models an international crisis as a political 'war of attrition'. He justifies his model based on the way crises unfold; "crises are public events carried out in front of domestic political audiences".[649] This means that crises have two defining features. "First, at each moment a state can choose to attack, back down, or escalate the crises further. Second, if a state backs down, its leaders suffer audience costs that increase as the crisis escalates," Fearon states.[650] Because crises unfold in this way, Fearon's equilibrium analysis shows how "audience costs enable leaders to learn an adversary's true preferences concerning settlement versus war and thus whether and when attack is rational."[651] One of the key implications is that the side with the highest audience costs (normally a democracy) is less likely to back down.[652]

The implications of Fearon's argument are compelling for cyber crises. When it comes to the potential use of a cyber weapon a crises does not have to unfold in public. How and when audience costs come into play depends both on the offender and defender, and possibly other actors. Overall, what becomes apparent from the discussion below is that, if a state - or dyad of states - is aware of how to play out audience cost' dynamics, it opens up a lot of room for strategic manoeuvre and calculation.

There are various ways in which a 'cyber crisis' may unfold. A simple scenario is when the threat of using a cyber weapon is conceived as a single act; i.e. no cyber-attack with as aim to cause harm or damage has yet occurred, and one state is threatening another state to conduct this type of activity (possible starting a cyber conflict, or broader conflict). A more iterative scenario is possible too. One can conceive of a situation in which cyber weapons have been used on a minor scale; for example, a certain 'wiper' has damaged a number of desktops of a government entity. The attacking state

[647] Considering the transitory nature of cyber weapons, it is unclear how the perception changes after multiple periods (i.e. t=x). But the basic idea is that there is some retention of talent following t=0 which affects this reputation. See: Smeets, "A Matter of Time"
[648] James D. Fearon, "Domestic Political Audiences and the Escalation of International Disputes," *American Political Science Review*, 88:3 (1994)577-592
[649] Ibid, p.577
[650] Ibid, p.577
[651] Ibid, p.577
[652] Ibid.

threatens to conduct a follow on cyber-attack; possibly against the control system architecture of an important process plant.

One dynamic which exists across all cyber crises is the difficulty for the defender of uncovering activities of the attacker in preparation of conflict. Preparation for conventional warfare generally requires the physical movement of military equipment and people. Perhaps the most overt and infamous in its kind is the mobilization of the Russian army pre-World War I, then the largest standing army in the world with around five million soldiers. A more recent example concerns Vladimir Putin's placement of some 40,000 troops along the Ukrainian border.[653] Less overt preparation concerned Khrushchev's placement of missiles in Cuba or the U.S. placement of medium-range Jupiter missiles in Turkey.[654]

For most cyber operations, no actual movement of capabilities is required in preparation of an attack. In the exceptional circumstance in which physical facilities are constructed as a testbed for malware, they can generally be prepared far away from the target's location - at a place most convenient to the attacker. [655] Stuxnet is alleged to have been tested at laboratories of the Department of Energy across the U.S. and at the Dimona facility of Israel.[656]

Even if the preparations of a cyber-attack are discovered further complications remain. If the defending actor discovers malicious activity in its systems, it is difficult to gauge the exact intensions of the attacker.[657] Sophisticated cyber-attacks generally take place across multiple 'stages', i.e. multi-stage cyber-attack.[658] The first stage is *reconnaissance*.[659] This includes the attacker 'sniffing' (to eavesdrop on existing data traffic), 'footprinting' (to gain knowledge of the network or security posture), and/or 'enumeration' (to identify user accounts which can potentially be exploited). The

[653] Unknown Author, "Ukraine troops on high alert as tension with Russia grows", (2016, August 12), *BBC News*, retrieved from: http://www.bbc.co.uk/news/world-europe-37049313
[654] Allison and Zelikow, *Essence of Decision*
[655] For a more detailed discussion see chapter 3.
[656] Sanger, *Confront and Conceal*
[657] For a more detailed discussion of the potential implications see: Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations*, (London: Hurst Publications: 2017)
[658] The term multi-stage attack is often used in the literature. It has at least two different meanings. For Landau and Clarke this occurs when computer A penetrates computer B, which is then used to penetrate computer C, and so on. For others (e.g. Rid and Buchanan), multi-stage is when a cyber attack occurs through steps that can be temporarily be distinguished. It refer to the latter meaning in this article. See David D. Clarke and Susan Landau, "The problem isn't attribution; It's multi-stage attacks," *ACM ReArch*, (November 30, 2010); Rid and Buchanan, "Attributing Cyber Attacks"
[659] I follow the framework of: S. Mathew, R. Giomundo, S Upadyaya, M. Sudit, and A. Stotz, "Understanding Multistage Attacks by Attack-Track based Visualization of Heterogeneous Event Streams" VizSEC '06, *Proceedings of the 3rd international workshop on Visualization for computer security* (2016)1-6; Other frameworks exist, see for example: FireEye, "Advanced Targeted Attacks: How to Protect Against the Next Generation of Cyber Attacks," *White Paper*, (2012), Retrieved from: http://www.softbox.co.uk/pub/fireeye-advanced-targeted-attacks.pdf

second stage concerns *intrusion*. We commonly distinguish between user intrusion (with non-administrative user privileges) and root intrusion (with administrative user privileges). The third stage of a cyber-attack is *privilege escalation'*.[660] At this stage a vulnerability is exploited in an operating system (OS) or specific service / software package. Finally, there is the stage which gives away the *goal* of the attacker. This could be Denial of Service (DoS), installation of a backdoor, exfiltrating data, espionage or corruption (with as aim to cause harm or damage). The order of activities conducted by APTs is often highly complex, and different tasks may be executed - even outside of cyberspace - with long periods of time in between.[661] This means that, if for example, an attack is discovered at the third-stage, the defender is still unsure as to what the attacker is aiming to do. Also, as more recent malware cases with a highly modular structure like Duqu have shown, that the functionality of malware may change on a case-by-case basis - depending on the target system and context.

If a cyber crises unfolds iteratively, an additional complication to raise audience costs concerns the leeway for plausible deniability following discovery of initial activities (i.e. after the first series of attacks). The problem of attribution has been addressed at-length in Chapter 3. In the case of the DNC hack, all signs pointed to Russian state actors being behind it and not a '400-pound hacker.'[662] Yet, at international conferences or seminars one of the most common questions asked by people outside the intelligence community remains; 'do we *really* know it was Russia?' This complicates efforts to raise audience costs, go public, and potentially prevent an iterative scenario to unfold.

There are also numerous examples of incidents in which the defender instead of the attacker denies that an attack has ever occurred. Being victim of a cyber-attack is often seen as an embarrassment, leading actors to count their losses behind closed doors rather than going public.[663] This leads to a broader question which has been insufficiently addressed to date which is: under what conditions should a defensive actor 'name and shame' (i.e. go public) the attacker following an intrusion? Even though a lengthy discussion of this topic goes beyond the scope of this research, possible considerations may include; nature of the attacker (e.g. some actors such as ISIS may gain in reputation when being called out); nature of the attack (e.g. going public and publishing a report on

[660] This is usually for buffer overflow attacks, in which the program overwrites memory adjacent to a buffer that should not have been modified.
[661] For example, a backdoor (i.e. a way to bypass normal authentication) may be initially installed in t=0, and check-ups might take place in later time periods t=1, t=2, and t=3 to see if it still exists, but a future attack using that backdoor might occur only in t=x.
[662] Thomas Rid, "All Signs Point to Russia Being Behind the DNC Hack," *Motherboard*, (2016, July 25), retrieved from: https://motherboard.vice.com/en_us/article/all-signs-point-to-russia-being-behind-the-dnc-hack
[663] A more detailed discussion is provided in section 6.3.

a sophisticated APT might prevent future attacks, especially if zero-day exploits are used); and historical context.

Finally, cybersecurity firms - or other actors - can raise the audience costs of a cyber crises between two states. Though the publication of malware samples and reports is much more political than sometimes depicted, cybersecurity firms do have independent agency (some more than others).[664] This may lead to potential cyber crises in which both state actors may not want to incur audience costs - as it would make backing down more difficult - but other actors force them to. Stuxnet may again be an excellent case in point. After all, it was not the Iranian government which went public about the attack - in fact they denied Stuxnet disrupted their nuclear program at all.[665] Instead, the worm was discovered and disclosed by private sector researchers from VirusBlokAda, Symantec, the Langner Group and later others.[666]

The above section assessed three propositions to better understand to what degree the (potential) possession of cyber weapons can provide strategic utility. An analysis of the first two propositions indicated that a state's ability to develop or possession of a cyber arsenal is unlikely to provide bargaining advantages. However, as an assessment of the last proposition has revealed, the threat of using cyber weapons can provide strategic utility. More specifically, when states develop a reputation over time, the expectation is that 'cheap talk' can become more effective. Also, the potential involvement of domestic or international audiences could make cyber threat postures more credible and effective.

6.4 The Strategic Value of using Cyber Weapons

The purpose of this section is to assess how the usage of cyber weapons can provide strategic advantages. I distinguish between the use of two different types of cyber weapons - that is, 'counterforce cyber weapons' (CFCW) and 'countervalue cyber weapons' (CVCW) - and show how each could support different objectives.[667]

[664] Smeets, "When Naming Cyber Threat Actors Does More Harm Than Good,"
[665] Unknown Author, "Iran denies Stuxnet disrupted its nuclear programme," *BBC News*, (2010, November 24), retrieved from: http://www.bbc.co.uk/news/technology-11821011
[666] There is of course the opportunity to deny the event in public and then respond covertly.
[667] Austin Long has previously made a similar distinction. However, the scholar only briefly describes what strategic goals the capabilities can achieve. See: Austin Long, "A cyber SIOP? Operational consideration for strategic offensive cyber planning," *Journal of Cybersecurity*, 3:1 (2017), 19-28

6.4.1 Distinguishing between Counterforce and Countervalue Capabilities

When thinking about the strategic utility of using cyber weapons, a useful distinction to consider is that of 'counterforce' and 'countervalue' targeting. The terms have been long used in nuclear planning as the two main courses of military action.[668] Counterforce is when an actor decides to strike at the opponent's military forces or infrastructure. This is differentiated from countervalue strikes which targets the sources of an opponent's national strength.[669] In this context, CFCW concerns a capability designed to be used against targets relevant to the military operation. CVCW refers to a capability designed to be used against vital assets of the adversary. I present these two categories as Weberian 'ideal-types' meaning that in reality the distinction might become blurred.

Table 6.1 lays out the dimensions of the two capabilities, revealing in which areas they likely overlap and differ. First, the conventional notion of 'range' is not part of the definition and not a characteristic of either type of cyber weapon. Normally, range refers to the distance to which a projectile may be send by a weapon. Range is thus inherently connected to geography, a principle which has little meaning in cyberspace.[670] "Places have become geographically disembedded, that is, they are less and less determined and defined by physical-geographical features," as Brey writes.[671] A capability may be a CFCW even though it is used against an adversary geographically distant (but on the battlefield). And, reversely, you may attack a country nearby with a CVCW.

There is also no inherent feature in the vulnerability, access, or payload of a cyber weapon which makes it either a countervalue or counterforce asset. Both capabilities can exploit either software, hardware, or network vulnerabilities and can access air-gapped or non-airgapped systems. Indeed, despite some of the uncertainty about the exact vulnerability exploited in the case of Operation Orchard, it can be classified as a CVCW.[672]

The discussion on payload is associated to what in nuclear terminology is referred to as 'yield'. Also, yield is not and cannot be considered a defining feature of the classifying cyber weapons. Yield is

[668] Dieter S. Lutz, "A Counterforce/Countervalue Scenario - or How Much Destructive Capability is Enough?", *Journal of Peace Research*, 20:1 (1983)
[669] William A. Stewart, "Counterforce, Damage-limiting, and Deterrence," *RAND Corporation*, (1967, July), retrieved from: https://www.rand.org/content/dam/rand/pubs/papers/2008/P3385.pdf
[670] This does not mean that geography does not matter at all in cyberspace, as discussed in chapter 2.
[671] Philip Brey, "'Space-Shaping Technologies and the Geographical Disembedding of Place," *Philosophy & Geography*, 3 (1998)239-263
[672] See Adlee's discussion on the possibility of backdoors. Adlee, "The Hunt for the Kill Switch"

conventionally calculated using precise, physical standards. For example, it was alleged that the early Soviet intercontinental ballistic missile could carry a three megaton warhead (RDS-37) or a five megaton warhead (RDS-46).[673] A similar classification for cyber weapons' payload is not possible; there is no convention for expressing 'maliciousness' in a code as it is target-dependent.[674] Having said that, for strategic purposes as becomes clear below, it is more likely that a counterforce cyber weapon intends to cause less direct harm or damage than a CVCW.

CVCW's principal target concerns the critical infrastructure of state actors. Targets may concern facilities for water supply, telecommunication, electricity generation, or public health. Most non-state actors are less dependent on territorial assets, making it more difficult to effectively use these capabilities. For counterforce cyber weapons, it concerns military and operational infrastructure of state and possibly non-state actors.[675]

Understanding the costs of these capabilities is not straightforward. Individually, a CFCW may be cheaper than a CVCW. Chapter 4 has laid out in detail the obstacles actors have to overcome to conduct a cyber-attack against an industrial control system of a critical infrastructure. Yet, overall, CFCW may actually be more expensive to maintain and use - especially when these capabilities are used in response to the actions of other actors.

To clarify this dynamic imagine a situation in which there are multiple terrains of potential conflict. To ensure an actor can use counterforce capability when an adversary mobilizes its military capability in one of those regions, it needs to develop a capability for all of them.[676] Yet, a state can use the same CVCW in this scenario, regardless of where the adversary will attack. The additional costs of relying on counterforce cyber weapons then comes from two sources: i) an actor needs to develop more weapons to impose costs on an adversary (if used reactionary), and ii) a more constant effort to maintain the effectiveness of these capabilities is required given cyber weapon's transitory nature.[677] This notion echoes John Lewis Gaddis conclusion on strategies of containment. A more limited form of containment, heavily relying on nuclear weapons, is cheaper but also less flexible. The more extensive form of containment - following the notion that the U.S. would defend any territory

[673] John Pike, Charles Vick, Mirko Jacubowski, and Patrick Garrett, "R-7 - SS-6 SAPWOOD", (2000, July 29), retrieved from: https://fas.org/nuke/guide/russia/icbm/r-7.htm
[674] For similar point see: Michael Fischerkeller, "Incorporating Offensive Cyber Operations into Conventional Deterrence Strategies", *Survival*, 59:1 (2017)103-134
[675] Notice that in practice operational infrastructure and critical infrastructure may overlap. For example, the distinction becomes blurred if one takes down the electricity grid which feeds a town and a military base.
[676] This assumes that there is no overlap in weaknesses to exploit.
[677] Smeets, "A Matter of Time"

regardless of means and area - provides more flexibility; but it also strains budgets. The aggressor can pick location and you have to respond accordingly.

Table 6.1: Countervalue and Counterforce Dimensions of Cyber Weapons

Dimension	CVCW	CFCW
Target	Vital asset adversary	Operationally relevant asset
Type of Target	Often civilian	Often military
Range	Irrelevant	Irrelevant
Vulnerability	Undetermined	Undetermined
Access	Undetermined (often air-gapped infrastructure)	Undetermined
Type of payload	Undetermined	Undetermined
Nature adversary	Normally state-actor	Both state and non-state actor
Costs	Individually, more expensive Collectively, cheaper	Individually, cheaper Collectively, more expensive

We can list numerous examples of counterforce targeting of cyber weapons by state actors.[678] In July and August 2008 Russia launched a DDoS-attack against Georgia's network, coinciding with troops entering the Georgian province South Ossetia. [679] The attack, conducted in two phases, initially focused on Georgian news and government websites and later embraced a broad set of targets including educational institutions, financial institutions, businesses, and Western media.[680] The attacks complicated Georgian efforts to manage its logistics, command commands and deliver its war materials on time.

Another example of a CFCW is US' Suter program, developed by BAE systems. A good overview of this capability is provided by Zheng:[681]

> Until now, there has been very little understanding of the Suter system by the external world. With limited information from scattered reports, all we know is that it is a set of wireless

[678] One may consider counterforce operations also more broadly - i.e. also assesses those operations which did not cause any harm or damage. An interesting case of this kind concerns a variant of X-Agent malware for Android devices created by Fancy Bear to collect intelligence on Ukrainian field artillery units. A Ukrainian officer had developed an app to simply artillery troops' targeting data for the D-30 towed howitzer. See: Crowdstrike, "Use of Fancy Bear Android Malware in Tracking of Ukrainiian Field Artillery Units," (2017, March 23) retrieved from: https://www.crowdstrike.com/wp-content/brochures/FancyBearTracksUkrainianArtillery.pdf

[679] Asmus Ronald, *Little War that Changed the World. Georgia, Russia and the Future of the West*, (New York: Palgrave Macmillan: 2010); Shakarian Paulo, "The 2008 Russian Cyber Campaign Against Georgia," *Military Review*, (2011, November-December), p. 63-64

[680] Numerous patriotic hackers joined the campaign in the second phase.

[681] Zheng, "From Cyberwarfare to Cybersecurity in the Asia-Pacific and Beyond"

> reconnaissance, attack, and control combat systems. Through upgrades and integration, the Suter system has been tested on the RC-135 electronic warfare reconnaissance aircraft, EC-130H electronic jamming aircraft, and the F-16CJ fighter (with electronic warfare pods), and is now able to achieve a high level of integration of electronic warfare, cyberwarfare, kinetic destruction, and many other attacking techniques. The US Army tested Suter 1, Suter 2, and Suter 3 in its "Joint Expeditionary Force Experiment" (JEFX) in 2000, 2002, and 2004 respectively. In 2006, the US Army did not exercise Suter 4, probably because they used it directly in the Iraq war and the war in Afghanistan. In 2008, Suter 5 was tested in the JEFX again.[682]

The Israeli Air force allegedly used a similar technology to conduct an airstrike against a nuclear reactor in Northern Syria.[683] On September 6, 2007 F-15Is and F-16Is fighters flew into Syrian airspace, bombing the precise location of the nuclear plant in the Dier ez-Zor region of the country. Syria's air defence systems were fed a false-sky picture which led the fighters to conduct the entire process completely unnoticed.[684]

What are cases of CVCWs? Stuxnet can be categorized as a CVCW. Another example concerns the attack on the Ukraine power grid. On December 23, 2015 hackers took down almost sixty substations in Ukraine leaving more than 230.000 people without electricity for several hours.[685] As Kim Zetter writes, "they were skilled and stealthy strategists who carefully planned their assault over many months, first doing reconnaissance to study the networks and siphon operator credentials, then launching a synchronized assault in a well-choreographed dance."[686] Overall, there are fewer examples of countervalue cyber weapons known today used far from national borders and fielded

---

[682] Ibid

[683] David A. Fulghum, Robert Wall, and Amy Butler, "Cyber-Combat's First Shot," *Aviation Week & Space Technology*, (2007, November 26); Clarke and Knake, *Cyberwar*, Zheng, "From Cyberwarfare to Cybersecurity in the Asia-Pacific and Beyond"

[684] Although most scholars and media sources have looked at the event in 2007, it can be said that first part of this operation started much earlier. As Der Spiegel reports: "[i]n late 2006, Israeli military intelligence decided to ask the British for their opinion. But almost at the same time as the delegation from Tel Aviv was arriving in London, a senior Syrian government official checked into a hotel in the exclusive London neighborhood of Kensington. He was under Mossad surveillance and turned out to be incredibly careless, leaving his computer in his hotel room when he went out. Israeli agents took the opportunity to install a so-called 'Trojan horse' program, which can be used to secretly steal data, onto the Syrian's laptop. The hard drive contained construction plans, letters and hundreds of photos. The photos, which were particularly revealing, showed the Al Kibar complex at various stages in its development. At the beginning - probably in 2002, although the material was undated - the construction site looked like a treehouse on stilts, complete with suspicious-looking pipes leading to a pumping station at the Euphrates." See: Erich Follath and Holger Stark, "How Israel Destroyed Syria's Al Kibar Nuclear Reactor," *Der Spiegel*, (2009, November 2) retrieved from: http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663-2.html

[685] Initially thirty substations were taken down. The attackers later targeted two other power distribution centers. Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid"

[686] Ibid

military forces. Herein also lies an important observation; there is still much strategic room for states to be explored in this area.

6.4.2 Strategic Utility of Using Counterforce and Countervalue Cyber Weapons

Having laid out the dimensions of CVCW and CFCW, we can now look at the distinct advantages and disadvantages of these capabilities. I develop four 'cyber usage propositions' below. The first proposition is considered to be the 'master' proposition as the other observations follow from it:

- *Cyber Usage Proposition I: Cyber weapons provide an 'extra option' for state leaders*
- *Cyber Usage Proposition II: Cyber weapons can be used in conjunction with other military capabilities.*
- *Cyber Usage Proposition III: Cyber weapons can be used to achieve a form of psychological ascendancy*
- *Cyber Usage Proposition IV: Cyber weapons can be used effectively and for strategic gain with few casualties.*

Cyber Usage Proposition I: Cyber weapons provide an 'extra option' for state leaders

Gray in his review on the strategic utility of special operation forces writes:

> special operations can expand the options available to political and military leaders. […] In theory, there are always alternatives to the use of force - diplomacy, economic sanctions, and the like. In practice, however, there are some situations that one cannot resolve successfully without resort to physical coercion. The availability of a special operations capability means that a country can use force flexibly, minimally, and precisely. The realization by the enemy that one has a special operations capability can have beneficial effects on calculations made abroad. In time of war, both in its independent and supporting roles, special operations enhance the flexibility with which one can use force.[687]

The key point which comes to fore in this section about the utility of cyber weapons is very similar; having the choice to use a cyber weapon expands the options available to leaders.

Sanger writes in *Confront and Conceal* that"[t]he origins of the [US] cyberwar against Iran goes back to 2006, midway through George W. Bush's second term. Bush had often complained to his secretary of state, Condoleeza Rice, and his national security adviser, Stephen Hadley, that his options regarding Iran looked binary: let them get the bomb or go to war to stop it. 'I need a third option,' Bush told them repeatedly. [...] When that option emerged, it came from inside the bowels of the U.S.

[687] Gray, *Explorations in Strategy*, p. 174

Strategic Command, which oversees the military's nuclear arsenal."[688] The product was Olympic Games, as discussed in Chapter 4. Sanger writes that the motivation behind this operation was twofold. "The first was to cripple, at least for a while, Iran's nuclear progress. The second, equally vital, was to convince the Israelis that there were a smarter, more elegant way to deal with the Iranian nuclear problem that could quickly escalate into another Middle East war, one that would send oil prices soaring and could involve all the volatile players in the region," Sanger writes.[689]

In simple terms, it is said that cyber weapons allow for action within the 'gray zone' of foreign activities; not war nor peace. Herb Lin states that "nuclear comes after conventional conflict has commenced. […] Escalation concerns involve moving from conventional conflict to nuclear conflict. Going nuclear is escalatory. [Instead,] Cyber comes in the early stages of conflict (before kinetic war). In principle, cyber [is] just another weapon to be used by […] military forces. Going cyber is pre-escalatory."[690] Overall, having the choice to use a cyber weapon, the idea is that states add a rung on the 'ladder of escalation'.

Though cyber weapons provide an 'extra option', I argue against the view that these are pre-war capabilities simply add another rung to the ladder of escalation. Cyber weapons can be used in times of both peace and war; in conflicts with different intensity; with and without kinetic force; can influence the activities of all other domains of warfare; and lead to escalation or de-escalation. The exact nature and utility of usage, however, inherently differs for countervalue and counterforce capabilities - as will become clear from the discussion below. [691]

Proposition 2. Cyber weapons can be used in conjunction with other military capabilities.

The 2010 U.S. Department of Defence's *Quadrennial Defense Review Report* notes that "[u]nlike weapons of mass destruction, cyber weapons are an integral part of the commander's arsenal in conducting force-on-force and asymmetric warfare and will be used in concert with kinetic weapons to soften up the adversary's defences."[692] Indeed, there is little question that CFCWs can be deployed in conjunction with other military capabilities - in fact, that is what makes them attractive to use.

[688] Sanger, *Confront and Conceal*, p. 190-191
[689] Ibid
[690] Herb Lin, "Thinking about Nuclear and Cyber Conflict: Same Questions, Different Answers," (2015, May 15), Retrieved from: https://sipa.columbia.edu/system/files/Thinking%20about%20Nuclear%20and%20Cyber%20Conflict-Columbia-2015-05-14.pdf
[691] Kinetic warfare "involve[s] the forces and energy of moving bodies, including physical damage to or destructruction of targets through use of bombs, missiles, bullets, and similar projectiles." U.S. Air Force, "Air Force Doctrine Document 1-2" (2007, January 11), Retrieved from: http://www.globalsecurity.org/military/library/policy/usaf/afdd/1-2/afdd1-2-2007.pdf
[692] US Department of Defense, "Quadrennial Defense Review Report," Washington, D.C., (2010, February), p. 91-92

Cases like the Georgia DDoS attack or Operation Orchard reveal that CFCWs can dramatically increase the effectiveness of other military capabilities. The F-15s and F-16s used by the Israeli air force against Syria in 2007 were not equipped with stealth technology. But tipping-off Syria's air defence radar system nevertheless ensured the Israeli air force to accomplish their missions whilst remaining undetected.

The demonstrated effectiveness of CFCW as a force multiplier has led to the view that 'cyber' is a key dimension of modern hybrid warfare.[693] Frank Hoffman writes that "[h]ybrid wars are not new, but they are different. In this kind of warfare, forces become blurred into the same force or are applied in the same battlespace."[694] Few public documents, however, exist on how military forces exactly can accomplish this integration.

Though CVCWs, by nature, are not integrated with kinetic forces on the battlefield, there are still incentives to use these capabilities in conjunction with other forces in certain conflict situations. Consider a scenario in which actor A attacks actor B through either conventional or cyber means. The most obvious response of actor B (or ally of actor B) would be to raise the cost of the attacker (actor A) by deploying defence capabilities on the battlefield. But actor B can further raise the costs of the attack by means of using a CVCW against a vital asset of actor A. There are three conditions which could make this response (particularly) effective.

Condition 1: Actor B must be able to cause significant amount of harm or damage against Actor A

The first condition is perhaps the most obvious: Actor B must be able to inflict enough harm or damage against actor A that is perceived to be a substantive cost (which in turn can be leveraged). Offensive cyber capabilities which have the potential to cause the high levels of harm or damage often go beyond effects created in cyberspace. One could for instance consider the sabotage of a water dam or power plant through a cyber attack, leading to the *physical* destruction of this infrastructure.

In discussions on the use of conventional capabilities for coercive purposes the focus is on a geographical area. In the case of a nuclear bomb, we can calculate the different radii of serious and less serious contamination. What we cannot do is differentiate *within* that area. The usage of a cyber weapon does not come with these restrictions; its effects can be selectively dispersed across a large

[693] Sorin Dumitru Ducaru, "The Cyber Dimension of Modern Hybrid Warfare and its Relevance for NATO," *Europolity*, 10:1 (2016)7-23
[694] James N. Mattis and Frank G. Hoffman, "Future Warfare: The Rise of Hybrid Warfare," *Naval Institute Proceedings*, (2005, November), p. 30-32; Frank Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Warfare* (Arlington, VA: Potomac Institute for Policy Studies: 2007)

geographical space (e.g. all hospitals in a certain country). This opens up new ways of thinking when it comes to countervalue capabilities. Instead of taking down one vital asset of a country, there is also an opportunity to paralyze the country through attacking a large amount of geographically dispersed systems.[695]

Condition 2: Actor A must be able to discern the 'cyber response' from Actor B.

The second condition is that actor A must be able to discern with a high level of certainty that the retaliatory act through cyberspace comes from actor B. This condition might seem trivial - and it is for conventional capabilities - but for cyber weapons there are two complications. First, actor A must be aware that the attack came from Actor B. As discussed above, plausible deniability is normally said to be to an advantage to the attacker. Yet, in this case it is an additional hurdle for actor B, as the aim for actor B is to show that it is retaliating in response to actor A's actions. This discussion has led to early talk about the need to develop 'loud' cyber weapons.[696]

Second, actor A must be able to delineate actors B's 'cyber response' from the more constant state of cyber activity. Cyberspace, given its interconnectedness, is said to be a space of constant contact, action, hostility, and change. In February 2017, the director of UK's National Cyber Security Centre said that the country had experienced 188 'high-level cyber attacks' in the last three months.[697] If allegedly a government is attacked multiple times a day by state-sponsored actors, how does it know this particular attack is part of a retaliatory strike?[698]

Condition 3: Actor B should design the CVCW in such a way that it does not just have a temporary effect, but that it has the ability to control this effect.

The third condition is that the actor designs the strategic weapon in such a manner that it is able to control the temporal nature of the harmful or damaging effects. Scholars often talk about cyber

[695] Dispersion (the scattering of damage) does not equal collateral damage.
[696] The discussion of loud cyber weapons has primarily been about "possibly deter future intrusions." Yet, it should also be considered in light of mitigating *current* intrusions and conflict. Chris Bing, "U.S. Cyber Command director: We want 'loud,' offensive cyber tools," *FedScoop*, (2016, August 3), Retrieved from: https://www.fedscoop.com/us-cyber-command-offensive-cybersecurity-nsa-august-2016; Herb Lin, "Developing "Loud" Cyber Weapons," *Lawfare*, (2016, September 1), retrieved from: https://www.lawfareblog.com/developing-loud-cyber-weapons; Herb Lin, "Still More on Loud Cyber Weapons," *Lawfare*, (2016, October 19), Retrieved from: https://www.lawfareblog.com/still-more-loud-cyber-weapons; Adam Segal, "Takeaways From a Trip to the National Security Agency," *Council on Foreign Relations: NetPolitics*, (2016, December 21), Retrieved from: https://www.cfr.org/blog-post/takeaways-trip-national-security-agency.
[697] Nick Ismail, "Under attack: the UK exposed to constant hostile cyber threats," *Information Age*, (2017, February 13) Retrieved from: http://www.information-age.com/uk-constant-threats-cyber-attacks-123464417/
[698] For high level counterforce cyber retaliation it might nevertheless be possible, but if they are used on a smaller scale it will be substantially more difficult

weapons' effect being (able to be) only temporal.[699] But a truly intelligent design of a capability goes beyond this and aims to *control* the duration of effect. Control refers to the adversary's inability to stop or revert the effects of the cyber attack, and attackers ability to stop or revert the effects of the attack at any given time desired.

This type of capability design would allow for countervalue cyber weapons to be used in the same way as economic sanctions. The simplest design for this type of capability would probably be large-scale DDoS attack with multiple command-and-control servers (i.e. avoiding a 'hub-and-spoke' design), and a large number of zombie computers (infected with different malware).[700] Another type of design would be a variant of a wiper. The wiper would copy all the relevant data before it executes the disk wiping command. The leverage is that the attacker could give the data back following conflict termination (in the scenario described above). Overall, if the usage of a strategic cyber weapon is discernible and its effects controllable, it can be used as an independent asset - and even allow for the prevention of further conflict and the maintenance of stability in a certain region.

Yet, it also has an advantage compared to economic sanctions. Sanctions are inherently public, which leads to additional reputational costs for the aggressor if it backs down post-action. The value of cyber weapons is that these activities could potentially take place in a covert manner – making it easier for a leader to save face after it backed down. Overall, this leads to a new possibilities of compellence, i.e. to *change* the behaviour of actors.

Ultimately, combining these conditions leads to a dilemma for the use of CVCW. After all, it is difficult to combine the first and last condition. If an effect is created beyond cyberspace, it is hard to reverse this effect at a later point in time. And, the other way around: if the direct effects of an operation do remain within cyberspace, the effects may not be substantial enough to be leveraged against the opponent.

Proposition 3. Cyber weapons can be used to achieve a form of psychological ascendancy

On an afternoon in June 1903, the Italian inventor and electrical engineer Guglielmo Marconi was about to demonstrate how Morse code messages could be wirelessly transmitted over long distances.

[699] According to Gartzke, this dimension of cyber weapons is a key limitation: "Cyberattacks are unlikely to prove particularly potent in grand strategic terms unless they can impose substantial, durable harm on an adversary." The argument here is that it can be turned into a strategic advantage as well. See: Gartzke, "The Myth of Cyberwar," p. 43

[700] The reason an actor would avoid a hub-and-spoke design is because it is easier to take down. Also if you infect the computers with different malware, it means that one software patch will not be adequate to take down the zombie network. The inclusion of the latter dimension has been rare. One other hypothetical option would be to ask/force companies to not provide any security updates and patches. Similarly, internet service provides could be 'asked' to not cooperate with any demands to flip proxy servers controlled by the attacker.

In the lecture theatre of the Royal Academy of Sciences, Marconi's assistant John Ambrose Fleming was waiting to showcase the powerful point-to-point system technology in front of a large audience. Marconi himself was about 300 miles away, preparing to send a signal to London from a clifftop station in Cornwall, UK.[701] Yet, what followed was not in Marconi's playbook:

> Minutes before Fleming was due to receive Marconi's Morse messages from Cornwall, the hush was broken by a rhythmic ticking noise sputtering from the theatre's brass projection lantern, used to display the lecturer's slides. […]. Someone, [Fleming's assistant] Blok reasoned, was beaming powerful wireless pulses into the theatre and they were strong enough to interfere with the projector's electric arc discharge lamp. Mentally decoding the missive, Blok realised it was spelling one facetious word, over and over: "Rats". A glance at the output of the nearby Morse printer confirmed this. The incoming Morse then got more personal, mocking Marconi: "There was a young fellow of Italy, who diddled the public quite prettily," it trilled. Further rude epithets - apposite lines from Shakespeare - followed.[702]

A trick was played by Nevil Maskelyne, a British magician using Morse code for his illusions, enlisted by the Eastern Telegraph Company.[703] Maskelyne's actions highlighted that Marconi's technology was nowhere near as secure as he claimed. After the incident, Marconi did not immediately respond publicly: "I will not demonstrate to any man who throws doubt upon the system".[704] The *New Scientist* writes that, "Fleming, however, fired off a fuming letter to The *Times of London*. He dubbed the hack "scientific hooliganism", and "an outrage against the traditions of the Royal Institution". He asked the newspaper's readers to help him find the culprit."[705]

The century old hack aptly demonstrated a potent ability of cyber weapons today: the ability to humiliate an enemy. The goal of Stuxnet was not to maximize damage, but to humiliate the Iranians.[706] And the worm has done so successfully. Natanz was a hardened Fuel Enrichment Plant (FEP), buried deep underground, seemingly impossible to strike. Some of the country's most renowned scientists and engineered were dismissed as incompetent, unable to explain what was going on with the industrial control systems in Natanz. The malware was only discovered after western

[701] Paul Marks, "Dot-dash-diss: The gentleman hacker's 1903 lulz," *New Scientists*, (2011, December 20), Retrieved from: https://www.newscientist.com/article/mg21228440-700-dot-dash-diss-the-gentleman-hackers-1903-lulz/?full=true
[702] Ibid
[703] Telegraphy companies had invested in a dense network of land and sea cable network. The transatlantic wireless messaging service was a major threat to their competitive position.
[704] Marks, "Dot-dash-diss"
[705] Ibid
[706] As mentioned before, the goal was not so much to slow Iran's ability to produce enriched uranium; it was to mess with Iran's best scientific and military minds. Sanger, *Confront and Conceal*, p. 199

security researchers started to analyse the code - another sign that the Iranians were unable to protect their own, most secretive and prestigious program.

Operation Orchard is one of Israel's military's finest moments. For Syrian President Bashar al-Assad, it was an embarrassing experience. After the attack the Syrian government initially claimed that its anti-aircraft weapons had fired at Israeli fighters, which had bombed an empty area in the desert. Later, Assad insisted during an interview with Der Spiegel at his palace that "[t]he facility that was bombed was not a nuclear plant, but rather a conventional military installation."[707]

These types of cyber-attacks - which could use both CVCW and CFCW - remind us of the psychological effects of some of the special operations Colin Gray describes. For example, "during the war of attrition with Egypt in 1968-70, Israeli commandos attacked one of the 'crown jewels' of the Egyptian economy, the Naj Hamadi transformer station and bride which were 320 kilometres inside Egypt. [It is an example of] a state being revealed as unable to protect its assets."[708] Overall, both special operations and cyber-attacks can "inflict exemplary punishment as well as actual loss."[709]

Many talk about the reputation damage a company suffers after it falls victim of a successful cyber attack. For a major cyber incident - like Target, J.P. Morgan, Ashley Madison, or Sony Pictures Entertainment - a company is said to face significant financial consequences (and management shake-ups). These reputation costs are often much higher than the cost to replace or restore the computer network that was initially damaged by the attack.[710] Though governments might not run a 'reputation risk' when their systems get compromise which is quantifiable in company losses, successful compromise by an adversary can reduce general public trust authority (or factions which are responsible for a specific program) - which in turn can be exploited by other states.

To achieve some form of psychological ascendancy could both be the main purpose or side-effect of using a cyber weapon. Some of the disclosure dynamics and how it can affect audience costs, have already been discussed in section 2 of this chapter. From an attacker's perspective - assuming the defender and/or other third party does not disclose the intrusion - there are three options: i) attack and immediately disclose; ii) attack and conceal, but disclose later; iii) attack and conceal. If an attacker

[707] Der Spiegel, "SPIEGEL Interview with Syrian President Bashar Assad 'Peace without Syria Is Unthinkable'", (2009, January 19), retrieved from: http://www.spiegel.de/international/world/spiegel-interview-with-syrian-president-bashar-assad-peace-without-syria-is-unthinkable-a-602110.html
[708] Gray, *Explorations in Strategy*, p.178
[709] Ibid
[710] While companies normally suffer a drop in stock value directly after the breach, stock prices normally quickly bounce back up. But the company suffers other breach-related costs - also often including law suits.
See: Elena Kyochko and Rajiv Pant, "Why Data Breaches Don't Hurt Stock Prices," *Harvard Business Review*, (2015, March 31), Retrieved from: https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-price

postpones disclosure it can expose the intrusion at a time when the strategic context is more favourable (e.g. when target is particularly exposed to this news - during for example election season - or when distraction of internal problems is convenient). If an attacker never discloses it can enhance credibility and make compellence easier in the future. These options are more likely to exist when countervalue cyber weapons are used.

Proposition 4. Cyber weapons can be used effectively and for strategic gain with few casualties.

In 2015, when India's Prime Minster Narendra Modi launched 'Digital India Week' he stated that "clouds of a bloodless war are hovering" in the world.[711] It was a reference to the global cyber threat which he believed India could play a lead role in countering.

Cyber-attacks so far have indeed not been lethal, but the argument is not that it cannot happen. A civilian can be a direct and indirect target of a cyber-attack. A potential example of a direct attack concerns the alteration of medical devices which could give a deadly shock if hacked. The doctor of former Vice President Dick Cheney ordered the wireless functionally of his heart implant to be disabled due to fears it might be hacked in an assassination attempt.[712] A few years later has proven to be a valid fear following Barnaby Jack's (demonstrated) research on vulnerability in medical devices.[713] More indirect forms of harm can be caused by using a cyber weapon against transportation networks (causing airplane/train crashes) or water and dam facilities (causing pollution or flooding).

Instead, the notion of 'bloodless war' rests on two pillars. The first pillar directly connects to the earlier debate on whether 'cyberwar' makes for a more or less violent world. Tim Maurer concludes "Cyberwarfare might be how we will fight the battles of the future. The evidence so far suggests, however, that a digital Pearl Harbor would cost fewer lives than the attack 70 years ago. It might not be pretty, but from a humanitarian point of view, that's good news." Maurer notes that Stuxnet pushed back Iran's nuclear development without killing anyone. Hence, his argument is that if we use a

[711] PTI, "World facing 'bloodless' cyber war threat: Modi," *The Hindu*, (2016, April 1) retrieved from: http://www.thehindu.com/news/national/world-facing-bloodless-cyber-war-threat-modi/article7375190.ece
[712] Sanjay Gupta, "Dick Cheney's Heart," (2013, October 20), *CBN News*, Retrieved from: http://www.cbsnews.com/news/dick-cheneys-heart/; Andrea Peterson, "Yes, terrorists could have hacked Dick Cheney's heart", *The Washington Post*, (2013, October 21), Retrieved from: https://www.washingtonpost.com/news/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheneys-heart/?utm_term=.ea14d571e5fc
[713] In 2012, Jack demonstrated how a model of an insulin pump could be lethally hacked to administer incorrect dosages from up to almost 100 meters away. In 2013, he hacked into a pacemaker to show he was able to explode it. See William Alexander and Barnaby Jack, "Could Hack Your Pacebmaker and Make your heart explode", *VICE* (2013, June 25), retrieved from: https://www.vice.com/en_se/article/i-worked-out-how-to-remotely-weaponise-a-pacemaker

Stuxnet-like capability more often it would reduce the human costs of war.[714] Similar conceptions are provided by Thomas Rid and John Arquilla.[715]

The other pillar on which the 'bloodless war' conception rests is that of the attacker's casualty sensitivity.[716] Though the literature is divided on whether mounting casualties by themselves drive public attitudes toward conflict and inherently lead to reduced public support, the scholarly consensus is that public attitudes towards war are not indifferent to the human costs of its soldiers.[717] The common conception is that the public makes some kind of 'end-means' calculus about war.[718] A 'cyber warrior' sits far away from the battleground - regardless of whether it is developing a tactical or strategic cyber weapon - and can drive home after a day of work. It is hard to conceive how these individuals can suffer bodily harm during a cyber operation.

Although the 'bloodless war' perception provides a powerful push factor to use a cyber weapon, there is a major caveat with respect to this discussion. The usage of cyber weapons can have the ability to

[714] Maurer considers a scenario in the past in which former Vice President Dick Cheney describes the decision-making process that occurred as the U.S. considered whether or not to bomb a Syrian nuclear facility in 2007. Despite Israeli requests to do so, President George W. Bush decided to pursue a diplomatic rather than military option. So Israel took matters into its own hands. Cheney writes, "[u]nder cover of darkness on September 6, 2007, Israeli F-15s crossed into Syrian airspace and within minutes were over the target at al-Kibar. Satellite photos afterward showed that the Israeli pilots hit their target perfectly." For Maurer, this highlights an important point: "Despite the attack being a perfect hit, a few people were probably still killed." Tim Maurer, "The Case for Cyberwarfare," *Foreign Policy*, (2011, October 19) retrieved from: http://foreignpolicy.com/2011/10/19/the-case-for-cyberwarfare/

[715] Libicki does not buy into the 'peaceful nature thesis' as it only holds in a few (theoretical) scenarios. Libicki does not contest that cyber attacks have the potential to cause less casualties as the alternative is less often chosen than others conceive it to be. The key question here seems to be whether cyber capabilities are used instead of 'war' or instead of 'doing nothing'. Most examples cited by proponents of the 'peaceful nature' argument focus on when a state could have gone to war but used a cyber capability instead. The Iranian attack against Saudi-Aramco and the North Korean attack against Sony may be two cases which follow the reverse pattern; instead of doing nothing, a cyber attack was conducted.

[716] Christopher Gelpi, Peter D. Feaver and Jason Reifler, *Paying the Human Costs of War: American Public Opinion and Casualties in Military Conflicts*, (Princeton: Princeton University Press: 2009)

[717] For an excellent overview see: Christopher Gelpi, Peter D. Feaver, and Jason Reifler, "Success Matters: casualty Sensitivity and the War in Iraq," *International Security*, 30:3 (2005-2006), pp. 7-46; Peter D. Feaver and Christopher Gelpi, *Choosing Your Battles: American Civil-Military Relations and the Use of Force* (Princeton, N.J.: Princeton University Press: 2004).

[718] Several factors are provided in the literature as to what can shape this calculus. Bruce Jentleson's 'pretty prudent' public argument is that tolerance is based on the objective of the military operation. Eric Larson argues that tolerance depends on 'elite consensus' behind the mission. Steven Kull believes that the international support for a mission is the essential factor. And Feaver and Gelpi identify expectation of success as a key factor of explaining public casualty tolerance. See: Bruce Jentleson, "The Pretty Prudent Public: Post-Vietnam American Opinion on the Use of Military Force," *International Studies Quarterly*, 36:1 (1992)49-74; Rebecca L. Britton and Bruce Jentleson, "Still Pretty Prudent," *Journal of Conflict Resolution*, 42:4 (1998) 395-418; Eric Larson, *Casualties and Consensus: The Historical Role of Casualties in Domestic Support for U.S. Military Operations* (Santa Monica, Calif.: RAND: 1996); Steven Kull, "What the Public Knows That Washington Doesn't," *Foreign Policy*, 102 (1995-1996)102-116; Peter Feaver and Christopher Gelpi, "How Many Deaths Are Acceptable? A Surprising Answer," *Washington Post*, (1999, November 7), retrieved from: http://www.washingtonpost.com/wp-srv/WPcap/1999-11/07/061r-110799-idx.html

limit casualties on both sides.[719] Yet, imprudent use can severely increase the undesired impact of these capabilities. As Bellovin, Landau and Lin note, "indiscriminate targeting is not an inherent characteristic of all cyber attacks."[720]

Historically, as I laid out in Chapter 2, there has often been mismatch between the intend and the actual damage caused by the cyber-attack. Bellovin et al. examine the requirements and policy implications of targeted cyber attacks. Their main conclusion is that "precise targeting requires good technical design [and] intelligence [...] of the target's environment".[721] The scholars note that precise intelligence on the configuration of a target machines is especially important when cyber attacks focus on physical assets considering the high risk of collateral damage. Overall, the belief held in many military quarters, is that - with sufficient testing and retesting prior to usage - cyber weapons can achieve a designed effect and minimize damage to entities that should remain unharmed. Yet, it does mean that the costs for developing a cyber weapon - as laid out in Chapter 4 - are substantially higher too.

6.5 Conclusion

The aim of this chapter was to extend the demand-side analysis and evaluate the strategic utility of cyber weapons. I first developed three propositions to assess whether the (potential) possession of cyber weapons can lead to coercive bargaining advantages. I have shown that it is difficult for a state to use its cyber latency as tool for coercion. Similarly, the prospect of a state giving up its cyber arsenal is unlikely to lead to bargaining advantages. Yet, the threat of using a cyber weapon can have strategic effects. Particularly, when the field continues to the develop and states develop a reputation over time, we can expect 'cheap talk' about capabilities to become more effective. Also, I have shown that there are various ways to involve domestic or international audiences to make threat postures more credible and effective.

In the second part of this chapter I examined the usage of cyber weapons, distinguishing between CFCW and CVCW capabilities. I concluded that cyber weapons provide an 'extra option' to leaders, and can lead to strategic advantages under certain circumstances. To be sure, cyber weapons will not displace traditional forms of force at all times. The cases of CFCW and CVCW usage suggest that

719 As Rid writes in the *Rise of the Machines*, Omni was one of the first magazines depicting the changing nature of war in 1979. Talking about the future of cybernetic war, Omni envisioned four features: speed, automation, espionage, and precision. See Rid, *Rise of the Machines*, chapter 7
720 Bellovin, Landau and Lin, "Limiting the Undesired Impact of Cyber Weapons"
721 Ibid, p. 59

they can be used both as an important force-multiplier enabler for conventional military assets or as independent capability. Cyber weapons can also be used to achieve a form of psychological ascendancy and can be used effectively with few casualties.

The focus of this chapter has been on the utility of using cyber weapons, and hence the propositions developed focused on the capability's distinct advantages. It should be clear that there are many things cyber weapons cannot do. For example, special operations can create heroes and raise public morale in this manner. As Gray writes, "[t]he clash of armies and army groups tends to be too vast for it to engage the imagination. The small scale and often heroic deeds of special operations forces bring war to a level to which most people can relate. In both world wars governments and their supportive media sought to raise domestic morale by personalizing the struggle through the promotion of heroes."[722] The 'cyber warrior' is much more anonymous and the way these operations unfold is difficult to relate to for a general audience.

[722] Gray, *Explorations in Strategy*, p. 175

Chapter 7: Conclusion

Why do states develop cyber weapons? Section 7.1 recaps the main arguments and analysis of prior chapters. Section 7.2 will flesh out general implications for both scholars and policymakers and relate the findings to prior research. Finally, the chapter closes by suggesting possible directions for future studies.

7.1 Summary of Findings

In this thesis I have aimed to offer a theoretical and empirical account of what causes the spread and restraint of cyber weapons. Although this research provides insights into several fields of scholarly debate, I hope that the study's findings as a whole are greater than its parts. A central purpose of this exercise has been to open up a new field of research: that of 'cyber proliferation'. I attempted to show that studying the question 'why cyber?' is at least as important as studying the impact of cyber proliferation. It can be said that this study adds a new unique perspective to the general debate on proliferation. Mechanisms which are identified in the nuclear scholarship - or other works on proliferation - cannot be uncritically adopted for cyber proliferation. Each form of proliferation, is worthy of analysis on its own. This especially holds true for cyber proliferation considering the unique mark up of cyberspace, the properties of offensive cyber capabilities, and its consequences for international security dynamics.

The key argument of this research is that the world is not at the brink of mass proliferation. The spread of cyber weapons will be limited in at least two manners. First, the number of states that will require cyber weapons is not and will not be as large as the above statements would suggest. Second, the rate in which these capabilities will spread in the future is not as fast. I have developed this argument in five steps in the body of this study.

To lay the foundation for understanding the requirements for development cyber weapons, I have initially clarified the meaning of the term 'cyber weapon'. The study's extension of Goertz' three-level framework to a four-level framework - i) the base, ii) the qualificatory, iii) secondary, iv) and indicator level allowed for an enhanced understanding of cyber weapons as a multilevel and multidimensional concept. I argued that cyber weapons should be viewed as a type of weapon; it concerns a capability designed to access a computer system or network to damage or harm living or material entities. It has three necessary and sufficient components; a vulnerability, access vector and

payload. Separating these components into various indicators, however, also revealed that it is not always straightforward to empirically distinguish between a cyber weapon and a generic offensive cyber capability. To move from defining a cyber weapon to identifying a cyber weapon can indeed be a laborious process.

States are at different stages of cyber proliferation. And whilst many have commented on the number of states developing offensive cyber capabilities, few have backed this up with any data. In Chapter 3, I have provided a fine-grained analysis of states' exploration, pursuit, and acquisition of cyber weapons. Currently just below forty states are known to be *exploring* the development cyber weapons - a number far lower than many commentators have suggested in the past. It is hardly surprising that the United States, China, and Russia were among the states attentive to the cyber perils relatively early. The data also showed that, even though several other states expressed interest in 'going cyber' in the early 2000s, there is a clear spike in interest after 2008. Introducing a new type of cyber capability analysis, I showed that about a dozen states currently seem to have acquired cyber weapons.

Uncovering the current landscape of cyber proliferation, leads to two essential questions about why states develop cyber weapons: first, are there states which have the potential to develop cyber weapons but are currently not exploring or pursuing these capabilities? And second do all states which are currently exploring or pursuing cyber weapons have the actual capacity to develop them? To address these questions in Chapter 4 I focused on the supply-side of cyber proliferation. The notion underlying the supply-side imperative is that once a state acquires the *latent* capability to develop cyber weapon, it will be compelled to also develop an operational capability and 'go cyber'. In order to elucidate the main obstacles actors have to overcome to develop a cyber weapon, distinguished between various type of cyber capabilities, and deployed a new dataset, *the Offensive Cyber Operations Dataset*, to identify the population of cases. I showed that the barriers to develop unsophisticated cyber weapons are indeed low. These weapons have little material and organizational costs. Being mostly based on 'known-how', the costs of these capabilities are likely to fall in future through learning curve effects like standardization, labour efficiency product redesign, and shared experience effects. The obstacles actors have to overcome to develop sophisticated cyber weapons, however, are shown to be disproportionately higher. In order to gather enough information about an adversary's systems - an activity which often takes place outside cyberspace - direct access to a dedicated intelligence network is required to develop these offensive capabilities. The material demands are also much higher for sophisticated cyber weapons. Not least, the mirroring of an Industrial Control System environment - in order to ensure the effectiveness and precision of a cyber

weapon - is an obstacle even well-funded actors find difficult to overcome. Also, for sophisticated capabilities, intelligence and military organizations have to work closely together while maintaining a high level of secrecy. These types of cyber weapons are also less susceptible to cost reduction effects in the future.

The supply-side covers a valuable piece to the cyber proliferation puzzle; revealing that the gap between technical potential to develop sophisticated cyber weapons and military reality is much smaller than what some scholars conceive it to be. However, an analysis of the demand-side - that is, the motivations underlying states' cyber proliferation - is required too, as there are numerous countries which have the latent capacity to develop cyber capabilities but have not done so.

Chapter 5 deployed three theoretical frameworks in a comparative fashion to assess the demand-side of cyber proliferation. The first framework suggested that the predominant cause for cyber proliferation is perceived insecurity. Though the imperative seems to provide an intuitive explanation for why states develop cyber weapons, I concluded that it does a poor job explaining most variation. At most, it provides a weak incentive for states to proliferate. This weak stimulus seems to be insufficient to push most states over the hurdles of acquiring sophisticated cyber weapons - especially small powers lacking large defence budgets. The domestic politics framework instead posited that cyber proliferation is driven by competing interests and incentives within the state. I distinguished between various actors who might encourage or discourage states from pursuing cyber weapons. Both the intelligence apparatus and military have strong incentives to push for the development of cyber weapons - albeit for different reasons. Although there are reduced incentives for the private sector to drum up demand for offensive cyber capabilities (due to nature of development, current regulation and overall market size), their influence continues to grow. The final framework considered the normative processes underlying cyber proliferation. Cyber weapons are currently not regarded with abhorrence in the same manner as weapons of mass destruction, even though a diverse group of actors have now called for the establishment of new 'cyber norms'. Despite the lack of a cyber taboo, status driven motives are less favourable to explain the variation in cyber weapon development given its element of surprise, limited attributive ability, and immateriality. Overall, I have argued that states are more inclined to poser with a publication of a national cyber security strategy and/or the public establishment of institutions like a cyber command instead of developing *actual* cyber weapons. It may not be 'all mouth and no trousers,' but policymakers and experts often confuse *apparent* proliferation with *actual* proliferation.

The demand-side analysis leads to an important question: if the value of cyber weapons is not 'obviously beneficial' and 'existential', what purpose *do* they serve? Chapter 6 therefore assessed the strategic utility of cyber weapons. The first part assessed whether cyber weapons can lead to coercive bargaining advantages, laying out three propositions. I have shown that it is difficult for a state to use its cyber latency as tool for coercion. Similarly, the prospect of a state giving up its cyber arsenal is unlikely to lead to bargaining advantages. Yet, the threat of using a cyber weapon can have strategic effects. More specifically, when states develop a reputation over time, we can expect 'cheap talk' about capabilities to become more effective. I have also shown that there are various ways to involve domestic or international audiences to make threat postures more credible and effective. The second part of the chapter examined the usage of cyber weapons, distinguishing between CVCW and CFCW capabilities. I concluded that cyber weapons provide an 'extra option' to leaders, and can lead to strategic advantages under certain circumstances. To be sure, cyber weapons will not displace traditional forms of force at all times. The cases of CVCW and CFCW usage suggest that they can be used both as an important force-multiplier for conventional military assets or as independent capability. Cyber weapons can also be used to achieve a form of psychological ascendancy and can be deployed effectively with few casualties.

7.2 Implications for Theory and Practice

These findings have implications for both scholars and policymakers. My research makes it possible to offer some predictions about several trends in cyber proliferation. The number of states exploring and pursuing cyber weapons is likely to grow exponentially in the (near) future. The number of states that will actually acquire cyber weapons is likely to continue to grow too, but at a much more gradual pace (considering the prestige dynamics as discussed in my demand-side analysis). Several major powers - e.g. Germany - which are establishing military cyber capabilities with 100+ million annual budgets and accommodate a large intelligence constituency, are top of the list when it comes to acquiring sophisticated cyber weapons. In the coming years, we may see from smaller powers with a small cyber command - like the Netherlands - the deployment of offensive cyber capabilities.[723] Yet,

[723] An analysis of the meaning of small and middle powers is beyond the scope of this discussion and is highly contested in the literature. The key work to-date looking at these states in relation to offensive cyber capabilities is from Joe Burton. Burton states "[m]oving beyond material definitions of what constitutes 'smallness', the security strategies of small states can be divided into three main conceptual frameworks: i) alliances, ii) institutions, iii) identity and norms." The scholar is unclear about the role of material capabilities in his definition. More generally, a key work on middle powers is from Cooper, Higgott and Nossal. The scholars define middle powers based on their behaviour; that is "their tendency to pursue multilateral solutions to international problems, their tendency to embrace compromise positions in international disputes, and their tendency to embrace notions of 'good citizenship' to guide their diplomacy". A different work from Lee defines middle powers from a network analysis point of view. In turn,

considering the critical role of post hoc-signalling when it comes to offensive cyber capabilities (especially for small and middle powers), as discussed in Chapter 6, we should not be too quick to jump to the conclusion that these states have an 'arsenal' of 'sophisticated' 'cyber warfare' capabilities.

The findings of the supply-side of cyber proliferation add further weight to the argument that the cyber revolution thesis is largely overblown. Cyber weapons to date have not been a weapon for the weak (see Chapter 3), and are unlikely going to be in the future (see Chapter 4). Also, the study's focus on the *obstacles* of capability development instead of the monetary costs provides several additional insights. First, it has provided a more realistic perspective for those states currently aiming to establish an offensive cyber capability on what they can achieve if they develop a capability on their own. It also elucidates how states can obtain a certain type of cyber capabilities. Second, and closely related, focusing on obstacles instead of costs shows that certain actors can *never* develop certain capabilities - no matter how much money they have. How could one keep a project like Stuxnet secret in a small country like the Netherlands which is trying to establish an offensive cyber capability? In fact, how would they be able to secretly obtain those specific centrifuges in the first place? And where would they get all the nuclear scientists from? Replicating the centrifuges in secret is just one example of unquantifiable costs. As I have shown, there are also other obstacles. Sophisticated cyber operations require not just intelligence obtained through previous cyber operations, but also conventional intelligence operations. Human, privileged access to certain air-gapped computer systems might take many years acquire. Also, offensive cyber cooperation between states, generally even more so than conventional operations, relies on a high level of trust. These types of close (intelligence) partnerships are not established overnight. On the whole, putting a price tag on these types of cyber weapons becomes a meaningless exercise. Money can't buy every cyber thing.

Henrikson defines middle powers based on their mediating role in international affairs. Finally, Laohathai uses number of citizens in a country as a sole criteria for being a middle power (i.e. those with more than 10 million people). See: Joe Burton, "Small states and cyber security: the case of New Zealand," *Political Science*, 65(2013)216; Andrew Cooper, Richard A. Higgott, Kim Richard Nossal, *Relocating Middle Powers: Australia and Canada in a Changing World Order*, (Vancouver: University of British Columbia Press: 1993), p. 19; Sook-Jong Lee, "South Korea as New Middle Power Seeking Complex Diplomacy," *EAI Asia Security Initiative Working Paper* (2012, September), retrieved from: https://www.eai.or.kr/data/bbs/kor_report/2012091210545762.pdf; Alan K. Henrikson, "Middle Powers as Managers: International Mediation within, across, and outside Institutions," in Andrew Cooper (ed.), *Niche Diplomacy*, (London: Palgrave Macmillan: 1997) Tanya Laohathai, "Small and Medium-sized states in the age of uncertainty: The art of punching above's weight," *Demos Working Paper*, (2013) retrieved from: http://www.demosservices.home.pl/www/files/Small%20and%20Medium_Tanya%20Laohathai.pdf

7.3 Limitations and Future Research

As the first study on cyber proliferation, this work inherently has its shortcomings. There are a number of ways in which this study has limited its scope and can be extended in the future.

First, the cases discussed in this research have served to shed light on whether certain variables matter in at least certain instances, and uncovered the underlying mechanisms. Future research can extend the cursory qualitative analysis of this thesis by means of process tracing the causal mechanisms of a select number of cases in more detail. This would not only help to generate and refine theories on cyber proliferation behaviour, it will also aid more rigorous testing of potential necessary and sufficient conditions. Furthermore, this study only assessed the three 'classic' frameworks for states' willingness to proliferate, whilst other frameworks remain untested. We would also benefit from an assessment in further studies about the role of other factors - such as psychological factors - in cyber proliferation behaviour.[724]

Second, this study has developed three new datasets (the *Cyber Exploration and Pursuit Dataset*, the *Cyber Threat Actor Dataset*, and the *Offensive Cyber Operations Dataset*). These datasets are the most comprehensive and transparent source of information on the development of cyber weapons that is publicly available. They nonetheless have some key limitations which users of the dataset should be aware. First, the datasets are inherently limited to *observable* incidents. It is likely that many (sophisticated) attacks are currently active or have been active but have not (yet) been discovered or publicly reported. A more general bias is that sophisticated attacks which caused visible harm or damage are likely to be over-represented compared with sophisticated espionage attacks as these are less likely to be discovered (particularly relevant for the *Offensive Cyber Operations Dataset*). Second, certain variables could not be included due to the limited information availability. For example, reports generally do not provide information on the resources/costs required to execute a certain cyber operation (which would benefit the supply-side analysis). In similar vein, no variable was included on financial or other damage caused by the event although it would be useful to include in the dataset (as it is valuable for the strategic utility analysis). Third, as said, the *Cyber Threat Actor* and the *Offensive Cyber Operations* datasets rely on reporting from cybersecurity firms. Despite their increasing prominence cybersecurity firms are often criticized for their biases when identifying cyber threat actors, which inherently introduces several biases.

[724] Jacques E. C. Hymans, *The Psychology of Nuclear Proliferation: Identity, Emotions and Foreign Policy*, (Cambridge: Cambridge University Press: 2006)

Bearing these limitations in mind, future research could compile these datasets (into a new time series cross section dataset) to employ a statistical analysis. After all, we are still at an early stage in assessing how important various variables are relative to another in explaining cyber proliferation. As Philipp Bleek also states "while qualitative analysis can shed light on whether and by what mechanisms different variables matter, it sheds far less light on how much they matter relative to one another. [… Indeed,] precisely where qualitative approaches gain less traction, quantitative analysis gains more. Quantitative approaches are suited for assessing multiple variables that are jointly and probabilistically related to the dynamic under study."[725] The dataset to conduct the quantitative analysis would require additional coding to include all the relevant independent and control variables, in accordance with the framework laid out above. The key stumbling block for this type of study lies in accurately operationalizing certain variables like 'normative restraint' and 'threat environment'. A good starting point for the operationalization and coding of this dataset would be Dong-Joon Jo and Erik Gartzke's study on 'Determinants of Nuclear Weapons Proliferation'.[726] An ordered logistic model would be best suited for this study considering that 'cyber proliferation' is an ordinal dependent variable.

The supply-side analysis has provided a general overview of the obstacles states have to overcome to develop different types of offensive cyber capabilities - and, as I noted above, providing key policy insights too. But the analysis can go even further. In 2006, sixty-one years after the first atomic bomb was dropped on Hiroshima, Robert Harney and his colleagues published *Anatomy of a Project to Produce a First Nuclear Weapon.*[727] They outlined almost 200 tasks required to produce a nuclear weapon. Undertaking a similar exercise to identify the barriers to the development of a cyber weapon may be challenging considering the rapid pace of technological change, but would be a fruitful way to extend my analysis. This would further help military strategists, policymakers and intelligence officials to understand the cost drivers for cyber weapons, and provide a better assessment who can access these capabilities in the future.

[725] Bleek, "Why do States Proliferate?," p. 12
[726] The scholars also distinguish between 'opportunity' and 'willingness' and build upon Sagan three frameworks to assess a state's willingness. This means that many of the independent variables used by Gartzke and Jo can be used for a study on cyber proliferation as well with only modest modification. Dong-Joon Jo and Erik Gartzke, "Determinants of Nuclear Weapons Proliferation." Also see: Sonali Sigh and Christopher Way, "The Correlates of Nuclear Proliferation: a Quantitative Test," *Journal of Conflict Resolution,* 48:6 (2004)859-885; Matthew Kroenig, "Importing the Bomb"
[727] Robert Harney, Gerald Brown, Matthew Carlyle, Eric Skroch, and Kevin Wood, "Anatomy of a Project to Produce a First Nuclear Weapon," *Science and Global Security,* 14(2006)163-182;

Also, the interaction between demand and supply has not been central to my discussion.[728] There are at least three ways in which a state can expand their offensive cyber capacity when demand for cyber weapons increases: i) they can ask for higher budges to develop new in-house capability; ii) they can expand their group of 'suppliers' and go to the private sector; iii) they can persuade other states, close allies to take up a new specialized role. Future research may look into these mechanisms in more detail to show how demand may lead to supply - and vice versa.

The analysis of non-state actors was important in this thesis in so far as it contributed to our understanding of why states develop cyber weapons. It became clear that, non-state actors can influence both the supply-side of cyber proliferation - through the provision or transfer of offensive cyber capabilities - as well as the demand-side - through influencing states' willingness to develop cyber weapons (by means of lobbying, advisory or acting as a securitizing actor). Future research may place this group of actors at the centre of attention and look at (the potential different causal mechanisms of) why certain non-state actors seek to develop cyber weapons.

Finally, the focus of this research has been on *horizontal* proliferation, that is the acquisition of weapons by actors that did not previously have them. Yet, *vertical* proliferation also deserves a more rigorous analysis.[729] A narrow understanding of vertical proliferation focuses on the mere build-up of capabilities. In the nuclear context, numerous info graphs portray the stacking of nuclear warheads during the Cold War. In the case of cyber operations, the most analogous is probably the hoarding of zero-days. In broader terms, vertical proliferation can be viewed as an overall improvement of force structure of a state.[730] For offensive cyber capabilities, one can think of improving and diversifying the suite of platforms.[731]

---

[728] As Sagan notes, also more interdisciplinary work is required on how nuclear supply and nuclear demand influence each other. See: Sagan, "The Causes of Nuclear Weapons Proliferation," p. 240

[729] After all, one of the most important findings from the Snowden and Shadowbrokers leaks is that it revealed the depth of NSA (and CIA)'s cyber operations and the range of toolsets available. And also other actors continue to build up their capabilities. Sources close to the Russian Ministry of Defense have revealed that Russia is investing in the range of US$ 200 million to US$ 250 million per year in offensive cyber operations. Although the estimates vary widely on the workforce the Chinese government currently deploys, there are also no signs that China is slowing down on its cyber capability development. A report from McAfee suggests that China is conducting less unsophisticated espionage operations. Yet, there is no sign that china has become less interested in the development of cyber weapons. See: Eugene Gerden, "Russia to spend $250m strengthening cyber-offensive capabilities," *SC Magazine UK*, (2016, February 4), retrieved from: http://www.scmagazineuk.com/russia-to-spend-250m-strengthening-cyber-offensive-capabilities/article/470733

[730] Erik Gartzke, Jeffrey M. Kaplow, Rupal N. Mehta, "The Determinants of Nuclear Force Structure*," Journal of Conflict Resolution*, 58:3 (2014)481-508;

[731] In the nuclear case it is not merely about the increase in number of warheads, but also the quality and diversification of delivery platforms. For cyber, we can think about Equation group's toolbox including EquationLaser, EquationDrug, and GrayFish. Zetter, "Suite of Sophisticated Nation-State attack tools found with connection to Stuxnet,"; Kaspersky Lab, "Equation"

Rational-choice theory finds it famously difficult to explain the vertical nuclear proliferation behaviour of states since 1968. As Feaver notes, "the strategic arms race *after* both the United States and the Soviet Union secured second-strike capabilities[..] is a mystery to nuclear optimists. Perhaps it was bureaucratic imperatives run amok, perhaps it was madness, perhaps it was foolishness. In any case, Waltz avers, it was 'pointless'. Whatever it was, it certainly cannot be explained by Waltz's theory which has states recognizing the futility of war and the abundance of security at extraordinarily *low levels of nuclear capability."*[732] Indeed, after having obtained a second-strike capability, ensuring the deterrent effect, the rational incentives for an actor to add to its nuclear stockpiling are gone. Only bureaucratic politics, irrationality, or profligacy can explain further build up straining economic sources.

An important question for future research is to address the drivers (and barriers) of vertical cyber proliferation. In other words, is there a similar theoretical 'tipping point' in the build-up of offensive cyber capabilities when a further build up is irrational?

There are three key aspects which seem to suggest that this 'tipping point' for offensive cyber capabilities does not exist, meaning there is always an incentive to add offensive cyber capabilities. First, unlike nuclear weapons, the mutual build-up of cyber weapons does not lead to an inherent situation of MAD. As has been noted before, cyber deterrence is inherently difficult to achieve. Second, I have argued earlier that, unlike conventional weapons, cyber weapons are transitory in nature. Hence, to have an assembly line of cyber weapon production running like a clockwork - ensuring a cycle that, when one cyber weapon becomes ineffective, the next weapon can be put to use if necessary - it makes sense to keep developing capabilities.[733] Third, increased diversification of a state's cyber capabilities ensures that it is less perceptible to arsenal fluctuations.[734]Cyber weapons are generally part of a larger collection of capabilities - sharing vulnerability exploits, propagation techniques and/or other features. Stuxnet's "father", for example, is supposed to be USB worm Fanny and has also been linked to espionage platforms Duqu, Flame, Gauss, and Duqu 2.0.[735] Using a capability which is likely to be discovered early - i.e. a cyber weapon causing visible harm or damage - runs the risk that other capabilities are soon exposed as well; not least because cyber security firms are establishing special detection tools in attempt to uncover the cluster of

[732] Peter D. Feaver, "Optimists, Pessimists, and Theories of Nuclear Proliferation Management: Debate," *Security Studies*, 4:4 (1995)754-772, p. 756
[733] Smeets, "A Matter of Time"
[734] Smeets, "Organisational Integration of Offensive Cyber Capabilities"
[735] Boldizsár Bencsáth, "Duqu, Flame, Gauss: Followers of Stuxnet," *Presented at RSA Conference Europe*, (2012), retrieved from: http://www.rsaconference.com/writable/presentations/file_upload/br-208_bencsath.pdf

capabilities.[736] Hence, vertical proliferation by means of diversifying platforms allows a state to not put all its eggs in one basket, making a cyber program more reliable.

The key dimension which matters from this perspective concerns the obstacles states have to overcome to develop cyber weapons (see Chapter 3). Figures 7.1 and 7.2 provide a comparative analysis of the cost-security relationship for nuclear and cyber capabilities.[737] Figure 7.1 depicts the relationship between costs and security for vertical nuclear proliferation. Area 'A' highlights that the initial build-up can be rationalized given the marginal increase in security (if a state can bear the general costs of development). Area 'B' illustrates the period in which a state obtains a second-strike capability. Considering there is no clear cut-off point in practice when a state exactly obtains a second-strike capability, further build up continues to make sense for a short period of time in order to reduce uncertainty (for all actors involved). Area 'C' shows the area in which further build up does not lead to more security. From this point onwards, the marginal return will be negative - even if nuclear weapons would be very inexpensive.[738]

Figure 7.2 depicts the cost-security relationship for vertical cyber proliferation. For any curve, A-E, there is no clear cut-off point as to when further build up no longer leads to a marginal increase in security. Meaning costs play a critical role in determining which curve most accurately represents the situation (In Chapter 3 I have also discussed what possibly affects the cost reduction curve of cyber weapons.)

Figure 7.1: Cost-Security relationship Vertical Nuclear Proliferation

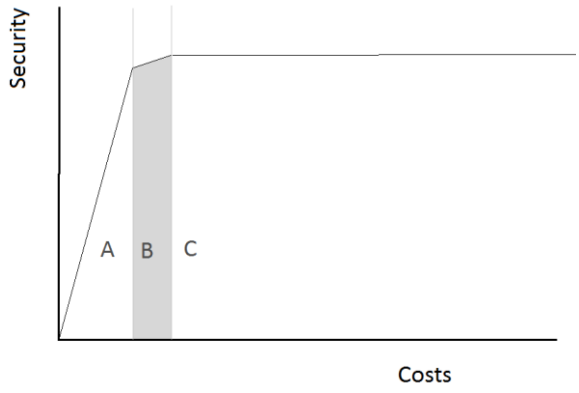
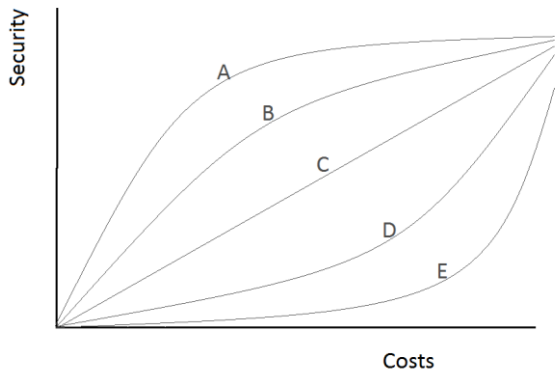


Figure 7.2: Cost-Security relationship Vertical Cyber Proliferation



[736] In the case of Fanny and Stuxnet see: Kaspersky, "A Fanny Equation"
[737] I use the word 'costs' here for simplicity, even though I have earlier discussed the problems with using this terminology. More accurately, we would talk about the marginal increase in 'effort' to develop these capabilities.
[738] The costs of nuclear capability development therefore only matters for Area A and B.

There are two principal factors which complicate the dynamic depicted in figure 7.2. First, the dynamic is complicated by the amount of overlap between the zero-day vulnerabilities or exploits one state holds and those its adversaries are stockpiling. If both sides would have exactly the same stockpiles, the basic principle would be that unilateral disarmament (i.e. disclosure and patching of the vulnerabilities) leads to mutual disarmament.[739] Studies on zero-day overlap have so far provided conflicting results, with estimates ranging between 5% and 20%.[740] A second aspect which affects the decision making of capability stockpiling is that it potentially affects the cyber security of its systems and people. The basic argument is that if a government actors discovers a vulnerability and discloses it to the vendor a system can be patched, creating more secure systems. In turn, a state decides to not disclose the vulnerability it risks other actors exploiting the same vulnerability in the future.[741]

These general dynamics deserve further scrutiny in future studies.[742] Not least because they also have significant implications for arms control. As the incentives for nuclear build-up erode once a state obtains a second-strike capability, it opens up opportunities for arms-control initiatives - even unilaterally. The 2010 US-Russia Strategic Arms Reduction Treaty (START) between the U.S. and Russia, mandating further reductions of the countries' warhead deployments to 1550 (down from 6000 warheads when START I was signed in 1991), can be seen as an outgrowth of the dynamic laid out above. Further across-the-board cuts to delivery platforms are a realistic prospect as it does not

[739] As Joseph Nye Jr. states, "if the United States unilaterally adopted a norm of responsible disclosure of zero-days to companies and the public after a limited period, it would destroy their value as weapons - simultaneously disarming ourselves, other countries and criminals without ever having to negotiate a treaty or worry about verification. Other states might follow suit. In some aspects, cyber arms control could turn out to be easier than nuclear arms control. Cited in: Healey, "Feds and 0Days: From Before Heartbleed to After FBI-Apple"; Joseph Nye Jr., "The world needs new norms on cyber warfare," *Washington Post*, (2015, October 1), retrieved from: https://www.washingtonpost.com/opinions/the-world-needs-an-arms-control-treaty-for-cybersecurity/2015/10/01/20c3e970-66dd-11e5-9223-70cb36460919_story.html?utm_term=.706e47420fde

[740] According to the RAND paper, "[f]or a given stockpile of zero-day vulnerabilities, after a year, approximately 5.7 percent have been discovered by an outside entity." Yet, Herr, Schneier and Morris come to a different conclusion: "15% to 20% of vulnerabilities are discovered independently at least twice within a year." Lillian Ablon and Timothy Bogart, "Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits," *RAND Corporation,* (2017), retrieved from: https://www.rand.org/pubs/research_reports/RR1751.html, p.x; Trey Herr, Bruce Schneier and Christopher Morris, "Taking Stock: Estimating Vulnerability Rediscovery," (2017, March 7), retrieved from: http://papers.ssrn.co/sol3/papers.cfm?abstract_id=2928758;

[741] According to Healey's study, the United States retains only less than 10% of the vulnerabilities. The number of vulnerabilities the U.S. retains today is likely single digits (instead of hundreds or thousands). Healey, "Feds and 0Days: From Before Heartbleed to After FBI-Apple"

[742] This dynamic also becomes more important once more states have fully operationalized their cyber command.

put second-strike capabilities in danger.[743] Overall, this suggests that we should be less optimistic about the potential for a 'cyber arms treaty'.

[743] William T. Tow, "The Nuclear Waltz: Rational actors, deterrence and nuclear non-proliferation", *Australian Journal of Political Science*, 49:3 (2014)541-546; Kenneth Waltz, "Nuclear myths and political realities," *American Political Science Review*, 84, (1990)731-45.

Appendix 1: The Offensive Cyber Operations Dataset: Codebook

1.1 Overview

The *Cyber Operations Dataset* provides information on the main cyber operations which have occurred since the Cuckoo's Egg and the Morris Worm in the late 1980s and ends in July 2016. It includes details about 256 offensive cyber operations. The most essential aspects of the dataset are described in the *Chapter 1: Introduction* and *Chapter 4: The Supply-Side of Cyber Proliferation*. The purpose of this codebook is to help readers interpret the data contained in the file "Going_Cyber_Data_Smeets.xls" and further clarify some of the inherent limitations.

The aim of this dataset is to serve as a heuristic device to better capture in which cyber operations an actual cyber weapon was used. As such, it will allow scholars to better contextualize the sophistication of these weapons relative to other capabilities, such as espionage operations.

The dataset is easy to update if researchers wish to do so in the future. Researchers can also add variables or construct alternative measures for indicators in order to fit their research objectives.

1.2 Description

This dataset includes all cases on which an incident report was written by a reputable cyber security firm in English. The reports of the following firms are included in the dataset:

- Kaspersky / Securelist
- McAfee
- Symantec
- SANS Institute
- FireEye / Mandiant / iSIGHT Partners
- Crowdstrike
- TrendMicro
- IBM
- Cisco
- Dell / SecureWorks
- F-Secure
- Arbor
- Sophos
- Fox-IT
- Cyclance

The unit of observation in the dataset is 'Offensive Cyber Operation'. An offensive cyber operation concerns an activity in which an actor or group deploys a capability designed to access a computer system or network to achieve a certain purpose. This definition includes a wide range of activities ranging from cyber hacktivism to sophisticated cyber-attacks with as aim to cause significant harm or damage.[744]

A number of other cases - mentioned in the media or other reports - are excluded in this analysis. There are various reasons why I have followed these strict selection criteria. First, as several scholars have indicated, media reporters and policy makers have a tendency to exaggerate the sophistication (or destruction) of attacks.[745] If I would code sophistication based on these threat representations I would inherently introduce a bias into the dataset. As cyber security firms provide a technical report on the attacks, it allows me to better discern which attacks are (un)sophisticated.[746] Second, there are several controversial cases about which there is uncertainty whether the damage was caused by means of kinetic reaction rather than alternating computer code - for example the 'original logic bomb' in 1982 or the blast of the Baku-Tbilisi-Ceyhan pipeline in 2008. Selection on cases described by cyber security firms ensures that only 'real' cyber event are listed in the dataset.

Several prominent cases which are mentioned in the media but of which no public cyber security report exists include:

- The 'original logic bomb'
- The Baku-Tbilisi-Ceyhan pipeline
- Sands Casino attacks
- Navy Marine Corps Intranet (NMCI)
- LinkedIn Espionage Operations
- Hacking Scientology
- OpBlackSummer
- Canadian government hacking
- Citigroup attack
- New York Dam
- OP Armageddon

Finally, notice that 'year of disclosure' was used instead of date of exploit because it is often unclear when the system was initially compromised - especially for advanced attacks.

[744] In other words, it does not only collect data on when a cyber weapon is deployed.
[745] See for example: Bendrath, "The cyberwar debate"
[746] Similar biases may exist for attribution. It frequently happens that a technical report indicates does make a clear attribution statement, yet this nuance is lost when looking at media reports.

1.3 Variables

For each offensive cyber operation, I created the following variables:

- CYBER_OPERATION_NAME:
  - A descriptive variable: The variable denotes the name of the cyber operation.

- CYBER_ OPERATION _ABBR:
  - A descriptive variable: The variable denotes the abbreviated name of the cyber operation

- ALTERNATIVE_CYBER_NAME:
  - A descriptive variable: The variable denotes the alternative name of the cyber operation.

- SOURCE_OF_DISCLOSURE
  - A descriptive variable: The variable denotes the source of incident disclosure

- YEAR_OF_DISCLOSURE:
  - A time variable: The variable denotes the year the cyber operation was disclosed to the public

- DATE_OF_DISCLOSURE:
  - A time variable: the year and month the cyber operation was disclosed to the public

- THREAT_ACTOR
  - A descriptive variable: the variable denotes the name of the threat actor conducting the cyber operations

- THREAT_ACTOR_ALT
  - A descriptive variable: the variable denotes the possible alternative name(s) of the threat actor conducting the cyber operations

- CYBER_OPERATION_CATEGORY:
  - A binary variable: The variable denotes whether a cyber weapon was used during the operation. A cyber weapon is defined as a capability designed to access a computer system or network to damage or harm living or material entities.
  - 0: not a cyber weapon
  - 1: a cyber weapon
  - 2: Unknown

- NUMBER_OF_TARGETS
  - A categorical variable
  - 0: targeted attack: i.e. the attacker focuses on a specific company, governmental organization, or individual
  - 1: semi targeted attack; i.e. the attacker focuses on companies in one sector, various governm1ental organization of one country, or actors part of one entity.

- 2: untargeted attack; i.e. the attacker does not focus on a specific entity or group of entities.
- 3: unknown

- LEVEL_OF_SOPHISTICATION
  - An ordinal variable: Sophistication refers to the level of expertise and resources required to develop the capability in order to allow for the opportunity to obtain the objective.[747]
  - -3: highly unsophisticated
  - -2: unsophisticated
  - -1: moderately unsophisticated
  - 0: intermediate
  - 1: moderately sophisticated
  - 2: sophisticated
  - 3: highly sophisticated
  - 4: Unknown

- LEVEL_OF_SOPHISTICATION
  - A continuous variable: same definition as above, ranging from -3 to 3

1.4 Limitations

Even though this dataset is the most rigorous source of information on offensive cyber operations, there are several inherent limitations should be highlighted. First, the dataset is inherently limited to *observable* incidents. It is likely that many (sophisticated) attacks are currently active or have been active which have not (yet) been discovered. A more general bias is that attacks which caused visible harm or damage are likely to be over-represented compared to espionage attacks as these are less likely to be discovered.

Second, certain variables could not be included due to the limited information availability. For example, reports generally do not provide information on the resources/costs required to execute a certain cyber operation. Similarly, although it would be useful to include in the dataset, no variable was included on quantifying the amount of damage caused by the event.

Also, as said, the dataset relies on reports from cyber security firms.[748] Despite their increasing prominence cyber security firms are often criticized for their biases when identifying cyber threat actors. Three critiques stand out. First, most cyber security fail to discover/disclose threats from Western nations. Second, these firms have an incentive to exaggerate the cyber threat. If a firm is able

[747] Notice that "0" is not the average cyber incident since the majority of incidents are highly unsophisticated.
[748] Also, it may be that, to the best of their abilities, highly sophisticated actors exists which have so far remained under the radar of cyber security firms.

to discover a highly advanced threat, it creates the perception that it has advanced detection capabilities and you should buy their product. Third, like palaeontologists or astronomers, cyber security firms like to name their new discoveries which may cause a host of problems that confuses accurate data collection and determining whether a threat group still constitutes a threat.[749]

[749] For more extensive discussion on this topic see: Smeets, "When Naming Cyber Threat Actors Does More Harm Than Good"

Appendix 2: The Cyber Threat Actor Dataset: Codebook

2.1 Overview

The Cyber Threat Actor Dataset provides information on the acquisition of cyber weapon by states from the late 1980s until January 2017. It includes data on a wide range of threat actors and their relationship to a certain state. The relationship between this dataset and the 'cyber exploration and pursuit dataset' are discussed in the Chapter 1. Combined, both datasets aim to provide an overview of cyber proliferation across the world. This codebook alsohelps readers interpret the 'offensive cyber capabilities' figures, the data provided in the file "Going_Cyber_Data_Smeets.xls." as well as lay out several caveats.

2.2 Description

Table A2.1 serves to provide a general overview of the data collection and analysis phases related to this dataset. I will discuss each step in more detail below.

Table A2.1: Data Collection and Analysis Cyber Exploration and Pursuit

Steps	Activity
Step 0	Cyber threat actors (set Unit of Observation)
Step 1	Collection of information on all cyber threat actors on which a cyber security firm has written a threat report (Selection Criteria)
Step 3	Assessment of the of threat actor's 'country of origin'
Step 4	Assessment of the threat actor's relationship with the state
Step 5	Assessment of the 'attribution certainty' of actor
Step 6	Creation of 'offensive cyber capability' figure for each state
Step 7	Aggregating findings to estimate initial moment of cyber weapon acquisition
Step 8	Cross verifying findings based on other available information.

Step 0: Unit of Observation.

This dataset aims to collect information on all actors which have conducted cyber attacks. This includes both state and non-state actors, as well as both APTs and non-APTs.

Step 1: Selection Criteria: Collection of information on all cyber threat actors on which a cyber security firm has written a threat report.

Similar to the *Offensive Cyber Operations Dataset*, I include all actors about which one of the following cyber security firms has written a report (in English):

- Kaspersky Lab / Securelist
- McAfee
- Symantec
- SANS Institute
- FireEye / Mandiant / iSIGHT Partners
- Crowdstrike
- TrendMicro
- IBM
- Cisco
- Dell / SecureWorks
- F-Secure
- Arbor
- Sophos
- Fox-IT
- Cyclance

Cyber security firms do not always attribute an offensive cyber operation to a threat actor/group. This includes the following cases:

- WANK worm
- Ghost RAT
- Nimda attacks
- Safe
- Four Element Sword
- INOCNATION
- Poisoned Helmand
- Sin Digoo attack
- Sadmind worm
- RSA Security ID
- Canadian government hacking
- Navy Marine Corps Intranet
- LinkedIn espionage operations
- Madi
- Fin 4
- Strano Network sit-in
- Paypal attack
- Code Red I
- Code Red II
- Kyrgystan DdoS
- Georgian Cyber Attacks
- Estonian Attacks
- RUAG Espionage
- Cloud Atlas
- Red october
- Groundbait
- Tropic Trooper
- The Bagle Botnet
- Epsilon
- Mac OS X: Flashfake attacks
- Playstation attack
- SQL slammer worm
- Operation Potao Express
- Witty
- XDown
- Shylock
- German Steelworks Facility Attack
- Citigroup
- The Conflicker attacks
- IronGate
- Inception
- Project Sauron
- Wiper

Step 2: Assessment the country of origin of the threat actor

I subsequently assess the attackers relationship to the state.[750] Lin distinguishes between attributing malicious cyber activity to; a machine, a specific human being pressing the keys that initiate the activity, and an ultimately responsible party.[751] For this research the last type of attribution is most relevant - though the meanings are not mutually exclusive and interact.

Cyber security firms have identified various cyber threat actors of which we do not know country of origin. These concern:

- Andromeda Spider
- Bestamin
- Blue Termite
- CyberCaliphate
- Dextorous Spider
- El Machete
- Evanescent Bat
- EvilPost
- FruityArmor
- Ghoul
- Magnetic Spider
- Matsnu gang
- Singing Spider
- Slayer Kitten
- Team Sploit
- The Mask
- The Poetry Group
- Transparent Tribe
- TwoForOne
- Union Spider
- Group 27

Step 3: Assess the threat actor's relationship with the state

States often use cyber proxies to conduct offensive cyber operations, here understood as non-state actors used by a state actor to conduct offensive cyber operations. Jason Healey has developed a spectrum assigning ten categories of state responsibility for a particular attack.[752] For the purposes of this study, I simplify Healey's spectrum, and assess the relationship to the government for each actor. I distinguish between four categories: state-free, ii) state-encouraged; iii) state-sponsored; and iv) and state-conducted. Table A2.2 shows how each category aligns to Healey's earlier spectrum.

[750] A threat actor may occasionally have not one principal relationship with a state but multiple. I have coded this case for the multiple countries if that's the case.
[751] Herbert Lin, "Attribution of Malicious Cyber Incidents: From Soup to Nuts", *Aegis Paper Series on National Security, Technology, and Law*, (2016, September 2) Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2835719
[752] The framework has been subsequently adopted and extended in Maurer. Jason Healey, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks," *Atlantic Council:* Cyber Statecraft Initiative, Issue Brief (2011), retrieved from: http://www.atlanticcouncil.org/publications/issue-briefs/beyond-attribution-seeking-national-responsibility-in-cyberspace; Maurer, "'Proxies' and Cyberspace"

Table A2.2: Spectrum of State Responsibility Conducting Offensive Cyber Operations

Spectrum	**Healey's spectrum**	**Definition**
State-free	State-prohibited	The national government will help stop the third-party attack.
	State-prohibited-but-inadequate	The national government is cooperative but unable to stop the third-party attack.
	State-ignored.	The national government knows about the third-party attacks but is unwilling to take any official action.
State-encouraged	State-encouraged	Third parties control and conduct the attack, but the national government encourages them as a matter of policy.
State-sponsored	State-shaped.	Third parties control and conduct the attack, but the state provides some support.
	State-coordinated	The national government coordinates third-party attackers such as by "suggesting" operational details.
	State-ordered	The national government directs third-party proxies to conduct the attack on its behalf.
	State-rogue-conducted	Out-of-control elements of cyber forces of the national government conduct the attack.
State	State-executed.	The national government conducts the attack using cyber forces under their direct control.
	State-integrated.	The national government attacks using integrated third-party proxies and government cyber forces.

Step 4: Assess the 'attribution certainty' of actor

I subsequently assess the level of uncertainty for attributing an offensive cyber operation to a certain actor. Attribution is notoriously difficult – though not impossible - when it comes to cyber attacks. As Thomas Rid and Ben Buchanan indicate, the quality of attribution relies on bringing together technical, operational, and strategic markers.[753] In many cases, we only have circumstantial evidence about the threat actor - such as language artefacts.[754] In some cases, however, there is much more public information available due to mistakes made by the attacker, intensive malware analysis or the leakage of classified documents. The aim is to capture this variation in attribution (un)certainty, as it helps to better understand the likelihood a state acquired cyber weapons.

Step 5: Create 'offensive cyber capability' figure for each state

Following the above steps provides the opportunity to create an 'offensive cyber capacity' figure for each state (see figure A2.1). The level of sophistication of a cyber threat actor in this type of figure is

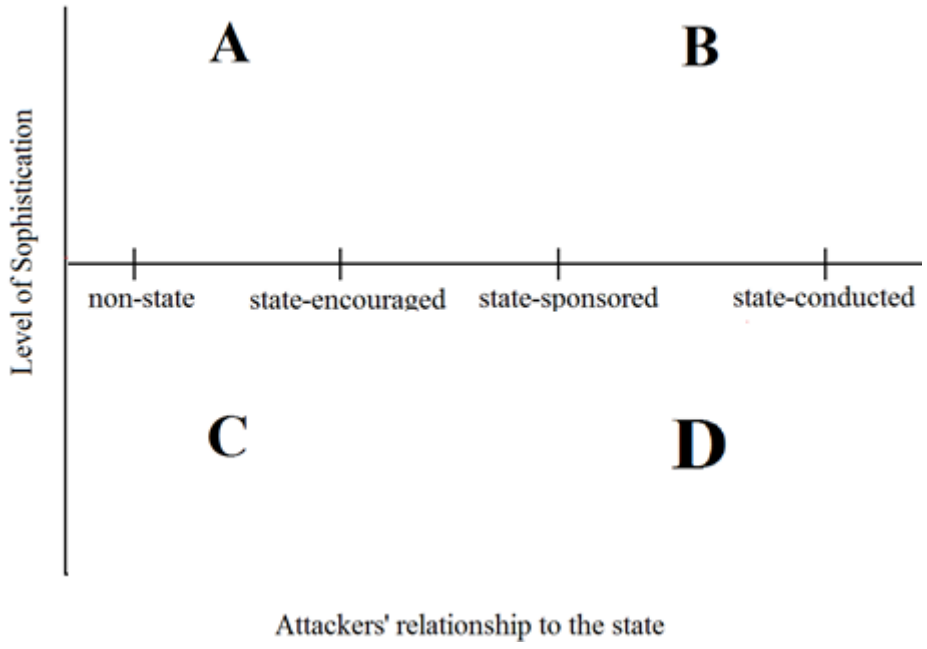
[753] Rid and Buchanan, "Attributing Cyber Attacks"
[754] But these may also be 'red herrings'. For an excellent case study see 'Inception'(also called 'Cloud Atlas').

provided on the y-axis, and the attackers' relationship with the state on the x-axis.[755] The cases above the x-axis are considered to be APTs. The length of the error bars indicates the attribution uncertainty of each actor. If the error bar is short we have a relative high degree of attribution certainty.

The figures provide a plain overview of the type of offensive cyber capacity a country relies on. If most actor groups in the 'offensive capacity figure' are shown in:

- Quadrant A: it suggests that cyber attacks within a state are primarily conducted by non-state actors with a high level of sophistication
- Quadrant B: it suggests that most cyber attacks within a state are conducted by government actors conducting highly sophisticated cyber attacks
- Quadrant C: it suggests that cyber attacks within a state are mostly conducted by non-state actors with low sophistication
- Quadrant D: it suggests that cyber attacks within a state are mostly conducted by government actors with low sophistication

Figure A2.1: Overview 'Offensive Cyber Capacity'



[755] The variable 'Actor's sophistication' is based on the most sophisticated operation by the threat group (not average sophistication).

Step 6: Aggregate findings to estimate initial moment of cyber weapon acquisition.
I subsequently aggregate these individual overviews of states to estimate the initial moment of cyber weapon acquisition by a state. This information is coded in (monad) year format.

Step 7: Cross verify findings based on other available information.
The above data collection efforts allow for a rigorous assessment of those states which already have conducted cyber attacks - and hence we know they have likely acquired cyber weapons. Yet, it may also be that a state has the capability but has not used it to date. I therefore aim to collect any additional information available on each state to cross verify my earlier findings and/or potentially provide new insights on states' capability.

2.3 Variables

2.3.1 Variables for 'offensive cyber capability' overview (see step 1-5)

- CYBER_THREAT_ACTOR__NAME:
  - A descriptive variable
  - The variable denotes the name of the cyber threat actor.

- CYBER_THREAT_ACTOR_ABBR:
  - A descriptive variable
  - The variable denotes the abbreviated name of the cyber threat actor

- ALTERNATIVE_CYBER__THREAT_ACTOR_NAME:
  - A descriptive variable
  - The variable denotes the alternative name of the cyber threat actor.

- THREAT_ORIGIN
  - A descriptive variable
  - The (principal) country which the threat actor is based.

- THREAT_REGION:
  - A categorical variable
  - The variable denotes the continent the threat actor is based.
    - 0: Middle-East
    - 1: Africa
    - 2: Asia
    - 3: Latin-America
    - 4: U.S. & Canada
    - 5: Europe
    - 6: Asia-Pacific
    - 7: Multi-regional
    - 8: unknown

- THREAT_STATE_LINK
    - An ordinal variable
    - The variable denotes the (average) relationship between the attacker and the state.
        - 0: There is no link between the attacker and the state
        - 1: There is a weak link between the attacker and the state: i.e. state-encouraged
        - 2: There is a strong link between the attacker and the state; i.e. state-sponsored
        - 3: A government entity itself is behind the attack
        - 4: Unknown

- ATTRIBUTION_CERTAINTY
    - An ordinal variable
    - The variable denotes the level of attribution information available about the threat actor.
        - 0: There is complete uncertainty about the threat actor
        - 1: There is a low level of certainty about the threat actor
        - 2: There is a moderate level of certainty about the threat actor
        - 3: There is a high level of certainty about the threat actor

- LEVEL_OF_SOPHISTICATION
    - An ordinal variable:
    - The variable denotes the threat actor's ability to conduct sophisticated cyber operations.
    - Sophistication refers to the level of expertise and resources required to develop the capability in order to allow for the opportunity to obtain the objective.
        - -3: highly unsophisticated
        - -2: unsophisticated
        - -1: moderately unsophisticated
        - 0: intermediate
        - 1: moderately sophisticated
        - 2: sophisticated
        - 3: highly sophisticated
        - 4: Unknown
- LEVEL_OF_SOPHISTICATION
    - An ordinal variable:
    - The variable denotes the threat actor's ability to conduct sophisticated cyber operations.
    - Sophistication refers to the level of expertise and resources required to develop the capability in order to allow for the opportunity to obtain the objective.
        - -3: highly unsophisticated
        - -2: unsophisticated
        - -1: moderately unsophisticated
        - 0: intermediate
        - 1: moderately sophisticated
        - 2: sophisticated
        - 3: highly sophisticated
        - 4: Unknown

2.3.2 Variables for general overview (see step 6-7)

- STATE_NAME
    - A descriptive variable
    - Name of the country

- STATE_ABB:
    - A descriptive variable
    - The three-letter abbreviation of the country name

- STATE_CODE:
    - A descriptive variable
    - The Correlates of War country code

- STATE_YEAR_ACQUISITION:
    - A time variable
    - The variable denotes the first year a country acquired a cyber weapon.

- STATE_ACQUISITION_SOPHISTICATION:
    - An ordinal variables
    - The variable denotes a country's ability to conduct sophisticated cyber attacks
    - 0: No capacity
    - 1: unsophisticated
    - 2: moderately sophisticated
    - 3: sophisticated

2.4 Limitations

The cyber acquisition dataset is the most comprehensive and transparent source for information on the acquisition of offensive cyber capabilities that is publicly available. It nonetheless has some key limitations of which users of the dataset should be aware. The following challenges I faced in constructing the dataset warrant discussion.

Not least, there are two underlying premises and potential caveats following this approach which should be addressed.[756] First, I collected data on those actors which have conducted offensive cyber operations, this includes - but is not limited to - the use of cyber weapons. Considering that it is relatively easy to move from espionage to destructive capacity (see Chapter 2), I assume that those states which have developed sophisticated espionage capability also possess a cyber weapon capability. This does not necessarily have to be the case.

[756] Other caveats of the Cyber Incident Dataset are discussed in Appendix 2.

Second, I assume that those states which have used a cyber weapon also currently possess a cyber weapon - unless evidence suggests otherwise. Given the transitory nature of cyber weapons, however, there is the potential that a state may have once possessed cyber capabilities but has 'lost' it.[757]

Third, similar to the *cyber operations dataset*, also this data collection effort relies on the reporting from cyber security companies. This means that the same biases are introduced in this dataset as well.

[757]Smeets, "A Matter of Time"

Appendix 3: The Cyber Exploration and Pursuit Dataset: Codebook

3.1 Overview

The cyber exploration and pursuit dataset is to provide more information on the *Cyber Exploration and Pursuit Dataset*. The dataset starts in 1980 and ends on January 1, 2017. The unit of analysis is monad (country) year. The data can be found in the file "Going_Cyber_Data_Smeets.xls."

In this research, I distinguish between four stages of cyber proliferation: i) no discernible activity, ii) exploration, iii) pursuit and iv) acquisition. This dataset aims to provide a better understanding of the first three stages of cyber proliferation.

I distinguish in between four stages of cyber proliferation: i) no discernible activity, ii) exploration, iii) pursuit and iv) acquisition. Section 3.2 of the codebook discusses the coding procedures related to the earliest three stages of proliferation. In turn, section 3.3 lays out the coding procedures related to the acquisition and use of cyber weapons. In the final section I discuss the codebook's limitations.

3.2 Description

There have been previous data gathering efforts on states offensive cyber activity. Two excellent initiatives stand out in this respect. First, in 2013, the United Nations Institute for Disarmament Research (UNIDIR) has conducted a general study on cyber security trends. [758] As part of this study James Lewis has provided an overview of states with military doctrine, policies, or organizations on 'cyberwarfare'. [759] Another comprehensive study is from the Wall Street Journal from 2015 "cataloging the World's cyberforces"[760]

T

[758] United Nations Institute for Disarmament Research (UNIDIR), "The Cyber Index International Security Trends and Realities"

[759] The general conclusions from Lewis are as follows: "41 states now have publicly acknowledged some military planning or specific military organizations for cyber activities. It appears that states are in a period of experimentation as they assess the risks and benefits of these new military capabilities, and as they develop strategies, doctrine, and organizations to best use them. The most advanced militaries are creating specific and dedicated military organizations for cyberwarfare. The 2011 assessment identified 12 states that had established or planned to establish specific military cyberwarfare entities. By 2012, that number had grown to 27, and of these, media reports indicate that 17 are developing offensive cybercapabilities. It is likely that other states are pursuing similar organizational experiments on a covert basis." Ibid, p. 3

[760] Valentino-Devries and Yadron, "Cataloging the World's Cyberforces". Their overall conclusion is that "29 countries now have formal military or intelligence units dedicated to offensive cyberefforts; 49 countries have bought off-the-shelf hacking software' 63 countries use cybertools for surveillance, either domestically or internationally." Ibid

his study builds upon and extends these research efforts in four ways. First, I recategorize evidence in line with the research goal of assessing cyber proliferation. Second, as the field is (potentially) changing rapidly, I update the available data. Third, I add new sources and material to increase the certainty and comprehensiveness of the findings. Fourth, I aim to provide not only an indication *whether* a state has proliferated, but also *when* a state has started to explore, pursue or acquire cyber weapons.

Notice that many countries may not have a military cyber program but have basic surveillance capabilities, often bought off-the-shelf. This includes Azerbaijan, Bahrain, Chile, Cyprus, Ecuador, Egypt, Ethiopia, Honduras, Hungary, Lebanon, Luxembourg, Morocco, Qatar, Panama, Mexico, Nigeria, Turkmenistan, and Zimbabwe.[761] Yet, following the definition of cyber weapons laid out in Chapter 2, this is not regarded to be a form of cyber proliferation.

Also, there are several states in the dataset which we know have established an organization dedicated to military cyber activities in a certain year, but no earlier statements are known that it was 'exploring' the development of these capabilities. In these cases, the same year is coded for 'exploration' and pursuit'. This includes: Canada, Germany, South Korea, Myanmar, and Norway.

Finally, the descriptions file of this dataset does not list countries which fall in the category of ' no discernible activity'.[762]Also, it only lists sources other than the UNIDIR report and Wall Street Journal study.

3.3 Variables

- STATE_NAME
  - A descriptive variable
  - Name of the country

- STATE_ABB:
  - A descriptive variable
  - The three-letter abbreviation of the country name

- STATE_CODE:
  - A descriptive variable
  - The Correlates of War country code

- STATE_YEAR_EXPLORATION:
  - A time variable

[761] Ibid; WikiLeaks, "Spy Files," retrieved from: https://wikileaks.org/spyfiles/
[762] Again, this concerns countries that were not listed in the UN report or in the WSJ report. I was unable to find evidence that would suggest otherwise.

- The variable denotes the first year a country first started to explore cyber weapons

- STATE_YEAR_PURSUIT:
  - A time variable
  - The variable denotes the first year a country first started to pursue cyber weapons

3.4 Limitations

Though I have aimed to consider a wide range of sources to construct the dataset, there is an inherent reliance on public statements of officials and other experts making certainty and comprehensiveness impossible.

Hence, a useful exercise is to look at which governments may not have *publicly* declared they are pursuing or exploring cyber weapons (and there is no private information available about proliferation), but - from other indicators - may in fact be at the early stages of proliferation.[763] This will helps us understand the bandwidth of uncertainty and likely (future) proliferators.[764]

Several states recognize the cyber threat as a priority issue, but do not promote the establishment of military cyber command or unit. For example, as Lewis notes, "Georgia's National Security Concept, approved by Parliament in December 2011, identifies cybersecurity as a key priority, emphasizing the need for rapid response and mitigation capabilities, information security, and international cooperation. [...] The Georgian Ministry of Defence Minister's Vision 2012-2013 prioritizes the development of cybersecurity capabilities, as well as streamlining communication and information systems." A similar discussion is provided in the 2015 Security Strategy of the Czech Republic, the cyber strategy of the Slovak Republic, and the national strategy of Sri Lanka.[765] Also, Lithuania considers cyberspace to be a new environment of warfighting and recognizes the cyber threat, yet there is no evidence to suggest that the government has established a program to develop offensive

[763] There is no specific theoretical framework underlying this discussion.
[764] Similarly, we could conduct an exercise where we look at those states which do not even have basic cyber security measures in place. The premise would be that, if a country does not even have institutions in place which coordinate prevention and response against (potential) cyber attacks, it is highly unlikely they are pursuing or exploring the development of cyber weapons.
[765] For Slovak Republic "Slovak Republic, Cyber Security Concept of the Slovak Republic for 2015 - 2020," retrieved from: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1; European Parliament, "Cyber defence in the EU Preparing for cyber warfare?" (2014, October) retrieved from: http://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf, p. 8; Matteo Gramaglia, Emmet Tuohy, Piret Pernik, "Military Cyber Defense Structures of NATO Members: An Overview,"(2013, December), retrieved from: https://www.icds.ee/fileadmin/media/icds.ee/failid/Military%20Cyber%20Defense%20Structures%20of%20NATO%20Members%20-%20An%20Overview.pdf

cyber capabilities. Kazakhstan considers the use of info technology more generally to interfere with internal affairs as a threat facing the country.[766]

In turn, there are also states which are known to have well-institutionalized cyber defence programs which seem to conduct only defence activities. Even though there is no evidence they have deployed a cyber weapon, these states may be exploring or pursuing these capabilities. An interesting case is Latvia which established a "Cyber Defence Unit" in 2014 as part of the (voluntary) National Guard of Latvia.[767] Also, Malaysia has established various organizations to promote cybersecurity. Most notably, a Cyber Defence unit was created in 2015 under the purview of the Defence Staff Intelligence Division, the military intelligence agency of the armed forces.[768] Another interesting country concerns Singapore.[769] The sovereign city-state in Southeast Asia has multiple organizations dealing with cybersecurity. For example, it has a dedicated cyber training centre to develop cyber security expertise. Yet, Singapore has no known cyber 'warfare' strategy, organization, or capability.

In addition, one may argue that countries listed above, which are known to have developed or bought off-the-shelf surveillance capabilities, are 'red hot' to pursue or explore cyber weapons (in the future).

Finally, many reports exist on the supposedly ongoing 'India-Pakistan cyber war'.[770] However, it should be noticed that these low-level activities are conducted by non-state actors. Pakistan does not have a military doctrine, organization, or capability according to the most recent U.N report or the Wall Street Journal. I was unable to find any other sources providing evidence that would support otherwise. Another peculiar coding decision may be Syria. In this dataset, it is coded as not exploring or pursuing cyber weapons. Yet, the 'Syrian Electronic Army' exists which is known to be conducting

[766] Ministry of Defence of the Republic of Kazakhstan, "Military doctrine", (2009), retrieved from: http://mod.gov.kz/mod-en/index.php/2009-06-26-02-25-27.
[767] The government is said to have just 13 "cyber guards". Ģederts Ģelzis, "Latvia launches Cyber Defence Unit to beef up online security", (2014, March 4), *Deutsche Welle*, Retrieved from: http://www.dw.com/en/latvia-launches-cyber-defence-unit-to-beef-up-online-security/a-17471936
[768] Australian Strategic Policy Institute & International Cyber Policy Centre, "Cyber Maturity in the Asia-Pacific region 2014," (2014, April), retrieved from: http://kipis.sfc.keio.ac.jp/wp-content/uploads/2014/04/ASPI_cyber_maturity_2014.pdf ; Adrian Lai, "Armed Forces set up cyber defence unit last year to prevent info leakage, hacking," *New Straits Times,* (2016, August 28) retrieved from: http://www.nst.com.my/news/2016/08/168808/armed-forces-set-cyber-defence-unit-last-year-prevent-info-leakage-hacking
[769] Lim Guang He, "Cyberspace: What are the Prospects for the SAF?" *Pointer, Journal of the Singapore Armed forces,* 41:1 (2015)58-70
[770] The News, "India, Pakistan cyber war intensifies," (2017, January 4), retrieved from: https://www.thenews.com.pk/print/176619-India-Pakistan-cyber-war-intensifies; Shashank Shekhar, "The India - Pakistan cyber war intensifies as retaliatory ransomware attack cripples websites of Islamabad, Multan and Karachi airports," *Daily Mail,* (2017, January 2), retrieved from: / http://www.dailymail.co.uk/indiahome/indianews/article-4082644/The-India-Pakistan-cyber-war-intensifies-retaliatory-ransomware-attack-cripples-websites-Islamabad-Multan-Karachi-airports.html;

relatively unsophisticated attacks. It seems that its actions thus far are not directed by the government, but this may change over time.[771]

[771] There are potential similar groups in Tunisia and Yemen. See: Unknown, "Tunisian cyber army Cyber attack against French websites," *E Hacking News*, (2013, February 2), retrieved from: http://www.ehackingnews.com/2013/02/tunisian-cyber-army-cyber-attack.html; SC Staff, "Yemen Cyber Army promises more attacks, but are they a front for Iran?, *SC Magazine UK*, (2015, July 22), retrieved from: https://www.scmagazineuk.com/yemen-cyber-army-promises-more-attacks-but-are-they-a-front-for-iran/article/534402/; Perlorth, "Hunting for Syrian Hackers' Chain of Command"

References

Aalto, Pami, "Interdisciplinary International Relations in Practice," *Forum,* 29:2 (2015)255-230

Ablon, Lillan, Martin C. Libicki, and Andrea A. Golay, "Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar," *RAND Corporation,* (2014), retrieved from: http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf

Adee, Sally, "The Hunt for the Kill Switch," *IEEE Spectrum,* (2008) Retrieved from: http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch

Aitel, David, "Useful Fundamental Metrics for Cyber Power," *CyberSecPolitics,* (2016). Retrieved from: https://cybersecpolitics.blogspot.com/2016/06/useful-fundamental-metrics-for-cyber.html.

Alberts, Jaco¸ and Harry Lensink, "Te Land, ter zee en op het web; Profiel van ons cyberleger," *Vrij Nederland,* (2014, March 29)

Alex Grisby, "Shouting at Americans: A Peek Into French Signals Intelligence," *Council on Foreign Relations: NetPolitics,* (2016, September 15), retrieved from: http://blogs.cfr.org/cyber/2016/09/15/shouting-at-americans-a-peek-into-french-signals-intelligence/

Alexander, Keith B., "Warfighting in Cyberspace," *Joint Force Quarterly,* 46 (2007):58-61

Alexander, William, and Barnaby Jack, "Could Hack Your Pacebmaker and Make your heart explode", *VICE* (2013, June 25), retrieved from: https://www.vice.com/en_se/article/i-worked-out-how-to-remotely-weaponise-a-pacemaker

Alexandrov, Maxym, "The Concept of State Identity in International Relations: A Theoretical Analysis," *Journal of International Development and Cooperation,* 10:1(2003)33-46

Allen, Nick, "Barack Obama warns of Cold War-style 'cyber arms race' with Russia," *The Telegraph,* (2016, September 5), retrieved from: http://www.telegraph.co.uk/news/2016/09/05/barack-obama-warns-of-cold-war-style-cyber-arms-race-with-russia/

Allison, Graham T., and Philip Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis,* (Pearson Education:1999)

Anderson, Ross, "Why Information Security Is Hard, an Economic Perspective," Proceedings of 17th Annual Computer Security Applications Conference (2001)

Arbor Networks, "ASERT Threat Intelligence Report 2016-03 The Four-Element Sword Engagement," (2016), retrieved from: https://www.arbornetworks.com/blog/asert/wp-content/uploads/2016/04/ASERT-Threat-Intelligence-Report-2016-03-The-Four-Element-Sword-Engagement.pdf

Arbor Networks, “The Risk vs. Cost of Enterprise DDoS Protection How to Calculate the ROI from a DDoS Defense Solution,” *White Paper* (2014), retrieved from: https://enterprise.brighthouse.com/content/dam/bhn/ent/resources/whitepapers/wp-TheRiskvsCostofENTDDoSProtectionWhitePaper.pdf

Arimatsu, Louise, “A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations”, Rain Ottis, Katharina Ziolkowski, and Christian Czosseck (Eds.) in *proceedings 4th International Conference on Cyber Conflict,* (NATO CCD COE Publications: Tallinn: 2012)

Asabere, Nana Yaw, and Wisdom Kwawu Torgby, “Structured Query Language Injection (SQLI) Attacks: Detection and Prevention Techniques in Web Application Technologies*,” International Journal of Computer Applications,* 71:11 (2013) 29-39

Aufderheide, Patricia, *Communications Policy and the Public Interest: The Telecommunications Act of 1996,* (Guilford Press: New York City:1999)

Australian Government Department of Defence, “CSOC - Cyber Security Operations Centre,” retrieved from: https://www.asd.gov.au/infosec/csoc.htm

Australian Strategic Policy Institute & International Cyber Policy Centre, “Cyber Maturity in the Asia-Pacific region 2014,” (2014, April), retrieved from: http://kipis.sfc.keio.ac.jp/wp-content/uploads/2014/04/ASPI_cyber_maturity_2014.pdf

Australian Times, “Australia implicated in Regin mega cyber-warfare program,” (2015, January 30), Retrieved from: http://www.australiantimes.co.uk/australia-implicated-regin-mega-cyber-warfare-program/

Aviram, Jenik, “Cyberwar in Estonia and the Middle East,” *Network Security*, 4 (2009)4-6

Baldwin, David, “The Concept of Security,” *Review of International Studies*, 23 (1997)5-26

Ball, James, “Good news for lobbyists: Cyber dollars,” *The Washington Post,* (2012, November 13), retrieved from: https://www.washingtonpost.com/postlive/good-news-for-lobbyists-cyber-dollars/2012/11/12/158a361e-29f9-11e2-b4e0-346287b7e56c_story.html?utm_term=.507e1e4df797

Ball, Nichole, "Third World arms control: a Third World responsibility," in Thomas Ohlson (ed.), *Arms Transfer Limitations and Third World Security*, (Oxford: Oxford University Press: 1988)

Barber, Bryan, “Cheese Worm: Pros and Cons of a Friendly Worm,” *Sans Institute GSEC v1.2e,* (2001) retrieved from: https://www.sans.org/reading-room/whitepapers/malicious/cheese-worm-pros-cons-friendly-worm-31

Barki, Henri and Alain Pinsonneault, “A Model of Organizational Integration, Implementation Effort, and Performance,” *Organization Science,* 16:2 (2005)165-179.

Barlow, John Perry, “A Declaration of the Independence of Cyberspace, ” *Electronic Frontier Foundation,* (1996) retrieved from: https://www.eff.org/cyberspace-independence

Barnaby, Frank, "How States can "go nuclear," *Annals of the American Academy of Political and Social Science,* 430 (1977):29-43

Barreira, Victor, "Brazil announces establishment of new cyber defence command," *Jane's 360,* (2016, December 29), retrieved from: http://www.janes.com/article/66601/brazil-announces-establishment-of-new-cyber-defence-command

Baumgartner, Kurt, "Sony/Destover: mystery North Korean actor's destructive and past network activity: Comparisons with Shamoon and DarkSeoul," (4 December 2014), retrieved from: https://securelist.com/blog/research/67985/destover/

BBC News, "North Korea 'hacks South's military cyber command," (2016, December 6), retrieved from: http://www.bbc.com/news/world-asia-38219009

Beaton, Leonard¸ and John Maddox, *The spread of nuclear weapons,* (New York: Praeger: 1962)

Bell, Mark S., "Examining Explanations for Nuclear Proliferation: Research Note," *International Studies Quarterly,* 60 (2016)520-529

Bellovin, Steven M., Susan Landau, and Herbert S. Lin, "Limiting the Undesired Impact of Cyber Weapons: Technical Requirements and Policy Implications," *Journal of Cybersecurity,* 3:1(2017)59-68

Bencsáth, Boldizsár, "Duqu, Flame, Gauss: Followers of Stuxnet," *Presented at RSA Conference Europe*, (2012), retrieved from: http://www.rsaconference.com/writable/presentations/file_upload/br-208_bencsath.pdf

Bendrath, Ralf, "The American cyber-angst and the real world - any link?" Paper presented at: International Studies Association Annual Convention, University of Bremen (2004)

Bendrath, Ralf, "The American Cyber-Angst and the Real World," in *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*, (ed.) Robert Latham (New York: The New Press: 2003).

Bendrath, Ralph, "The Cyberwar Debate Perception and Politics in U.S. Critical Infrastructure Protection," in *Information & Security,* 7 (2001): 80-103

Betz, David J., and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-power,* (Adelphi Books: Washington DC, 2011)

Betz, David, "Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed," *Journal of Strategic Studies,* 35:5, (2012), 689-711

Betz, David, and Tim Stevens, "Analogical Reasoning and Cyber Security," *Security Dialogue,* 44:2(2013):147-164.

Bilge, Leyla and Tudor Dumitras, "Before We Knew It An Empirical Study of Zero-Day Attacks In The Real World," CCS '12 Proceedings of the 2012 ACM conference on Computer and communications security (2012) 833-844

Bing, Chris, "U.S. Cyber Command director: We want 'loud,' offensive cyber tools," *FedScoop*, (2016, August 3), Retrieved from: https://www.fedscoop.com/us-cyber-command-offensive-cybersecurity-nsa-august-2016

Blake, Duncan, and Joseph S. Imburgia, " 'Bloodless weapons?' The Need to Conduct Legal Reviews of Certain Capabilities and the Implications of Defining them as 'Weapons,'" *The Air Force Law Review*, 66 (2010)

Blakesware "A Guide to Texas Hold'em Poker," retrieved from: http://www.how-to-hold-a-party.com/downloads/HowToPlayPoker.pdf

Bleek, Philip, "Does proliferation beget proliferation? Why nuclear dominoes rarely fall" *PhD Dissertation Georgetown University*, (2010)

Bloom, Gedare, Eugen Leontie, Bhagirath Narahari, and Rahul Simha, "Chapter 12: Hardware and Security: Vulnerabilities and Solutions" in Sajal K Das, Krishna Kant, Nan Zhang (eds.), *Handbook on Securing Cyber-Physical Critical Infrastructure: Foundations and Challenges*, (Elsevier: 2012);

Boere, Raymond, "Leger zoekt 150 whizzkids voor Cyber Commando," *Het Algemeen Dagblad*, (2013, November 2), retrieved from: http://www.ad.nl/binnenland/leger-zoekt-150-whizzkids-voor-cyber-commando~a2e242d5/?vwoParameters=vwo-abbo

Borghard, Erica D., and Shawn W.Lonergan, "Can States Calculate the Risks of Using Cyber Proxies?," *Orbis*, 60:3 (2016) 395-416

Boston Consulting Group, "Perspective on Experience," *Technical Report* (1972)

Boulanin, Vincent, "Arms production goes cyber: a challenge for arms control," *SIPRI Publication*, (2013, May 30), retrieved from: https://www.sipri.org/node/361

Boulanin, Vincent, "Cybersecurity and the arms industry," *SIPRI Yearbook 2013: Armaments, disarmament and international security* (Oxford: Oxford University Press: 2013), pp. 218-226

Bouwmeester, Hans, Hans Folmer and Paul Ducheine, "Cyber Security and Policy Responses," in Paul Ducheine, Frans Osinga, Joseph Soeters (eds.), *Cyber Warfare: Critical Perspectives*, (The Hague: Asser Press: 2012)

Brazil's Ministry of Defence, "National Strategy of Defense," (2008, December 18), retrieved from: https://www2.gwu.edu/~clai/recent_events/2010/Brazil_Defense/National_Strategy_of_Defense.pdf

Brehm, John, and Scott Gates, *Working, Shirking, and Sabotage: Bureaucratic Response to a Democratic Public*, (Michigan: University of Michigan Press: 1997)

Brenner, Joel, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*, (New York: Penguin Press: 2011)

Brey, Philip, "'Space-Shaping Technologies and the Geographical Disembedding of Place," *Philosophy & Geography*, 3 (1998)239-263

Brey, Rajoy. "National Cyber Security Strategy of Spain," (2013), retrieved from: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_ESen.pdf

Bristow, Sharon, "Code Red Worm Invasion," *SANS Institute* (2001) Retrieved from: https://www.sans.org/reading-room/?utm_source=web&utm_medium=text-ad&utm_content=generic_rr_pdf_logo1&utm_campaign=Reading_Room&ref=36909

Brito, Jerry, and Tate Watkins, "The Cybersecurity-Industrial Complex," *Reason*, 43:4 (2011):1-39

Britton, Rebecca L., and Bruce Jentleson, "Still Pretty Prudent," *Journal of Conflict Resolution*, 42:4 (1998) 395-418

Broad, William J., and David E. Sanger, "Israeli Test on Worm Called Crucial in Nuclear Delay," *The New York Times*, (2011), retrieved from: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

Brodie, Bernard (ed.), *The Absolute Weapon: Atomic Power and World Order*, (New York: Brace and Company: 1946)

Brown, Robert L., and Jeffrey M. Kaplow, "Talking Peace, Making Weapons IAEA Technical Cooperation and Nuclear Proliferation," *Journal of Conflict Resolution*, 58:3 (2014) 402-428

Buchanan, Ben, "A not-so Secret History of Cyber War," *War on the Rocks*, (2016, June 30), retrieved from: https://warontherocks.com/2016/06/a-not-so-secret-history-of-cyber-war/

Buchanan, Ben, *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations*, (London: Hurst Publications: 2017)

Budd, Christopher, "Operation Iron Tiger: Attackers Shift from East Asia to the United States," *TREND Micro*, (2015, September 15), retrieved from: Newsroom.trendmicro.com/blog/operation-iron-tiger-attackers-shift-east-asia-united-states

Burns, Nicholas, and Jonathon Price, *Securing Cyberspace: A New Domain for National Security*, (Aspen, CO: Aspen Institute, 2012)

Burton, Joe, "Small states and cyber security: the case of New Zealand," *Political Science*, 65(2013)216

Buzan, Barry, "Will the 'Global War on Terror' Be the New Cold War?," *International Affairs*, 82 (2006):1102-1118.

Byres, Eric, Andrew Ginter, Joel Langill, "How Stuxnet Spreads - A Study of Infection Paths in Best Practice Systems," Version 1.0, (2011, February 22), Retrieved from: http://www.abterra.ca/papers/how-stuxnet-spreads.pdf

Calhoun, Craig, *Dictionary of the Social Sciences*, (Oxford: Oxford University Press: 2002)

Cardon, Edward C., "The Future of Army Maneuver - Dominance in the Land and Cyber Domains," *The Cyber Defense Review*, 1:1 (2016), 15-21

CBS News, "Stuxnet: Computer Worm Opens New Era of Warfare," *60 Minutes*, Transcript (2012, March 4)

CBS News, "Cyber War: Sabotaging the System," (2009, November 6), Retrieved from: http://www.cbsnews.com/news/cyber-war-sabotaging-the-system-06-11-2009/

CBS News, "Fmr. CIA head calls Stuxnet virus 'good idea," *60 Minutes*, (2012, March 1), Retrieved from: http://www.cbsnews.com/news/fmr-cia-head-calls-stuxnet-virus-good-idea/

Center for Human Rights in Iran, "Khamenei Consolidates Power over Internet Policy in Hard Line Council He Controls," (2015, September 14), retrieved from: https://www.iranhumanrights.org/2015/09/khamenei-internet-policy-iran/

Chang, Jennifer, "US, South Korea join forces to prevent cyberattacks by North Korea," PC World / IDG News Service, (2013, April 3), retrieved from: http://www.pcworld.com/article/2032918/us-south-korea-join-forces-to-prevent-cyberattacks-by-north-korea.html

Cho, Dong-Sung, Dong-Jae Kim, and Dong Kee Rhee, "Latecomers Strategies: Evidence from the Semiconductor Industry in Japan and Korea," *Organizational Science*, 9:4 (1998, July-August), p. 498-504

Cirenza, Patrick, "The flawed analogy between nuclear and cyber deterrence," *Bulletin of the Atomic Scientists*, (2016, February 22), Retrieved from: http://thebulletin.org/flawed-analogy-between-nuclear-and-cyber-deterrence9179

Clapper, James R., Marcel Lettre, and Michael S. Rogers, "Joint Statement for the Record to the Senate Armed Services Committee Foreign Cyber Threats to the United States," (2017, January 5), Retrieved from: http://www.globalsecurity.org/intell/library/congress/2017_hr/160105_clapper-lettre-rogers_sasc.pdf

Clarke, David D., and Susan Landau, "The problem isn't attribution; It's multi-stage attacks," *ACM ReArch*, (November 30, 2010)

Clarke, Richard A., and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: Harpercollins: 2010)

Clifford Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*, (Pocket Books: 2000)

Cohen, Raymond, "Threat Perception in International Crisis," *Political Science Quarterly*, 1(1978)93-107,

Collier, David, and James E. Mahon, Jr., “Conceptual “Stretching” Revisited: Adapting Categories in Comparative Analysis,” *The American Political Science Review,* 87:4 (1993):845-855

Collins, Sean, and Stephen McCombie, “Stuxnet: the emergence of a new cyber weapon and its implications,” *Journal of Policing, Intelligence, and Counter Terrorism,* 7:1 (2012)80-91

Constantin, Lucian, “Kill timer found in Shamoon malware suggests possible connection to Saudi Aramco attack,” Computerworld, (2012, August 23), retrieved from: http://www.computerworld.com/article/2491501/malware-vulnerabilities/kill-timer-found-in-shamoon-malware-suggests-possible-connection-to-saudi-ar.html

Cooper, Andrew, Richard A. Higgott, Kim Richard Nossal, *Relocating Middle Powers: Australia and Canada in a Changing World Order*, (Vancouver: University of British Columbia Press: 1993)

Cornish, Paul, David Livingstone, Dave Clemente and Claire Yorke, “On Cyber Warfare,” A *Chatham House Report,* (2010, November)

Cornwell, Rubert, “Intercepted Shipment was a Key to Libya Deal,” *Financial Times Global News Wire,* (2004, January), retrieved from: http://www.independent.co.uk/news/world/politics/intercepted-shipment-was-key-to-libya-deal-72546.html

Crawford, Vincent P., “Lying for Strategic Advantage: Rational and Boundedly Rational Misrepresentation of Intentions,” *The American Economic Review,* (2003, March)133-149

Crawford, Vincent P., and Joel Sobel, Strategic Information Transmission, *Econometrica,* 50:6(1982)1431-1451

Crowdstrike, “Use of Fancy Bear Android Malware in Tracking of Ukrainiian Field Artillery Units,” (2017, March 23) retrieved from: https://www.crowdstrike.com/wp-content/brochures/FancyBearTracksUkrainianArtillery.pdf

Cyber Studies Conflict Association, “ Cyber Conflict State of the Field Conference,” New York City: Columbia University - School of International and Public Affair, (2017, June 8-9)

Czosseck, Christian, Rain Ottis and Anna-Maria Talihärm, "Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security," *Journal of Cyber Warfare and Terrorism*, 1:1 (2011)57-64

Dahl, Matt, “Sakula Reloaded”, *Crowdstrike,* (2015, November 18), Retrieved from: www.crowdstrike.com/blog/sakula-reloaded/

Darczewska, Jolanta, “The anatomy of Russian information warfare; the Crimean operation, a case study,” *Centre for Eastern Studies*, (2014) retrieved from: https://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf

Davies, Martin, "Knowledge - Explicit, implicit and tacit: Philosophical aspects," in James D. Wright (ed.), *International Encyclopaedia of Social and Behavioral Sciences*, retrieved from: http://www.mkdavies.net/Martin_Davies/Papers_files/KnowledgeExpImpTacit.pdf

Davis, Joshua, "Hackers take down the most wired country in Europe," *Wired*, (2008, August 21), retrieved from: https://www.wired.com/2007/08/ff-estonia/

De Maizière, Thomas, "Die Lage der IT-Sicherheit in Deutschland 2014," *Bundesamt für Sicherheit in der Informationstechnik*, (2014), retrieved from: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile

De Telegraaf, "Cyberspecialist belangrijk wapen; Slimme virussen verlammen de vijand," (2015, April 15), retrieved from: https://www.pressreader.com/netherlands/de-telegraaf/20150415/281672548470641

De Telegraaf, "Militair moet zelf pang-pang reopen," (2015, August 1) retrieved from: http://www.telegraaf.nl/binnenland/24330771/__Soldaat_moet__pang__roepen__.html

DefenseNews, "Poll 2014: Cyberwarfare Is Top Threat Facing US," (2014, January 5), retrieved from: http://www.defensenews.com/article/20140105/DEFREG02/301050011/Poll-Cyberwarfare-Top-Threat-Facing- US

Deibert, Ronald J., "The Growing 'Dark Side' of Cyberspace," *Penn State Journal of Law and International Affairs*, 1:2(2012) 260-274.

Deibert, Ronald J., "Cyclone in cyberspace: information shaping and denial in the 2008 Russia-Georgia war," *Security Dialogue*, 43 (2012):3-24

Denning, Dorothy, "Reflections of Cyberweapons Controls," *Computer Security Journal*, 16:4(2000):43-53

Department of Defense, "All Cyber Mission Force Teams Achieve Initial Operating Capability," *U.S. Cyber Command News Release*, (2016, October 24), retrieved from: http://www.defense.gov/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability

Der Spiegel, "Routine Disposal Goes Wrong: Three Killed in Explosion of World War II Bomb in Germany", *Spiegel Online International*, (2 June, 2010), Retrieved from: http://www.spiegel.de/international/germany/routine-disposal-goes-wrong-three-killed-in-explosion-of-world-war-ii-bomb-in-germany-a-698245.html

Der Spiegel, "SPIEGEL Interview with Syrian President Bashar Assad 'Peace without Syria Is Unthinkable'", (2009, January 19), retrieved from: http://www.spiegel.de/international/world/spiegel-interview-with-syrian-president-bashar-assad-peace-without-syria-is-unthinkable-a-602110.html

DiMaggio, Paul J., and Walter W. Powell, "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields," *American Sociological Review*, 48: 2 (1983)147-160

Dinstein, Yoram, "Computer Network Attacks and Self-Defense," *International Law Studies,* 76(2002):103.

Dipert, Randall, "The Ethics of Cyberwarfare," *Journal of Military Ethics,* 9:4 (2010):284-410

Dmitry Tarakanov, "Shamoon The Wiper: Further Details (Part II)," *Securelist,* (2012, September 11) retrieved from: https://securelist.com/blog/incidents/57784/shamoon-the-wiper-further-details-part-ii/

Doctorow, Cory, "Feds admit they used secret anti-terror mass surveillance tool to catch an undocumented waiter," *BoingBoing,* (2017, May 19), Retrieved from: http://boingboing.net/2017/05/19/swatting-jaywalkers-with-tacti.html

Dubnick, Melvin J., and Barbara S. Romzek, "Accountability and the Centrality of Expectations in American Public Administration," *Research in Public Administration,* 2 (1993): 37-78

Dumitru Ducaru, Sorin, "The Cyber Dimension of Modern Hybrid Warfare and its Relevance for NATO," *Europolity*, 10:1 (2016)7-23

Dunn Cavelty, Myriam, *Cyber-Security and Threat Politics US Efforts to Secure in the Information Age* (Abingdon: Routledge: 2008)

Dunn, Lewis A., and Herman Kahn, *Trends in nuclear proliferation, 1975-1995,* (Croton-on Hudson: Hudson Institute: 1976)

Dunn, Myriam, "A Comparative Analysis of Cybersecurity Initiatives Worldwide," *International Telecommunications Union*, WSIS, Thematic Meeting on Cybersecurity, Geneva, (2005, June/July) , retrieved from: https://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_InitiativesWorldwide.pdf

Duyvesteyn, Isabelle, "Between doomsday and dismissal Cyber war, the parameters of war, and collective defense," (2012) retrieved from: https://www.atlcom.nl/ap_archive/pdf/AP%202014%20nr.%207/Duyvesteyn.pdf;

E Hacking News, "Tunisian cyber army Cyber attack against French websites," (2013, February), retrieved from: http://www.ehackingnews.com/2013/02/tunisian-cyber-army-cyber-attack.html

EastWest Institute, "Working Towards Rules for Governing Cyber Conflict Rendering the Geneva and Hague Conventions in Cyberspace," (2011),retrieved from: https://www.eastwest.ngo/sites/default/files/ideas-files/US-Russia%20(1).pdf

Ebert, Hannes, and Tim Maurer, "Contested Cyberspace and Rising Powers," *Third World Quarterly,* 34:6 (2013): 1054-1074

Eckert, Sue, "Protecting Critical Infrastructure: The Role of the Private Sector," University of Pittsburg (2006), retrieved from: http://www.ridgway.pitt.edu/Portals/1/pdfs/Publications/Eckert.pdf

Eckstein, Harry, "Case Studies in Political Science," in Alexander L. George and Andrew Bennet, *Case Studies and Theory Development in the Social Sciences* (Cambridge, MA: MIT Press: 2004)

Ecology, "World Birth and Death Rates," retrieved from: http://www.ecology.com/birth-death-rates/

Een Vandaag, "Wat gebeurt er bij het Defensie Cyber Commando?," (2014, September), retrieved from: http://www.eenvandaag.nl/binnenland/54190/wat_gebeurt_er_bij_het_defensie_cyber_commando_

Eisenberg, Ted, David Gries, Juris Hartmanis, Don Holcomb, M. Stuart Lynn, Thomas Santoro, "The Cornell Commission: On Morris and the Worm," *Communications of the ACM*, 32:6, (1989), p. 706-709

Endicott, John E., *Japan's Nuclear Option*, (New York: Praeger, 1975), p. 114.

Epstein, William, "*The Last Chance: The Unbearable Lightness of the NPT*," (New York: Free Press: 1976)

European Parliament, "Cyber defence in the EU Preparing for cyber warfare?" (2014, October) retrieved from: http://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf

Evron, Gadi, "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War," *Georgetown Journal of International Affairs*, 9:1 (2008): 121-126

Ewert, Burkhard, "Marschbefehl in den Cyberkrieg," *Deutschlandfunk*, (2017, April 8), retrieved from: http://www.deutschlandfunk.de/neues-bundeswehrkommando-marschbefehl-in-den-cyberkrieg.720.de.html?dram:article_id=383346

Farraposo, Sílvia, Laurent Gallon, Philippe Owezarski, "Network Security and DoS Attacks" Unpublished Manuscript, (2005)

Farrell, Joseph, and Matthew Rabin, "Cheap Talk," *Journal of Economic Perspectives*, 10:3 (1996):103-118

Farrell, Joseph, and Robert Gibbons, "Cheap Talk with Two Audiences," *The American Economic Review*, 79:5 (1989)1214-1223

Farwell, James P., "Industry's Vital Role in National Cyber Security," *Strategic Studies Quarterly* (2012): 10-41.

Farwell, James P., and Rafal Rohozinski, "Stuxnet and the Future of Cyber War", *Survival: Global Politics and Strategy*, 53:1 (2011):23-40

Fearon, James D., "Domestic Political Audiences and the Escalation of International Disputes," *American Political Science Review*, 88:3 (1994)577-592

Fearon, James D., "Rationalist Explanations for War," *International Organization*, 49:3 (1995)379-414

Feaver, Peter D., "Optimists, Pessimists, and Theories of Nuclear Proliferation Management: Debate," *Security Studies*, 4:4 (1995)754-772, p. 756

Feaver, Peter D., and Christopher Gelpi, *Choosing Your Battles: American Civil-Military Relations and the Use of Force* (Princeton, N.J.: Princeton University Press: 2004).

Feaver, Peter, and Christopher Gelpi, "How Many Deaths Are Acceptable? A Surprising Answer," *Washington Post,* (1999, November 7), retrieved from: http://www.washingtonpost.com/wp-srv/WPcap/1999-11/07/061r-110799-idx.html

Feinberg, Joel, *The Moral Limits of the Criminal Law Volume 1: Harm to Others*, (Oxford: Oxford University Press: 1987)

Finish Ministry of Defence, "Finland´s Cyber security Strategy," (2013, January 24), retrieved from: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/FinlandsCyberSecurityStrategy.pdf

Finkle, Jim, "Exclusive: FBI warns of 'destructive' malware in wake of Sony attack," *Reuters,* (2014, December 2), retrieved from: www.reuters.com/article/us-sony-cybersecurity-malware-idUSKCN0JF3FE20141202

Finnemore, Martha, and Kathryn Sikkink, "International norm dynamics and political change," *International Organization* 52 (1998): 887-917

Finnemore, Martha, *National Interests in International Society,* (Ithaca: Cornell University Press: 1996)

FireEye, "Advanced Targeted Attacks: How to Protect Against the Next Generation of Cyber Attacks," *White Paper,* (2012), Retrieved from: http://www.softbox.co.uk/pub/fireeye-advanced-targeted-attacks.pdf

FireEye, "Redline Drawn: China Recalculates its use of cyber espionage," (2016, June 20), retrieved from: https://www.fireeye.com/blog/threat-research/2016/06/red-line-drawn-china-espionage.html.

Fischerkeller, Michael, "Incorporating Offensive Cyber Operations into Conventional Deterrence Strategies", *Survival,* 59:1 (2017)103-134

Florida Center for Instructional Technology "Chapter 2: What is a Protocol?" (2013), Retrieved from: http://fcit.usf.edu/network/chap2/chap2.htm

Follath, Erich, and Holger Stark, "How Israel Destroyed Syria's Al Kibar Nuclear Reactor," *Der Spiegel,* (2009, November 2) retrieved from: http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663-2.html

Folmer, Hans, "Defense Cyber Commando: Een nieuwe loot aan de defensie boom", *Operationeel: Intercom*, 45:1 (2016)22-28

Foong Khong, Yuen, *Analogies at War: Korea, Munich, Dien Bien Phu and the Vietnam Decisions of 1965*, (1992: Princeton University Press, Princeton, New Jersey)

FoxIT, "Ministerie van Defensie en Fox-IT sluiten Raamovereenkomst," (2017) Retrieved from: https://www.fox-it.com/nl/over-fox-it/corporate-nieuws/news/derde-leergang-cyberopleidingsprogramma-cop-iii-start/

Frank, Jim W., "Summary Report of the Nth Country Experiment," *Lawrence Radiation Laboratory*, (1967, March)

Frenceschi-Bicchierai, Lorenzo, "The New Shadow Brokers Leak Connects the NSA to the Stuxnet Cyber Weapon Used on Iran," *Motherboard*, (2017, April 17), Retrieved from: https://motherboard.vice.com/en_us/article/shadow-brokers-nsa-stuxnet-iran

Friedersdorf, Conor, "Keith Alexander's Unethical get-Rich-Quick-plan", *The Atlantic*, (2014, July 31), Retrieved from: www.theatlantic.com/politics./archive/2014/07/keith-alexanders-unethical-get-rich-quick-plan/375367/

F-Secure, "The Dukes: 7 years of Russian cyberespionage," *Whitepaper*, (2011, January 29), retrieved from: https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf

Fuhrmann, Matthew, and Benjamin Tkach, "Almost nuclear: Introducing the Nuclear Latency dataset," *Conflict Management and Peace Science*, 32:4 (2015) 443-461

Fulghum, David A., Robert Wall, and Amy Butler, "Cyber-Combat's First Shot," *Aviation Week & Space Technology*, (2007, November 26)

Gady, Franz-Stefan, and Greg Austin, "Russia, The United States, And Cyber Diplomacy Opening the Doors" *East West Institute*,(2010) retrieved from: https://info.aiaa.org/tac/isg/SOFTC/Public%20Documents/Technical%20Working%20Groups/Cybersecurity/USRussiaCyber_WEB.pdf

Gallagher, Ryan, and Glenn Greenwald, "How the NSA plans to infect 'millions' of computers with malware," *The Intercept*, (2014, March 12), retrieved from: https://theintercept.com/2014/03/12/nsa-plans-infect-millions-commputers-malware/

Gallie, Walter B., "Essentially Contested Concepts," *Proceedings of the Aristotelian Society,* New Series, 56 (1955 - 1956):167-198

Gartner, "Gartner Says Worldwide PC Shipments Grew 1 Percent in Fourth Quarter of 2014," (2015, January), Retrieved from: http://www.gartner.com/newsroom/id/2960125

Gartzke, Erik, and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies*, 24:2, (2015) 316-348.

Gartzke, Erik, Jeffrey M. Kaplow, Rupal N. Mehta, "The Determinants of Nuclear Force Structure," *Journal of Conflict Resolution,* 58:3 (2014)481-508

Geller, Eric, "NSA-created cyber tool spawns global attacks — and victims include Russia," *Politico,* (2017, May 12), retrieved from: http://www.politico.com/story/2017/05/12/nsa-hacking-tools-hospital-ransomware-attacks-wannacryptor-238328

Gellman, Barton, and Ellen Nakashima, "U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show,"(2013, August 30), *The Washington Post,* retrieved from: https://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html?utm_term=.dfb3852da14a;

Gellman, Barton, and Ellen Nakashima, "U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show," *The Washington Post,* (2013, August 30), Retrieved from: https://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html

Gelpi, Christopher, Peter D. Feaver and Jason Reifler, *Paying the Human Costs of War: American Public Opinion and Casualties in Military Conflicts,* (Princeton: Princeton University Press: 2009)

Gelpi, Christopher, Peter D. Feaver, and Jason Reifler, "Success Matters: casualty Sensitivity and the War in Iraq," *International Security,* 30:3 (2005-2006), pp. 7-46

Ģelzis, Ģederts, "Latvia launches Cyber Defence Unit to beef up online security", (2014, March 4), *Deutsche Welle,* Retrieved from: http://www.dw.com/en/latvia-launches-cyber-defence-unit-to-beef-up-online-security/a-17471936

Gerard Ruggie, John, "What Makes the World Hang Together? Neo-utilitarianism and the Social Constructivist Challenge," *International Organization,* 52:4 (1998) 855-885

Gerden, Eugene, "Russia to spend $250m strengthening cyber-offensive capabilities," *SC Magazine UK,* (2016, February 4), retrieved from: http://www.scmagazineuk.com/russia-to-spend-250m-strengthening-cyber-offensive-capabilities/article/470733

Gilbert, David, "Cost of Developing Cyber Weapons Drops from $100M Stuxnet to $10K IceFog," *International Business Time*s, (2014, February 6) retrieved from: http://www.ibtimes.co.uk/cost-developing-cyber-weapons-drops-100m-stuxnet-10k-icefrog-1435451

Gjelten, Tom, "Shadow Wars, Debating Cyber 'Disarmament,'" *World Affairs,* 173:4 (2010)33-42

Goertz, Gary, *Social Science Concepts: A User's Guide* (Princeton: Princeton University Press: 2005)

Goldsmith, Jack, "The United States' Feckless Cyber Deterrence Policy," *Lawfare,* (2015, August 1), retrieved from: https://www.lawfareblog.com/united-states-feckless-cyber-deterrence-policy

Gompert, David C.,and Martin Libicki, “Waging Cyber War the American Way,” *Survival*, 57:4 (2015)7-28

Gostev, Alexander, “Agent.btz: a Source of Inspiration?” *Securelist*, (2014, March 12), Retrieved from: https://securelist.com/blog/virus-watch/58551/agent-btz-a-source-of-inspiration/

Government of South Africa, “South African Defence Review 2012,” retrieved from: http://www.gov.za/sites/www.gov.za/files/defence%20review_daft.pdf

Gramaglia, Matteo, Emmet Tuohy, Piret Pernik, “Military Cyber Defense Structures of NATO Members: An Overview,”(2013, December), retrieved from: https://www.icds.ee/fileadmin/media/icds.ee/failid/Military%20Cyber%20Defense%20Structures%20of%20NATO%20Members%20-%20An%20Overview.pdf

Gray, Colin S., *Explorations in Strategy,* (Westport: Praeger Publishers: 1996)

Greenberg, Andy, “How an Entire Nation Became Russia’s Test Lab for Cyberwar,” *Wired*, (2017, June 20), retrieved from: https://www.wired.com/story/russian-hackers-attack-ukraine/

Greenwald, Glenn, “NSA Claims Iran Learned from Western Cyberattacks,” *The Intercept*, retrieved from: https://theintercept.com/2015/02/10/nsa-iran-developing-sophisticated-cyber-attacks-learning-attacks/

Greenwood, Ted, Harold A. Feiveson, and Theodore B. Taylor, *Nuclear proliferation: Motivations, capabilities, and strategies for control*, (New York: McGraw-Hill: 1977);

Griffiths, James, “Price of website disabling DDoS attacks fall to US$38 per hour as botnets proliferate in China, Vietnam,” *South China Morning Post*, (2015, June 12), retrieved from: http://www.scmp.com/tech/enterprises/article/1820464/price-website-disabling-ddos-attacks-fall-us38-hour-botnets

Griffiths, Peter, “World faces "cyber cold war" threat,” *Reuters*, (2007, November 29) retrieved from: http://www.reuters.com/article/us-britain-internet-idUSL2932083320071129

Grindal, Karl, and Jason Healey, “Hand out: Cyber Conflict History,” State of the Field of Cybersecurity Studies: Columbia University, (2016, June 15-17)

Gross Stein, Janice, “Threat Perceptions in International Relations,” in Leonie Huddy, David O. Sears, and Jack S. Levy (eds.) *The Oxford Handbook of Political Psychology*, (Oxford: Oxford University Press: 2013).

Guang He, Lim, “Cyberspace: What are the Prospects for the SAF?” *Pointer, Journal of the Singapore Armed forces*, 41:1 (2015)58-70

Guisinger, Alexandra and Alastair Smith, "Honest threats: The interaction of reputation and political institutions in international crises," *Journal of Conflict Resolution*, 46, (2002)175-200

Gupta, Sanjay, “Dick Cheney’s Heart,” (2013, October 20), *CBN News*, Retrieved from: http://www.cbsnews.com/news/dick-cheneys-heart/

Hammond, Philip, “National Cyber Security Strategy 2016 to 2021,” (2016, November) retrieved from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Hansen, Lene, and Helen Nissenbaum, “Digital Disaster, Cyber Security, and the Copenhagen School”, 53,4 (2009):1155-1175

Harney, Robert, Gerald Brown, Matthew Carlyle, Eric Skroch, and Kevin Wood, “Anatomy of a Project to Produce a First Nuclear Weapon,” *Science and Global Security*, 14(2006)163-182

Harris, Shane, “The NSA’s Cyber-King Goes Corporate: Here’s why Keith Alexander thinks he’s worth a million dollars a month,” *Foreign Policy,* (2014, July 29), retrieved from: www.foreignpolicy.com/2014/07/29/the-nsas-cyber-king-goes-corporate

Hartung, William D., “The International Arms Trade,” in Paul D. Williams (Ed), *Security Studies: An Introduction,* (Abingdon: Routledge: 2008)

Hathaway, Melissa, "Leadership and Responsibility for Cybersecurity", *Georgetown Journal of International Affairs*, (2012):71-80

Hayden, Michael V., "The Future of Things Cyber," *Strategic Studies Quarterly*, 5:1(2011):3-8; p.3

Hayden, Michael, *Playing to the Edge: American Intelligence in the Age of Terror*, (New York, Penguin Random House, 2016)

Healey, Jason, “Beyond Attribution: Seeking National Responsibility for Cyber Attacks,” *Atlantic Council:* Cyber Statecraft Initiative, Issue Brief (2011), retrieved from: http://www.atlanticcouncil.org/publications/issue-briefs/beyond-attribution-seeking-national-responsibility-in-cyberspace

Healey, Jason, “Feds and 0Days: From Before Heartbleed to After FBI-Apple,” *DefCon, Las Vegas* (2016)

Hennis- Plasschaert, Jeanine, “Antwoorden op feitelijke vragen van de vaste commissie voor Defensie over de begrotingsstaten van het Ministerie van Defense (X) voor het jaar 2017,” *Dutch House of Representatives,* (2016, November 6)

Hennis-Plasschaert, Jeanine A., “Antwoorden op feitelijke vragen van de vaste commissie voor Defensie over de begrotingsstaten van het Ministerie van Defensie (X) voor het jaar 2017,” Dutch House of Representatives, BS2016025082, (2016)

Henrikson, Alan K., “Middle Powers as Managers: International Mediation within, across, and outside Institutions,” in Andrew Cooper (ed.), *Niche Diplomacy*, (London: Palgrave Macmillan: 1997)

Herken, Gregg, “The Not-Quite-Absolute Weapon: Deterrence and the Legacy of Bernard Brodie,” *Journal of Strategic Studies,* 9:4 (1986)15-24

Herr, Trey, “PrEP: A Framework for Malware & Cyber Weapons,” *The Journal of Information Warfare,* 13:1 (2014)1-28

Herr, Trey, Bruce Schneier and Christopher Morris, “Taking Stock: Estimating Vulnerability Rediscovery,” (2017, March 7), retrieved from: http://papers.ssrn.co/sol3/papers.cfm?abstract_id=2928758

Hichkad Ravi R., and Christopher J. Bowie. "Secret Weapons & Cyberwar." *Armed Forces Journal,* 149:10 (2012):14-18

Hodges, David A., and Robert C. Leachman, “Outsourcing and Offshoring in the Semiconductor Industry,” Sloan Industry Centers Annual Conference Atlanta, GA (2004)

Hoffman, Frank, *Conflict in the 21st Century: The Rise of Hybrid Warfare* (Arlington, VA: Potomac Institute for Policy Studies: 2007)

Hollis, David M., “Cyberwar case Study: Georgia 2008,” *Small Wars Journal,* (2011, January)

Hollis, Martin, and Steve Smith, *Explaining And Understanding International Relations,* (Oxford: Oxford University Press: 1991)

Homan, Kees, “Ambitieniveau defensie op droevig dieptepunt”, *Reformatorisch Dagblad,* (2013, September 21)

Hopf, Ted, *Social Construction of International Politics: Identities & Foreign Policies, Moscow, 1955 and 1999,* (Ithaca, NY: Cornell University Press: 2002)

Horm, Johannes, “Exploit CVE-2015-0274,” Unpublished Manuscript, (2015) Retrieved from: http://kodu.ut.ee/~mroos/turve/2015/referaadid/CVE-2015-0274_Johannes_Horm.pdf

Horowitz, Michael C., and Neil Narang, “Poor Man’s Atomic Bomb? Exploring the Relationship between ‘Weapons of Mass Destruction’”, *Journal of Conflict Resolution,* 00:0 (2013) 1-27

Hosenball, Mark, “FBI paid under $1 million to unlock San Bernardino iPhone,” *Reuters,* retrieved from: http://www.reuters.com/article/us-apple-encryption-idUSKCN0XQ032

House of Commons, “Russia: Implications for UK defence and security ,” *First Report of Session 2016-17,* (2016), retrieved from: https://www.publications.parliament.uk/pa/cm201617/cmselect/cmdfence/107/107.pdf

Hun, Choe Shang, and John Markoff, “Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea,” *The New York Times,* (9 July 2009), retrieved from: www.nytimes.com/2009/07/technology/10cyber.html?_r=0

Hussain, Alefiya, John Heidemann, Christos Papadopoulos, “A framework for classifying denial of service attacks,” Proceedings of the SIGCOMM 2003 conference on Applications, technologies, architectures, and protocols for computer communications

Hymans, Jacques E. C., *The Psychology of Nuclear Proliferation: Identity, Emotions and Foreign Policy,* (Cambridge: Cambridge University Press: 2006)

Hymans, Jacques E.C., "Theories of Nuclear Proliferation," *The Nonproliferation Review,* 13:3 (2006): 455-465

Info Security, "Cyberwar between India and Bangladesh escalates," *Info Security,* (February 16, 2012), Retrieved from: http://www.infosecurity-magazine.com/news/cyberwar-between-india-and-bangladesh-escalates/

INFOSEC, "The Rise of Cyber Weapons and Relative Impact on Cyberspace," (2012, October 5), Retrieved from: http://resources.infosecinstitute.com/the-rise-of-cyber-weapons-and-relative-impact-on-cyberspace/

International Crisis Group, "Implementing the Iran Nuclear Deal: A Status Report," *Middle East Report,* 173, (2017, January 16), retrieved from: https://www.crisisgroup.org/middle-east-north-africa/gulf-and-arabian-peninsula/iran/173-implementing-iran-nuclear-deal-status-report

Ismail, Nick, "Under attack: the UK exposed to constant hostile cyber threats," *Information Age,* (2017, February 13) Retrieved from: http://www.information-age.com/uk-constant-threats-cyber-attacks-123464417/

Hymans, Jacques E.C., "Nuclear Proliferation and Non-Proliferation," *International Studies Encyclopaedia,* (2009) 5447-5466

Jang-Jaccard, Julian, and Surya Nepal, "A Survey of Emerging Threats in Cybersecurity," *Journal of Computer and System Sciences,* 80:5 (2014)973-993

Jenkins, Ryan, "Is Stuxnet Physical? Does it Matter?" *Journal of Military Ethics,* 12:1 (2013): 68-79

Jentleson, Bruce, "The Pretty Prudent Public: Post-Vietnam American Opinion on the Use of Military Force," *International Studies Quarterly,* 36:1 (1992)49-74

Jervis, Robert, *Perception and Misperception in International Politics,* (Princeton: Princeton University Press:1976)

Jervis, Robert, "War and Misperception, " *Journal of Interdisciplinary History,* 18(1988):675-700

Jo, Dong-Joon and Erik Gartzke, "Data notes for Determinants of Nuclear Weapons Proliferation," (2007), Retrieved from: http://jcr.sagepub.com/content/vol51/issue1/images/data/167/DC1/Jo&Gartzke_(Feb_07).zip

Jones, Allen, Adam Freeman, Matthew MacDonald, Rakesh Rajan, *Visual C# 2010 Recipes: A Problem-Solution Approach,* (New York: Apres: 2010)

Jorritsma-Lebbink, Annemarie, “Verhoging budget subsidieregeling demonstratie-en ontwikkelingsprojecten Joint Strike Fighter (JSF) - Nederlandse luchtvaartcluster,” Dutch House of Representatives, (1999, September 13), retrieved from: www.parlement.com

Joseph, Robert G., *Countering WMD: The Libyan Experience* (Fairfax, Virginia: National Institute Press, 2009)

Kanwal, Gurmeet, “China's Emerging Cyber War Doctrine,” *Journal of Defence Studies*, 3:3(2009)14-22

Kaplan, Fred, *Dark Territory: The Secret History of Cyber War*, (New York: Simon and Schuster: 2016)

Karri, Ramesh, Jeyavijayan Rajendran, Kurt Rosenfeld, Mark Tehranipoor, “Trustworthy hardware: Identifying and classifying hardware Trojans,” *Computer*, 43:10(2010)39-46

Kaska, Kadri, Anna-Maria Osula, Jan Stinissen, *The Cyber Defence Unit of the Estonian Defence League Legal, Policy and Organisational Analysis*, (NATO Cooperative Cyber Defence Centre of Excellence Publications: Tallinn: 2013)

Kaspersky Lab, “ A Fanny Equation: “I am your father, Stuxnet,” *Securelist*, (2015, February 17), Retrieved from: https://securelist.com/blog/research/68787/a-fanny-equation-i-am-your-father-stuxnet/

Kaspersky Lab, “Animals in the APT Farm,” *Securelist*, (2015, March 6), retrieved from: https://securelist.com/blog/research/69114/animals-in-the-apt-farm/

Kaspersky Lab, “Equation Group, Questions and Answers,” Version 1.5 (2015, February) Retrieved from: https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf

Kaspersky Lab, “Equation: The Death Star of Malware Galaxy,” (2015, February 16), retrieved from: https://securelistcom/blog/research/68750/equation-the-death-star-of-malware-galaxy/

Kaspersky Lab, “Targeted Cyberattacks Logbook.” (2016), Retrieved from: https://apt.securelist.com/

Kaspersky Lab, “Welchia - The Anti-Virus Virus?,” (2003, August 19), Retrieved from: http://www.kaspersky.com/about/news/virus/2003/Welchia_The_Anti_Virus_Virus_

Kaspersky Lab, “BlackEnergy APT Attacks in Ukraine employ spearphishing with Word documents,” *Securelist*, (2016, January 28), retrieved from: https://securelist.com/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/73440/

Kaspersky Lab, “What was that Wiper thing?,” (2012, August 29), retrieved from: https://securelist.com/blog/incidents/34088/what-was-that-wiper-thing-48/

Kaspersky Lab, “Future Risks: Be prepared: Special Report on Mitigation Strategies for Advanced Threats,” (2015, May), retrieved from: http://media.kaspersky.com/en/business-security/APT-Report.pdf?icid=en-GL:ent-gallery

Katzenstein, Peter, *Cultural Norms and National Security: Police and Military in Postwar Japan,* (Ithaca: Cornell University Press: 1996)

Katzenstein, Peter, *The Culture of National Security, Norms and Identity,* (New York: Columbia University Press: 1996)

Keck, Zachary, "South Korea Seeks Offensive Cyber Capabilities," *The Diplomat* , (2015, October 11), Retrieved from: the diplomat.com/2014/10/south-korea-seeks-offensive-cyber-capabilities

Kello, Lucas, "Cyber Disorders: Rivalry and Conflict in a Global Information Age," Presentation, International Security Program Seminar Series, Cambridge, Mass. International Security Program, Belfer Center for Science and International Affairs, Harvard Kennedy School (2012, May), Retrieved from: http://www.belfercenter.org/publication/cyber-disorders-rivalry-and-conflict-global-information-age

Kello, Lucas, "The Virtual Weapon: Dilemmas and Future Scenarios." *Politique étrangère,* 79: 4 (2014-15)

Kello, Lucas, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft", *International Security,* 38: 2 (2013)7-40

Kennedy, John F., "News Conferences 52", John F. Kennedy Presidential Library and Museum, (1963, March 21), retrieved from: https://www.jfklibrary.org/Research/Research-Aids/Ready-Reference/Press-Conferences/News-Conference-52.aspx

Keohane, Robert O., "Review: Lilliputians' Dilemmas: Small States in International Politics," *International Organization,* 23:2(1969):291-310

Kershner, Isabel, "Meir Dagan, Israeli Spymaster, Dies at 71; Disrupted Iran's Nuclear program," *The New York Times,* (2016, March 17), retrieved from: http://topics.nytimes.com/top/news/international/countriesandterritories/iran/nuclear_program/index.html?inline=nyt-classifier

Kinsella, David, "Arms Production in the Third Tier: an Analysis of Opportunity and Willingness", I*nternational Interactions,* 26:3 (2000) 253-286

Kissinger, Henry, *World Order: Reflections on the Character of Nations and the Course of History,* (London: Penguin Books: 2015)

Kissinger, Henry, *World Order: Reflections on the Character of Nations and the Course of History* (London: Penguin Books Limited, 2015)

Knake, Robert, "Internet Governance in an age of cyber insecurity, "*Council on Foreign Relations,* Council Special Report No. 56 (2010, September)

Koblentz, Gregory D., and Brian M. Mazanec, "Viral Warfare: The Security Implications: of Cyber and Biological Weapons," *Comparative Strategy,* 32:5 (2013)418-434

Kolkowicz, Roman (ed.), *Dilemmas of Nuclear Strategy* (London: Frank Cass & Co.: 1987)

Korzak, Elaine, "The 2015 GGE Report: What Next for Norms in Cyberspace?," *Lawfare*, (2015, September 23), retrieved from: https://www.lawfareblog.com/2015-gge-report-what-next-norms-cyberspace

Kozy, Adam, "Rhetoric Foreshadows Cyber Activity in the South China Sea," *Crowdstrike*, (2015, June 1), retrieved from: https://www.crowdstrike.com/blog/rhetoric-foreshadows-cyber-activity-in-the-south-china-sea/

Krause, Keith, *Arms and the State: Patterns of Military Production and Trade*, (Cambridge; Cambridge University Press: 1992)

Kroenig, Matthew, "Spreading temptation: proliferation and peaceful Nuclear Cooperation Agreements," *International Security*, 34:1 (2009): 7-41

Kroenig, Matthew, "Taking a walk on the supply side: the determinants of civilian nuclear cooperation," *Journal of Conflict Resolution*, 53:2 (2009):181:208

Kroenig, Matthew, "Exporting the Bomb: Why States Provide Sensitive Nuclear Assistance," *American Political Science Review*, 103:1 (2009): 113-133

Kroenig, Matthew, "Importing the Bomb: Sensitive Nuclear Assistance and Nuclear," *Journal of Conflict Resolution*, 53:2 (2009):161-180

Kroenig, Matthew, *Exporting the Bomb: Technology Transfer and the Spread of Nuclear Weapons*, (Ithaca, New York: Cornell University Press: 2010)

Kull, Steven, "What the Public Knows That Washington Doesn't," *Foreign Policy*, 102 (1995-1996)102-116

Kydd, Andrew, "Which Side Are You On? Bias, Credibility, and Mediation," *American Journal of Political Science*, 47:4 (2003)597-611

Kyochko, Elena, and Rajiv Pant, "Why Data Breaches Don't Hurt Stock Prices," *Harvard Business Review*, (2015, March 31), Retrieved from: https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-price

LaFrance, Adrienne, "How Much Will Today's Internet Outage Cost?," *The Atlantic*, (2016, October 21) retrieved from: http://www.theatlantic.com/technology/archive/2016/10/a-lot/505025/

Lai, Adrian, "Armed Forces set up cyber defence unit last year to prevent info leakage, hacking," *New Straits Times*, (2016, August 28) retrieved from: http://www.nst.com.my/news/2016/08/168808/armed-forces-set-cyber-defence-unit-last-year-prevent-info-leakage-hacking

Langner, Ralf, "Stuxnet: Dissecting a Cyberwarfare Weapon," *Security and Privacy*, 9:3 (2011):49-51

Langner, Ralph, “Stuxnet’s Secret Twin,” *Foreign Policy*, (2013, November 19), retrieved from: http://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/

Langner, Ralph, “To Kill a Centrifuge: A Technical Analysis of What Stuxnet’s Creators Tried to Achieve,” The Langner Group, (November 2013), retrieved from: http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf

Laohathai, Tanya,“Small and Medium-sized states in the age of uncertainty: The art of punching above's weight,” *Demos Working Paper*, (2013) retrieved from: http://www.demosservices.home.pl/www/files/Small%20and%20Medium_Tanya%20Laohathai.pdf

Larson, Eric, *Casualties and Consensus: The Historical Role of Casualties in Domestic Support for U.S. Military Operations* (Santa Monica, Calif.: RAND: 1996)

Lawrence, Paul R., and Jay W. Lorsch, ‘Differentiation and Integration in Complex Organisations’, *Administrative Science Quarterly*, 12:1 (1967), 1-47

Lee, Robert M., “Critiques of the DHS/FBI’s GRIZZLY STEPPE Report,” (2016, December 30), retrieved from: http://www.robertmlee.org/critiques-of-the-dhsfbis-grizzly-steppe-report/

Lee, Robert M., and Thomas Rid, “OMG Cyber!,” *The RUSI Journal*, 159:5 (2014) 4-12

Lee, Robert M., Michael J. Assante, and Tim Conway, “German Steel Mill Cyber Attack,” *SANS Industrial Control Systems*, (2014, December 30), retrieved from: https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf

Lee, Sook-Jong, “South Korea as New Middle Power Seeking Complex Diplomacy,” *EAI Asia Security Initiative Working Paper* (2012, September), retrieved from: https://www.eai.or.kr/data/bbs/kor_report/2012091210545762.pdf

Lei, Ya-Wen, “The Political Consequences of the Rise of the Internet: Political Beliefs and Practices of Chinese Netizens,” *Political Communication*, 28:3 (2011) 291-322

Leiner, Barry M., Vinton G. Cerf,David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff, " A Brief History of the Internet, ” *ACM SIGCOMM Computer Communication Review*, 39:5 (2009)22-31

Levine, Mike, “Russia tops list of 100 countries that could launch cyberattacks on US,” *ABC News*, (2017, May 18), Retrieved from: http://abcnews.go.com/US/russia-tops-list-100-countries-launch-cyberattacks-us/story?id=47487188;

Li, Zoe, “What we know about the Chinese army's alleged cyber spying unit, ” *CNN* (2014, May 20), retrieved from: http://edition.cnn.com/2014/05/20/world/asia/china-unit-61398/index.html

Libicki, Martin C., “Cyberspace Is Not a Warfighting Domain,” *I/S: A Journal of Law and Policy*, 8:2 (2012)321-336

Libicki, Martin C., C*onquest in Cyberspace: National Security and Information Warfare,* (Cambridge: Cambridge University Press: 2007)

Libicki, Martin C., *What Is Information Warfare?* (Washington DC., RAND Corporation, 1995)

Libicki, Martin, C*onquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007)

Libicki, Martin, *Cyberspace in Peace and War*, (Annapolis, Naval Institute Press: 2016)

Lieberman, Marvin B., "The Learning Curve, Diffusion, and Competitive Strategy," *Strategic Management Journal*, 8:5 (1987):441-452;

Lieberman, Marvin B., and David B. Montgomery, "First-Mover advantages," *Strategic Management Journal*, 9 (1988)41-58

Liff, Adam P., "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," *Journal of Strategic Studies*, 35:3(2012)

Liik, Kadri, "The 'Bronze Year' of Estonia-Russia relations," International Centre for Defence Studies, (2007), retrieved from: https://www.icds.ee/fileadmin/media/icds.ee/failid/Kadri_Liik_Bronze_Year.pdf

Lillian Ablon and Timothy Bogart, "Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits," *RAND Corporation*, (2017), retrieved from: https://www.rand.org/pubs/research_reports/RR1751.html

Limnéll, Jarno, "The cyber arms race is accelerating - what are the consequences?" *Journal of Cyber Policy*, 1:1(2016)50-60

Lin, Herb, "Developing "Loud" Cyber Weapons," *Lawfare*, (2016, September 1), retrieved from: https://www.lawfareblog.com/developing-loud-cyber-weapons

Lin, Herb, "Still More on Loud Cyber Weapons," *Lawfare*, (2016, October 19), Retrieved from: https://www.lawfareblog.com/still-more-loud-cyber-weapons

Lin, Herb, "Thinking about Nuclear and Cyber Conflict: Same Questions, Different Answers," (2015, May 15), Retrieved from: https://sipa.columbia.edu/system/files/Thinking%20about%20Nuclear%20and%20Cyber%20Conflict-Columbia-2015-05-14.pdf

Lin, Herbert S., "Escalation Dynamics and Conflict Termination in Cyberspace," *Strategic Studies Quarterly*, 6:3 (2012)46-70

Lin, Herbert, "Attribution of Malicious Cyber Incidents: From Soup to Nuts", *Aegis Paper Series on National Security, Technology, and Law*, (2016, September 2) Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2835719

Lin, Herbert, "Oft-Neglected Cost Drivers of Cyber Weapons," *Council on Foreign Relations: Net Politics,* (2016, December 14), retrieved from: https://www.cfr.org/blog/oft-neglected-cost-drivers-cyber-weapons

Lindsay, Jon R., "Espionage and Cybercrime" in Jon R. Lindsay, Tai Ming Cheung, Derek S. Reveron (Eds.), *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain,* (Oxford: Oxford University Press: 2015)

Lindsay, Jon R., "Exaggerating the Chinese Cyber Threat," Harvard University, Belfer Center for Science and International Affairs, *Policy Brief,* (2015, May)

Lindsay, Jon R., "Stuxnet and the Limits of Cyber Warfare," *Security Studies,* 22:3 (2013) 365-404

Lindsay, Jon R., "The Impact of China on Cybersecurity: Fiction and Friction," *International Security,* 39:3 (2014/2015):7-47

Litwak, Robert S., and Meg King, "Arms Control in Cyberspace?" (2015, November 2), retrieved from; https://www.wilsoncenter.org/publication/arms-control-cyberspace

Loundy, David,"Is Your T-Shirt a Lethal Weapon?" *America Online,* (1996, May) retrieved from: http://www.loundy.com/Roadside_T-Shirt.html

Long, Austin, "A cyber SIOP? Operational consideration for strategic offensive cyber planning," *Journal of Cybersecurity,* 3:1 (2017), 19-28

Lovelace, Mary, Jichan Chong, Marcos Figueiredo Jr, Curtis Neal, Gabor Penzes, Naren Rajasingam, Joe Roa, Alexander Saupp, John Sing, Shradha Nayak Thakare, Mladen Vukoje, "Chapter 6: Networking considerations," in *IBM Redbook: SONAS Concepts, Architecture, and Planning Guide,* retrieved from: http://www.redbooks.ibm.com/redbooks/SG247963/wwhelp/wwhimpl/js/html/wwhelp.htm

Lutz, Dieter S., "A Counterforce/Countervalue Scenario - or How Much Destructive Capability is Enough?", *Journal of Peace Research,* 20:1 (1983)

Mearsheimer, John J., *The Tragedy of Great Power Politics,* (New York: W.W. Norton & Company: 2001)

Magnusson, Peter and David J. Boggs, "Order-of-Entry Effects for Service Firms in Developing Markets: An Examination of Multinational Advertising Agencies*," Journal of International Marketing,* 17:2 (2009)23-41

Mansfield-Devine, Steve, "Estonia: What Doesn't Kill you Makes you Stronger," *Network Security,* 7 (2012):12-20

March, James G., and Johan P. Olsen, "*Democratic Governance,"* (New York: Free Press: 1995)

Marks, Paul, "Dot-dash-diss: The gentleman hacker's 1903 lulz," *New Scientists,* (2011, December 20), Retrieved from: https://www.newscientist.com/article/mg21228440-700-dot-dash-diss-the-gentleman-hackers-1903-lulz/?full=true

Martin C. Libicki, *Cyberdeterrence and Cyberwar*, (Santa Monica, CA: RAND: 2009)

Martin C. Libicki, Lillian Ablon, Tim Web, "The Defender's Dilemma: Charting a Course Toward Cybersecurity," *RAND Publication*, (2015) Retrieved from: http://www.rand.org/content/dam/rand/pubs/research_reports/RR1000/RR1024/RAND_RR1024.pdf

Mattis, James N., and Frank G. Hoffman, "Future Warfare: The Rise of Hybrid Warfare," *Naval Institute Proceedings*, (2005, November)

Maurer, Tim "'Proxies' and Cyberspace", *Journal Conflict Security Law*, 21:3(2016) 383-403

Maurer, Tim, "'Proxies' and Cyberspace," *Journal of Conflict & Security Law*, 21:3 (2016) 383-403

Maurer, Tim, "Cyber Norm Emergence at the United Nations: An Analysis of the UN's Activities Regarding Cyber-security?," *Discussion Paper*, (September 2011)

Maurer, Tim, "Cyber Proxies and the Crisis in the Ukraine," in Kenneth Geers (ed.), in Kenneth Geers (Ed.), *Cyber War in Perspective: Russian Aggression against Ukraine*, (Tallinn: NATO CCD COE Publications: 2015)

Maurer, Tim, "Cybersecurity in a Complex Environment: Transatlantic Divergences and Diplomatic Achievements", (2016) retrieved from: http://www.dgvn.de/fileadmin/publications/PDFs/Zeitschrift_VN/VN_2016/Heft_2_2016/Maurer_Cyberraum_VN_2_16_engl_web.pdf

Maurer, Tim, "Hackers for hire: Cyber-mercenary industry grows worldwide," *IHS Jane's Intelligence Review*, (2015, September)

Maurer, Tim, "The Case for Cyberwarfare," *Foreign Policy*, (2011, October 19) retrieved from: http://foreignpolicy.com/2011/10/19/the-case-for-cyberwarfare/

Maurer, Tim, and Jason Healey, "What It'll Take to Forge Peace in Cyberspace," (2017, March 20), *Christian Science Monitor*, retrieved from: http://carnegieendowment.org/2017/03/20/what-it-ll-take-to-forge-peace-in-cyberspace-pub-68351

McAfee, "Ten Days of Rain Expert analysis of distributed denial-of-service attacks targeting South Korea," *White Paper*, Retrieved from: https://www.mcafee.com/us/resources/white-papers/wp-10-days-of-rain.pdf

McAllister, Neil, "Bruce Schneier: 'We're in early years of a cyber arms race'," *The Register*, (2015) pp.1-4

McConnell, Mike, "Cyberwar is the New Atomic Age," *New Perspectives Quarterly*, 26:3 (2009):72-77

McDonald, Geoff, Liam O Murchu, Stephen Doherty, Eric Chien, "Stuxnet 0.5: The Missing Link," *Symantec*, (2013, February 26), retrieved from:

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/stuxnet_0_5_the_missing_link.pdf

McGraw, Gary, "Cyber War is Inevitable (Unless We Build Security In)"*Journal of Strategic Studies,* 36:1 (2013)109-119

McKay, Angela, Paul Nicholas, Jan Neutze and Kevin Sullivan, "International Cybersecurity Norms: Reducing Conflict in an Internet-dependent World," (2014, December), *Microsoft WhitePaper*, retrieved from: https://blogs.microsoft.com/cybertrust/2014/12/03/proposed-cybersecurity-norms/

McReynolds, Joe, "China's Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy," *China Brief,* 15:8 (2015).

McWilliams, Brian, "North Korea's School for hackers," (2003, June 2), *Wired,* retrieved from: https://www.wired.com/2003/06/north-koreas-school-for-hackers/

Menn, Joseph, "Special Report: U.S. cyberwar strategy stokes fear of blowback," *Reuters,* (2013) Retrieved from: http://www.reuters.com/article/2013/05/10/us-usa-cyberweapons-specialreport-idUSBRE9490EL20130510

Meyer, Stephen M., *The Dynamics of Nuclear Proliferation,* (Chicago: The University of Chicago Press: 1984)

Mill, John Stuart, "Considerations on Representative Government", in John Robson (ed.), *Collected Works XIX, ,* (Toronto: Routledge, Kegan and Paul: 1977)

Miller, Robert L., and John D. Brewer, *The A-Z of Social Research: a dictionary of key social science research concepts,* (London: Sage: 2003)

Ministry of Defence of the Republic of Kazakhstan, "Military doctrine", (2009), retrieved from: http://mod.gov.kz/mod-en/index.php/2009-06-26-02-25-27.

Ministry of Defence, "Cyber Command," (2016), retrieved from: www.defensie.nl/onderwerpen/cyber-security/inhoud/cyber-commando

Ministry of Defense, "Opniew extra geld voor Defensie in 2016", *Defensiekrant,* (2015, January 18), Retrieved from: https://magazines.defensie.nl/defensiekrant/2015/18/01-prinsjesdag

Ministry of Defense, "Voortgangsrapportage uitvoering Defensie Cyber Strategie," *Dutch House of Representatives,* (2016, March 15)

Ministry of Economic Affairs, "Subsidieregeling demonstratie-en technologie-ontwikkelingsprojecten Joint Strike Fighter - Nederlandse luchtvaartcluster,"(1998, December 14), retrieved from: http://wetten.overheid.nl/BWBR0010265/2002-11-16

Mirkovic, Jelena, D-WARD: Source-End Defense Against Distributed Denial-of-Service Attacks, *PhD Manuscript*, retrieved from: http://ieeexplore.ieee.org/abstract/document/1510618/?reload=true

Mjolsnes, Stig F., *A Multidisciplinary Introduction to Information Security*, (CRC Press: London: 2011)

Montgomery Alexander H., and Scott D. Sagan, "The Perils of Predicting Proliferation, " *Journal of Conflict Resolution,* 53:2(2009) 302-328

Moore, Gordon E., "Cramming More Components onto Integrated Circuits," *Electronics Magazine,* 38:8(1965)

Moore, Gordon E., "Lithography and the Future of Moore's Law," *Proceedings of SPIE*, 24:37(1995).

Moran, Ned, Mike Scott, Mike Oppenheim, Joshua Homan, "Operation Double Tap," *FireEye*, (2014, November 21), retrieved from: https://www.fireeye.com/blog/threat-research/2014/11/operation_doubletap.html

Morgus, Rob, "WhoDunnit? Russia and Coercion through Cyberspace," *War on the Rocks*, (2016, October 19), retrieved from: http://warontherocks.com/2016/10/whodunnit-russia-and-coercion-through-cyberspace/

Morozov, Evgeny, "The Internet," *Foreign Policy,* 179 (2010), 40-44

Moravcsik, Andrew, "Taking Preferences Seriously: A Liberal Theory of International Politics," *International Organization,* 51:4(1997) 513-553

Most Benjamin A., and Harvey Starr, *Inquiry, Logic and International Politics*, (Columbia: University of South Carolina Press: 1989).

Mueller, Dennis C., "First-mover advantage and path dependence, " *International Journal of Industrial Organization,* 15:6 (1997) 827-850

Mathew, S., R. Giomundo, S Upadyaya, M. Sudit, and A. Stotz, "Understanding Multistage Attacks by Attack-Track based Visualization of Heterogeneous Event Streams" VizSEC '06, *Proceedings of the 3rd international workshop on Visualization for computer security* (2016)1-6

Munro, Kate, "Deconstructing Flame: the limitations of traditional defences," *Computer Fraud & Security,* 10 (2012): 8-11

Musil, Steven, "Anonymous targets Israel in another cyberattack," *CNet*, (2013, April 7), retrieved from: http://www.cnet.com/news/anonymous-targets-israel-in-another-cyberattack/

Musil, Steven, "Pre-emptive cyberattack defense possible, Panetta warns," *CNET* (2012, October 11), Retrieved from: http://www.cnet.com/news/pre-emptive-cyberattack-defense-possible-panetta-warns/

Nakashima, Ellen, "Cyber-intruder sparks response, debate," *The Washington Post*, (2011, December 8) , Retrieved from: https://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html

NATO, “Afghan Managers Train in Cyber Defence”, (2012, May 21), retrieved from: http://www.nato.int/cps/en/natohq/news_86990.htm?selectedLocale=en

Neil Cukier, Kenneth, and Viktor Mayer Schoenberger, and Lewis M. Branscomb, "Ensuring (and Insuring?) Critical Information Infrastructure Protection," *Working Paper, John F. Kennedy School of Government, Harvard University,* (2005, October 11).

Nicholas, Paul, “Keynote on Defending the Core,” 9th *International Conference on Cyber Conflict*, Tallinn, Estonia (2017, May 30- June 2)

Nissenbaum, Helen, “Where Computer Security Meets National Security*,” Ethics and Information Technology*, 7, 2(2005): 61-73

Novetta, “Operation Blockbuster: Unravelling the Long Thread of the Sony Attack,” (2014, December 4), retrieved from: www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf

NSA, “Iran - Current Topics, Interaction with GCHQ,” (2013 April 12), Retrieved from: https://www.eff.org/files/2015/02/21/20150210-intercept-iran_current_topics_-_interactions_with_gchq.pdf

Nuclear Threat Initiative, “Libya Nuclear Chronology,” (2011, February), retrieved from: http://www.nti.org/media/pdfs/libya_nuclear.pdf?_=1316466791

Nuclear Threat Initiative, “Libya Nuclear Chronology”; International Atomic Energy Agency, “Additional Protocol. What is the Additional Protocol?,” retrieved from: https://www.iaea.org/safeguards/safeguards-legal-framework/additional-protocol

Nuti, Leopoldo, “‘Me Too, Please’: Italy and the Politics of Nuclear Weapons, 1945-1975,” *Diplomacy and Statecraft,* 4:1(1993)114-148, p.136

Nye Jr., Joseph S., “Cyber Power,” *Belfer Center for Science and International Affairs*, (2010, May), retrieved from: http://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf

Nye Jr., Joseph S., “Nuclear Lessons for Cyber Security?” *Strategic Studies Quarterly*, 5:4 (Winter, 2011): 18-33

Nye Jr., Joseph S., “The Regime Complex for Managing Global Cyber Activities,” *Global Commission on Internet Governance Paper Series*, 1 (2014), retrieved from: https://www.cigionline.org/publications/regime-complex-managing-global-cyber-activities

Nye Jr., Joseph S.,“The world needs new norms on cyber warfare,” *Washington Post*, (2015, October 1), retrieved from: https://www.washingtonpost.com/opinions/the-world-needs-an-arms-control-treaty-for-cybersecurity/2015/10/01/20c3e970-66dd-11e5-9223-70cb36460919_story.html?utm_term=.706e47420fde

Nye Jr., Joseph S., “Transformational Leadership and U.S. Grand Strategy,” *Foreign Affairs*, 85(2006):139.

Obama, Barack "Taking the Cyberattack Threat Seriously," *Wall Street Journal, (*2012, July 19) retrieved from: https://www.wsj.com/articles/SB10000872396390444330904577535492693044650

Ogheneovo, Edward E., "On the Relationship between Software Complexity and Maintenance Costs. Journal of Computer and Communications," *Journal of Computer and Communications*, 2 (2014)1-16

Oleg Demidov and Maxim Simonenko, "Flame in Cyberspace," *Security Index: A Russian Journal on International Security*, 19:1 (2013); 69-72

Olmstead, Kenneth, and Aaron Smith, "What the Public Knows About Cybersecurity," *Pew Research Center*, (2017, March 22), retrieved from: http://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/

Onuf, Nicholas, *World of Our Making: Rules and Rule in International Relations*, (Columbia: University of South Carolina Press: 1989)

Onuf, Nicholas, "Rule and Rules in International Relations," Erik Castrén Institute of International Law and Human Rights University of Helsinki, (2014, April 24), retrieved from: http://www.helsinki.fi/eci/Events/Nicholas%20Onuf_Rule%20and%20Rules%20%204-2-14.pdf

Open Secrets, "Lobbying Database," retrieved from: https://www.opensecrets.org/lobby/lookup.php

Orbán, Viktor, *National cyber security strategy of Hungary*, (2013) retrieved from: https://ccdcoe.org/strategies-policies.html2;.

Ottis, Rain, "Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective," *Proceedings of the 7th European Conference on Information Warfare and Security* (Plymouth: Academic Publishing Limited: 2008), pp 163-168

Owens, William A., Kenneth W. Dam, and Herbert S. Lin (Eds.), "Excerpts from Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities," Committee on Offensive Information Warfare, *National Research Council*, (2009)

Oxford English Dictionary, W*eapon,* (Oxford: Oxford University Press, 2011)

Paganini, Pierluigi, "Dino Malware that targeting Iran belong to Animal Farm's arsenal," *Security Affairs*, (2015, July 1), retrieved from: http://securityaffairs.co/wordpress/38204/cyber-crime/dino-malware-animal-farm.html

Page, Bob, "A Report of the Internet Worm," (1988, November 7). Retrieved from: http://www.ee.ryerson.ca/~elf/hack/iworm.html

Paletta, Damian, Danny Yadron and Jennifer Valentino-DeVries, "Cyberwar Ignites a New Arms Race," *The Wall Street Journal*, (2015, October 11), retrieved from: https://www.wsj.com/articles/cyberwar-ignites-a-new-arms-race-1444611128

Panetta, Leon E., "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City, " *News Manuscript U.S Department of Defense*, (2012, October) Retrieved from: http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

Patterson Manson III, George, "Cyberwar: The United States and China Prepare For the Next Generation of Conflict," *Comparative Strategy*, 30:2(2011)121-133, p. 121;

Paulo, Shakarian, "The 2008 Russian Cyber Campaign Against Georgia," *Military Review*, (2011, November-December)

Peritz, Aki J., and Michael Sechrist, "Protecting Cyberspace and the US National 3 Interest," *Discussion Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School*, (2010, September)

Perlorth, Nicole, "Hunting for Syrian Hackers' Chain of Command," *The New York Times*, (2013, May 17), retrieved from: http://www.nytimes.com/2013/05/18/technology/financial-times-site-is-hacked.html?pagewanted=all&_r=0

Persson, Michael, "Cybersoldaten klaargestoomd voor de aanval," *De Volkskrant*, (2014, September 26), retrieved from: http://www.volkskrant.nl/binnenland/cybersoldaten-klaargestoomd-voor-de-aanval~a3755316/

Peterson, Andrea, "Yes, terrorists could have hacked Dick Cheney's heart", *The Washington Post*, (2013, October 21), Retrieved from: https://www.washingtonpost.com/news/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheneys-heart/?utm_term=.ea14d571e5fc

Pheonix TS, "The Iranian Cyber Threat ," (2013, September 12), Retrieved from: https://phoenixts.com/blog/the-iranian-cyber-threat-part-1-irans-total-cyber-structure/

Pike, John, Charles Vick, Mirko Jacubowski, and Patrick Garrett, "R-7 - SS-6 SAPWOOD", (2000, July 29), retrieved from: https://fas.org/nuke/guide/russia/icbm/r-7.htm

Polanyi, Michael, *The Tacit Dimension*, (London: Routledge: 1967)

Pollack, Jonathan D., *No Exit: North Korea, Nuclear Weapons, and International Security*, (Abingdon, United Kingdom: Routledge, 2011)

Porche III, Isaac R., Christopher Paul, Michael York, Chad C. Serena, Jerry M. Sollinger, Elliot Axelband, Endy Y. Min, Bruce J. Held, *Redefining Information Warfare Boundaries for an Army in a Wireless World*, (Santa Monica, CA: RAND: 2013)

President's Commission on Critical Infrastructures, "Infrastructure Protection, Critical Foundations: Protecting America's: The Report of the President's Commission on Critical Infrastructure Protection," (1997, October 13), Retrieved from: https://www.fas.org/sgp/library/pccip.pdf

PTI, "World facing 'bloodless' cyber war threat: Modi," *The Hindu*, (2016, April 1) retrieved from: http://www.thehindu.com/news/national/world-facing-bloodless-cyber-war-threat-modi/article7375190.ece

Quester, George H., *Offensive and defense in the international system,* (New York: John Wiley: 1977)

Quester, George H., *The Politics of Nuclear Proliferation,* (Baltimore: Johns Hopkins University Press, 1973), p. 167-187.

Radianti, Jaziar, and Jose. J. Gonzalez, "Understanding Hidden Information Security Threats: The Vulnerability Black Market," Proceedings of the 40th Hawaii International Conference on System Sciences (2007)

Ramsay, Kristopher, "Politics at the Water's Edge: Crisis Bargaining and Electoral Competition," *Journal of Conflict Resolution,* 48, (2004)459-86.

Reardon, Robert, and Nazli Choucri, "The Role of Cyberspace in International Relations: A View of the Literature," Presented at the 2012 ISA Annual Convention, San Diego, (2012, April 1)

Rees, John C., "A Re-Reading of Mill On Liberty", in John Gray and G.W. Smith (eds.), *J. S. Mill On Liberty in Focus,* (London: Routledge: 1996)

Reeve, Tom, "France unveils cyber command in response to 'new era in warfare' ," *SC magazine,* (2016, December 16), retrieved from: https://www.scmagazineuk.com/france-unveils-cyber-command-in-response-to-new-era-in-warfare/article/579671/

Reus-Smit, Christian, "Constructivism" in Scott Burchill, Andrew Linklater, Richard Devetak, Jack Donnelly, Matthew Paterson, Christian Reus-Smit and Jacqui True (eds.), *Theories of International Relations,* (Hampshire: Palgrave Macmillan: 2009), pp. 212-236.

Rid, Thomas, "All Signs Point to Russia Being Behind the DNC Hack," *Motherboard,* (2016, July 25), retrieved from: https://motherboard.vice.com/en_us/article/all-signs-point-to-russia-being-behind-the-dnc-hack

Rid, Thomas, "Cyber War Will Not Take Place," *Journal of Strategic Studies,* 35:1 (2011): 5-32

Rid, Thomas, "Cyberwar and Peace: Hacking Can Reduce Real-World Violence," *Foreign Affairs,* (2013, November/December), retrieved from: https://ridt.co/d/rid-foreign-affairs-cyberwar.pdf

Rid, Thomas, "What War in the Fifth Domain?," *Kings of War,* (2012, August) Retrieved from: http://kingsofwar.org.uk/2012/08/what-war-in-the-fifth-domain/

Rid, Thomas, and Ben Buchanan, "Attributing cyber attacks" *Journal of Strategic Studies,* 38:1-2 (2015)4-37

Rid, Thomas, and Peter McBurney, "Cyber-Weapons," *RUSI Journal* 157:1 (2012): 6-13

Rid, Thomas, *Cyber War Will Not Take Place,* (London: C.Hurst & Co.: 2013)

Rid, Thomas, *Rise of the Machines: A Cybernetic History*, (New York: W. W. Norton & Company: 2016)

Ries, Al, and Jack Trout, "Marketing Warfare," *Journal of Consumer Marketing,* 3:4 (1986) 77-82

Rigter, Niels, "Cybercommando nu al overvraagd," *De Telegraaf*, (2017, February 16), retrieved from:http://www.telegraaf.nl/binnenland/27637681/__Commando_nu_al_overvraagd__.html

Risse, Thomas 'Let's Argue,' *International Organization*, 54 (2000) 1–41;

Robinson, Jones, and Helge Janicke, "Cyber warfare: Issues and Challenges," *Computers & Security*, 49 (2015) 70-94

Ronald, Asmus, *Little War that Changed the World. Georgia, Russia and the Future of the West*, (New York: Palgrave Macmillan: 2010)

Rosenfield, Daniel K., "Rethinking Cyber War," *Critical Review: A Journal of Politics and Society,* 21:1(2009):77-90

Ross, Alec, "Want job security? Try online security," *Wired*, (2016, April 25), retrieved from: http://www.wired.co.uk/article/job-security-cybersecurity-alec-ross

RTL Nieuws, "Hennis: grappen over 'pang pang' vernietigend," (2015, August 14), retrieved from: https://www.rtlnieuws.nl/nieuws/binnenland/hennis-grappen-over-pang-pang-vernietigend

Rufi, Antoon, "Chapter 1: Vulnerabilities, Threats, and Attacks" in *Network Security 1 and 2 Companion Guide,* (ed.) Antoon Rufi, (Cisco Networking Academy: 2006)

Russian government, "Information Security Doctrine of the Russian Federation" (200, September 9), retrieved from: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf

Sagan, Scott D., "The Causes of Nuclear Proliferation," *Current History*, (April 1997), pp. 151-156; Scott D. Sagan "Why Do States Build Nuclear Weapons?" in Victor Utgoff, ed., *The Coming Crisis: Nuclear Proliferation, U.S. Interests, and World Order* (Cambridge, MA: MIT Press:1999), p. 17-50

Sagan, Scott D., "Why Do States Build Nuclear Weapons? Three Models in Search of a Bomb," in *New Global Dangers: Changing Dimensions of International Security* (Cambridge, MA: MIT Press: 2004).

Sagan, Scott D., "The Causes of Nuclear Weapons Proliferation," *Annual Review of Political Science,* 14 (2011):225-244

Sagan, Scott D., "Two Renaissances in Nuclear Security Studies," *H-Diplo/ISSF* (15 June 2014), retrieved from: https://issforum.org/ISSF/PDF/ISSF-Forum-2.pdf

Sagan, Scott D., "Why Do States Build Nuclear Weapons? Three Models in Search of a Bomb," *International Security*, 21:3 (Winter, 1996-1997), pp. 54-86.

Sanger, David, “U.S. Decides to Retaliate Against China’s Hacking,” *The New York Times*, (2015, July 31), retrieved from: https://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html?_r=0

Sartori, Anne, "The Might of the Pen: A Reputational Theory of Communication in International Disputes," *International Organization*, 56 (2002)121-50

Sartori, Giovanni, “Concept Misinformation in Comparative Politics,” *The American Political Science Review*, 64:4 (1970): 1033-1053

Saxena, Shobhan, “Brazil, Argentina push for joint cyber shield for South America,” (November 24, 2013), retrieved from: http://www.thehindu.com/news/international/world/brazil-argentina-push-for-joint-cyber-shield-for-south-america/article5386962.ece

Saydjari, Sami, “Defending Cyberspace,” *Computer*, 35:12 (2002):125-127

SC Staff, “Yemen Cyber Army promises more attacks, but are they a front for Iran?, *SC Magazine UK*, (2015, July 22), retrieved from: https://www.scmagazineuk.com/yemen-cyber-army-promises-more-attacks-but-are-they-a-front-for-iran/article/534402/

Schachtman, Noah, “Insiders Doubt 2008 Pentago Hack Was Foreign Spy Attack,” *Wired*, (2010, August 25), retrieved from: https://www.wired.com/2010/08/insiders-doubt-2008-pentagon-hack-was-foreign-spy-attack/

Scheffer, Ulrike, “Bundeswehr startet Kommando gegen Cyberattacken,” *Der Tagesspiegel*, (2017, April 4), Retrieved from: http://www.tagesspiegel.de/politik/verteidigung-bundeswehr-startet-kommando-gegen-cyberattacken/19608528.html

Schelling, Thomas C., *Arms and Influence* (New Haven, Conn.: Yale University Press: 1966)

Schelling, Thomas C., *Strategy of Conflic*t, (Cambridge, Mass.: Harvard University Press: 1960)

Schmitt, Michael N. (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, (Cambridge: Cambridge University Press, 2013)

Schmitt, Michael N., *Tallinn Manual on the International Law Applicable to Cyber Warfare*, (New York: Cambridge University Press: 2013)

Schneier, Bruce, “Counterterrorism Mission Creep,” *Schneier on Security,* (2013, July 19), Retrieved from: https://www.schneier.com/blog/archives/2013/07/counterterroris_1.html

Schneier, Bruce, “NSA Surveillance and Mission Creep,” *Schneier on Security,*(2013, August 6) Retrieved from: https://www.schneier.com/blog/archives/2013/08/nsa_surveillanc.html

Schneier, Bruce, “Talk by the Former Head of French SIGINT,” (2016, September 7) Retrieved from: https://www.schneier.com/blog/archives/2016/09/talk_by_the_for.html

Schneier, Bruce,“Crypto-Gram”, *Schneier on Security*, (2000, September 15), retrieved from: https://www.schneier.com/crypto-gram/archives/2000/0915.html

Schramade, Krijn, "Defensiebudget historish laag," (2016, September 30),*FTM*, Retrieved from: https://www.ftm.nl/artikelen/defensiebudget-historisch-laag

Scott, James, and Drew Spaniel, "China Espionage Dynasty: Economic Death by A Thousand Cuts," *Institute for Critical Infrastructure Technology,* (2016, July 28), retrieved from: http://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2016/2016.07.28.China_Espionage_Dynasty/ICIT-Brief-China-Espionage-Dynasty.pdf

Scott-Smith, Giles, and Max Smeets, "Noblesse oblige: The transatlantic security dynamic and Dutch involvement in the Joint Strike Fighter program," *International Journal,* (2012-2013)49-69

Seegers, Jules, "Leopard-tank toch verkocht, Defensie vindt in Finland alsnog koper," *NRC,* (201, December 19), retrieved from: ww.nrc.nl/nieuws/2013/12/19/leopard-tank-toch-verkocht-defensie-vindt-in-finland-alsnog-koper-a1428711

Segal, Adam, "Retaliating Against China's Great Firewall," *Council on Foreign Relations: Net Politics,* (2015, August 3), retrieved from: https://www.cfr.org/blog-post/retaliating-against-chinas-great-firewall

Segal, Adam, "Takeaways From a Trip to the National Security Agencu," *Council on Foreign Relations: NetPolitics,* (2016, December 21), Retrieved from: https://www.cfr.org/blog-post/takeaways-trip-national-security-agency.

Segal, Adam, "Using Incentives to Shape the Zero-Day Market" *Council on Foreign Relations, Cyber Brief* (2016, September 19), retrieved from: https://www.cfr.org/report/using-incentives-shape-zero-day-market

Segura, Vincente, and Javier Laheurta, "Modelling the economic incentives of DDoS attacks: femtocell case study," (paper presented at the Workshop on the Economics of Information Security (WEIS), University College London, England, 24-25 June 2009) retrieved from: http://weis09.infosecon.net/files/113/paper113.pdf

Senior Military Cyber Commander, "The Second International Cyber Symposium: Cyberspace and the Transformation of 21st Century Warfare," *The Royal United Services Institute (RUSI),* (Church House, Westminster: London), 19-20 October 2016

Shakarian, Paulo, "Stuxnet: Cyberwar Revolution in Military Affairs," *Small Wars Journal,* (2011)

Shariat, Sheryll, Sue Mallonee, and Shelli Stephens-Stidham, "Summary Of Reportable Injuries In Oklahoma," (1998, December) retrieved from: http://web.archive.org/web/20080110063748/http://www.health.state.ok.us/PROGRAM/injury/Summary/bomb/OKCbomb.htm

Shea, Jamie, "Lecture 6 - Cyber attacks: hype or an increasing headache for open societies?," (2012, February 29), retrieved from: http://www.nato.int/cps/en/natolive/opinions_84768.htm;

Shekhar, Shashank, “The India - Pakistan cyber war intensifies as retaliatory ransomware attack cripples websites of Islamabad, Multan and Karachi airports,” *Daily Mail* (2017, January 2), retrieved from: / http://www.dailymail.co.uk/indiahome/indianews/article-4082644/The-India-Pakistan-cyber-war-intensifies-retaliatory-ransomware-attack-cripples-websites-Islamabad-Multan-Karachi-airports.html

Sherstobitoff, Ryan, Itai Liba, and James Walter, “Dissecting Operation Troy: Cyberespionage in South Korea,” McAfee, (2013, March 20), retrieved from: www.mcafee.com/it/resources/white-papers/wp-dissecting-operation-troy.pdf

Shires, James, and Max Smeets, “What do we talk about when we talk about ‘cyber’?” *SSRN: Working Paper,* (2016, October 5), retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2860839

Sharp, Travis, “Theorizing cyber coercion: the 2014 North Korean operation against Sony,” *Journal of Strategic Studies,* (2017)1-29

Shultz, George, “Preventing the Proliferation of Nuclear Weapons,” *Department of State Bulletin*, 84:2093 (1984)

Siboni, Gabi, and Sami Kronenfeld, “Iran and Cyberspace warfare,” *Military and Strategic Affairs,* 4:3 (2012)101-117

Sigh, Sonali and Christopher Way, “The Correlates of Nuclear Proliferation: a Quantitative Test,” *Journal of Conflict Resolution,* 48:6 (2004)859-885

Singer, Peter W., and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know?* (Oxford University Press: New York: 2014)

Sinpeng, Aim, “State Repression in Cyberspace: The Case of Thailand,” *Asian Politics and Policy,* 5:3 (2013): 421-440

Skorobogatov, Sergei, and Christopher Woods, “Breakthrough silicon scanning discovers backdoor in military chip,” Cryptographic Hardware and Embedded Systems Workshop, 9-12 September 2012,(Leuven), retrieved from: https://www.cl.cam.ac.uk/~sps32/ches2012-backdoor.pdf

Slovak Republic “Slovak Republic, Cyber Security Concept of the Slovak Republic for 2015 - 2020,” retrieved from: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1

Smeets, Max “A Matter of Time: On the Transitory Nature of Cyberweapons,” *Journal of Strategic Studies,* (2017)1-28

Smeets, Max, “Diplomacy in Cyberspace,” Workshop Diplomatic Studies, London, Senate House, (2016)

Smeets, Max, “Organizational Integration of Offensive Cyber Capabilities: A Primer on the Benefits and Risks”, in Henry Roigas, Raik Jakschis, Lauri Lindstrom, and Tomáš Minarik

(Eds), *9th International Conference on Cyber Conflict* (Tallinn, NATO CCD COE Publications: 2017)

Smeets, Max, "When Naming Cyber Threat Actors Does More Harm Than Good," *Council on Foreign Relations: NetPolitics*, (2016, October 24), retrieved from: https://www.cfr.org/blog/when-naming-cyber-threat-actors-does-more-harm-good

Smith, David J., "How Russia Harnesses Cyberwarfare," *American Foreign Policy Council (2012, August), retrieved from:* http://www.afpc.org/files /august2012.pdf.

Solingen, Etel, "The Political Economy of Nuclear Restraint," *International Security*, 19:2 (1994):126-169.

Solingen, Etel, *Nuclear Logics: Contrasting Paths in East Asia and the Middle East*, (Princeton: Princeton University Press: 2007)

Song, JaeSeung, Cristian Cadar, and Peter Pietzuch, "SYMBEXNET: Testing Network Protocol Implementations with Symbolic Execution and Rule-Based Specifications" *IEEEE Transactions on Software Engineering*, 40:7 (2013)695-709

Sood, Par Aditya, and Richard Enbody, *Targeted Cyber Attacks: Multi-staged Attacks Driven by Exploits and Malware*, (Elsevier: Waltham: 2014)

Sputnik News, "Russia Considering Cyber Security Command," (2012, March 21), retrieved from: http://en.rian.ru/russia/20120321/172301330.html

Stevens, Tim, "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace," *Contemporary Security Policy*, 33: 1 (2012): 148-170

Stewart, William A., "Counterforce, Damage-limiting, and Deterrence," *RAND Corporation*, (1967, July), retrieved from: https://www.rand.org/content/dam/rand/pubs/papers/2008/P3385.pdf

Stewart, Phil, Diane Bartz, Jim Wolf and Jeff Mason, "Special report: Government in cyber fight but can't keep up," *Reuters*, (2011, June 17) retrieved from: http://www.reuters.com/article/us-usa-cybersecurity-idUSTRE75F4YG20110617

Stockton, Paul, and Michele Golabek-Goldman, "Curbing the Market for Cyber Weapons," *Yale Law & Policy Review*, 32:1 (2013)239-266

Stone, Jeff, "Meet the Cyber-Industrial Complex: Private contractors may get $7B windfall from Pentagon's Cyberwar on ISIS," IB Times, (2016, July 3), retrieved from: http://www.ibtimes.com/meet-cyber-industrial-complex-private-contractors-may-get-7b-windfall-pentagons-2329652

Stone, John, "Cyber War Will Take Place!," *Journal of Strategic Studies*, 36:1 (2013) 101-108

Striek, Peter, "'Meer geld? Defensie krijgt juist nog veel minder geld'" *De Volkskrant*, (2014, September 26), retrieved from: http://www.volkskrant.nl/binnenland/-meer-geld-defensie-krijgt-juist-nog-veel-minder-geld~a3755100/

Strohm, Chris, “Lockheed to Boeing Building Security-Industrial Complex,” *Bloomberg Business*, (2013, June 10), Retrieved from: https://www.bloomberg.com/news/articles/2013-06-10/lockheed-to-boeing-building-security-industrial-complex

Suchman, Mark C., and Dana P. Eyre, “Military Procurement as Rational Myth: Notes on the Social Construction of Weapons Proliferation” , *Sociological Forum*, 7:1 (1992):137-161

Sudworth, John, “New 'cyber attacks' hit S Korea,” *BBC News*, (2009, July 9), Retrieved from: http://news.bbc.co.uk/1/hi/world/asia-pacific/8142282.stm

Symantec Corporation, “Internet Security Threat Report 2014,” (2014), retrieved from: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

Symantec Security Response, “Born on the 4th of July,” *Symantec Official Blog*, (2009, July 9), retrieved from: https://www.symantec.com/connect/blogs/born-4th-july

Symantec Security Response, “The Shamoon Attacks,” *Symantec Official Blog* (2012, August 16), retrieved from: http://www.symantec.com/connect/blogs/shamoon-attacks

Symantec, “Are the 2011 and 2013 South Korean Cyberattacks Related?”, (2013, March 29), retrieved from: www.symantec.com/connect/blogs/are-2011-and-2013-south-korean-cyberattacks-related

Symantec, “Four Years of DarkSeoul Backscatters Against South Korea Continue on Anniversary of Korean War,” (2013, June 26), retrieved from: www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war

Symantec, “Internet Security Threat Report,” (2003, September), Retrieved from: http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_iv.pdf

Symantec, “W32.Blaster.Worm,” (2015) , Retrieved from: https://www.symantec.com/security_response/writeup.jsp?docid=2003-081113-0229-99

Symantec, “W32.Distrack,” (2012, August 22), retrieved from: www.symantec.com/security_response/writeup.jsp?docid=2012-081608-0202-99

Tannewald, Nina, “Stigmatizing the Bomb: Origins of the Nuclear Taboo,” *International Security*, 30:1 (2005) 5-49.

Tarakanov, Dimitry, “Shamoon The Wiper: Further Details,” (2012, September 11), retrieved from https://securelist.com/blog/incidents/57784/shamoon-the-wiper-further-details-part-ii/

Tarakanov, Dmitry, “Shamoon The Wiper: further details (Part II),” *SecureList*, (2012, September 11), retrieved from: https://securelist.com/shamoon-the-wiper-further-details-part-ii/57784/

TEDx Talks, “The shape-shifting skulls of dinosaurs | Jack Horner | TEDxVancouver,” *YouTube*, (2011, April 13) retrieved from: https://www.youtube.com/watch?v=xYbMXzBwpIo

Thales, “Thales to build “Cyber Range” , a Cybersecurity Training and Testing Facility for the Dutch Defence Cyber Command,” (2016, May 18), retrieved from: https://www.thalesgroup.com/sites/default/files/asset/document/pr_thales_to_build_cyber_range_a_cybersecurity_training_and_testing_facility_for_the_dutch_defence_cyber_command.pdf

The Danish Ministry of Defence, “Danish Defence Agreement 2013-2017”, (2012, November 30), retrieved from: http://www.fmn.dk/eng/allabout/Documents/TheDanishDefenceAgrement2013-2017english-version.pdf

The Economist, “Hiring digital 007s,” (2013, June 15), retrieved from: http://www.economist.com/news/business/21579465-new-cyber-industrial-complex-rising-should-you-worry-hiring-digital-007s

The National Cyber Security Strategies of the NATO member states can be found at the website of the NATO Cooperative Cyber Defence Centre of Excellence: https://ccdcoe.org/strategies-policies.html

The News, “India, Pakistan cyber war intensifies,” (2017, January 4), retrieved from: https://www.thenews.com.pk/print/176619-India-Pakistan-cyber-war-intensifies

The White House, “Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure” (2009), retrieved from: https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf

The White House, “FACT SHEET: Cybersecurity National Action Plan,” (2016, February) Retrieved from: http://sitsd.mt.gov/Portals/77/docs/MT-ISAC/2016/2016%2002%2018/CNAP.pdf?ver=2016-02-16-093003-710

The White House, “Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment”, *Office of the Press Secretary*, (2016, December 29), retrieved from: https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity

The White House, “The Clinton Administration’s Policy on Critical Infrastructure Protection: Presidential Decision Directive,” *White Paper,* 63 (1998, May 22), retrieved from: www.fas.org/irp/offdocs/paper598.htm

The White House, “The Comprehensive National Cybersecurity Initiative,” (2014, February), retrieved from: http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative

The White House, “The National Strategy to Secure Cyberspace,” (February, 2003), retrieved from: www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

Thiels, Christian, “Mit Nerds in den Krieg,” *Tagesschau,* (2016, April 26), retrieved from: https://www.tagesschau.de/inland/cyber-bundeswehr-101.html

Thies, Wallace J., "Compellence Failure or Coercive Success? The Case of NATO and Yugoslavia," *Comparative Strategy,* 22:3 (2003)243-267

Thomas, Bindiya, "UAE Military To Set Up Cyber Command," *Defense World,* (2014, September 30), retrieved from: http://www.defenseworld.net/news/11185/UAE_Military_To_Set_Up_Cyber_Command#.WXIfz4jyiUk

Threat Connect, "A Tale of Two Targets,"(2016, October 17), retrieved from:Threatconnect.com/blog/threatconnect-discovers-chinese-apt-activity-in-europe/https://www.crowdstrike.com/blog/rhetoric-foreshadows-cyber-activity-in-the-south-china-sea/

Thyne, Clayon L., "Cheap Signals with Costly Consequences: The Effect of Interstate Relations on Civil War," *Journal of Conflict Resolution,* 50:6 (2006)937-961

Tobey, William H., "A Message from Tripoli: How Libya Gave Up Its WMD," *Bulletin of the Atomic Scientists,* Online Analysis, (2014, December)

Tow, William T., "The nuclear Waltz: Rational actors, deterrence and nuclear non-proliferation", *Australian Journal of Political Science,* 49:3 (2014)541-546

Trivitt, Bill, "The Evolution of APTs (Advanced Persistent Threats)," *Information System Security Association,* retrieved from: http://kern.issa.org/wp-content/uploads/2013/08/The-Evolution-of-APTsv1_2.pdf

Tsipenyuk, Katrina, Brian Chess, Gary McGraw, "Seven pernicious kingdoms: A taxonomy of software security errors," *Security and Privacy,* 3:6 (2005)81-84

Tsyrklevich, Vlad, "Hacking Team: a zero-day market case study," (2015, July 22), retrieved from: https://tsyrklevich.net/2015/07/22/hacking-team-0day-market/

Tulpule, Shruti, "Are we headed towards Web War I?," *International Journal of Law and Legal Jurisprudence Studies,* 1:7 (2014)

U.S. Air Force, "Air Force Doctrine Document 1-2" (2007, January 11), Retrieved from: http://www.globalsecurity.org/military/library/policy/usaf/afdd/1-2/afdd1-2-2007.pdf

US Cyber Command, "Cybercom Fragord 01 to taskord 16-0063 to Establish Joint Task Force (JST-ARES to Counter the Islamic State of Iraq and the Levant (ISIL) in Cyber Space," (2016, May 5), retrieved from: http://nsarchive.gwu.edu/dc.html?doc=3678213-Document-07-USCYBERCOM-to-CDRUSACYBER-Subj

U.S. Cyber Consequences Unit (US-CCU), "Overview by the US-CCU of the Cyber Campaign against Georgia in August 2008," *Special Report, US-CCU,* (2009, August), retrieved from: http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf.

U.S. Government, "The F-35 Lightning II", Retrieved from: http://www.jsf.mil/

UK government, “Britain’s cyber security bolstered by world-class strategy,” (2016, November 1), retrieved from: https://www.gov.uk/government/news/britains-cyber-security-bolstered-by-world-class-strategy

UK Parliament, “Russia: Implications for UK defence and security,” (2016, June 30), retrieved from: https://www.publications.parliament.uk/pa/cm201617/cmselect/cmdfence/107/10710.htm

United Nations Institute for Disarmament Research (UNIDIR), “The Cyber Index International Security Trends and Realities,” (2013), retrieved from: http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

Unknown Author, “Iran denies Stuxnet disrupted its nuclear programme,” *BBC News*, (2010, November 24), retrieved from: http://www.bbc.co.uk/news/technology-11821011

Unknown author, “Tunisian cyber army Cyber attack against French websites,” *E Hacking News*, (2013, February 2), retrieved from: http://www.ehackingnews.com/2013/02/tunisian-cyber-army-cyber-attack.html

Unknown Author, “Ukraine troops on high alert as tension with Russia grows”, (2016, August 12), *BBC News*, retrieved from: http://www.bbc.co.uk/news/world-europe-37049313

US Department of Defense, “Quadrennial Defense Review Report,” Washington, D.C., (2010, February)

US Department of Homeland Security and the Federal Bureau of Investigation, “GRIZZLY STEPPE - Russian Malicious Cyber Activity,” *Joint Analysis Report*, (2016, December 29), retrieved from: https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

Valentino-Devries, Jennifer, and Danny Yadron, “Cataloging the World’s Cyberforces,” *Wall Street Journal* (2015, October 11), retrieved from: http://graphics.wsj.com/world-catalogue-cyberwar-tools/

Valeriano, Brandon, and Anthony Craig, “Conceptualising Cyber Arms Races,” in Nikolaos Pissanidis, Henry Rõigas, Matthijs Veenendaal (Eds.), *8th International Conference on Cyber Conflict Cyber Power* (Tallinn: NATO CCD COE Publications: 2016)

Valeriano, Brandon, and Ryan Maness, “The dynamics of cyber conflict between rival antagonists, 2001-2011,” *Journal of Peace Research*, 51:3 (2014)347-360.

Van Camp, Jeffrey “HP Wants to Sell its PC Business, Kill Webos: so What Happens Now?,” Digital Trends, (August, 2011) Retrieved from: http://www.digitaltrends.com/mobile/hp-wants-to-sell-its-pc-business-kill-webos-so-what-happens-now/

Verizon, “Data Breach Investigations Report,” (2015), retrieved from: https://iapp.org/media/pdf/resource_center/Verizon_data-breach-investigation-report-2015.pdf

Volpe, Tristan A., "Proliferation Persuasion: Coercive Bargaining with Nuclear Technology," *PhD Dissertation*, George Washington University, (2015, May), retrieved from: https://e-reports-ext.llnl.gov/pdf/788895.pdf

Walt, Stephen M., "Is the Cyber Threat Overblown?,"*Foreign Policy*, (March 30, 2010), retrieved from: http://walt.foreignpolicy.com/posts/2010/03/30/is_the_cyber_threat_overblown

Walt, Stephen, *The Origin of Alliances*, (Ithaca, NY: Cornell University Press: 1987)

Waltz, Kenneth, "Nuclear myths and political realities," *American Political Science Review*, 84, (1990)731-45.

Waltz, Kenneth, *Man, the State and War*, (New York: Columbia University Press, 1959).

Waltz, Kenneth, *A Theory of International Politics*, (New York: McGraw-Hill: 1979).

Waqas, "Armenian Hackers Leak Azerbaijani Banking and Military Data," (2016) Retrieved from: https://www.hackread.com/armenian-hackers-leak-azeri-banking-military-data/

Ward, Dan, and Robert Morgus, "Professor Cy Burr's Graphic Guide to: International Cyber Norms," *New America: Cyber Security Initiative* (2016, November), Retrieved from: https://na-production.s3.amazonaws.com/documents/CyberNorms11.14.pdf

Warf, Barney, and John Grimes, "Counterhegemonic Discourses and the Internet," *Geographical Review*, 87:2 (1997) 259-274

Warner, Michael, "Cybersecurity: A Pre-history, Intelligence and National Security*", Intelligence and National Security*, 27:5 (2012)781-799

Warwick Ashford, "UK and US collaborating on cyber weapons, says Snowden," *Computer Weekly*, (2013, August 2) retrieved from: http://www.computerweekly.com/news/2240202997/UK-and-US-collaborating-on-cyber-weapons-says-Snowden

Washington Post, "The U.S. Government and Cybersecurity", (2003, May 16), retrieved from: http://www.washingtonpost.com/wp-dyn/articles/A50606-2002Jun26.html

Weaver, Nicholas, "A Close Look at the NSA's most powerful internet attack tool," *Wired*, (2014, March 13), Retrieved from: https://www.wired.com/2014/03/quantum/

Weaver, Nicholas, and Dan Ellis, "Reflections on Witty: Analyzing the Attacker," *Security*, 29:3 (2004) 34-37

Weedon, Jen, "Beyond 'Cyber War': Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine," in Kenneth Geers (Ed.), *Cyber War in Perspective: Russian Aggression against Ukraine*, (Tallinn: NATO CCD COE Publications: 2015)

Weiner, Norbert, *Cybernetics Or Control and Communication in the Animal and the Machine*, (Cambridge: the MIT press: 1961)

Weisberger, Marcus, “Japan, U.S. to expand missile defense, cyber cooperation”, *Defense News*, (2011, June 21).

Wendt, Alexander, "Anarchy is What States Make of It: the Social Construction of Power Politics," *International Organization,* 46:2 (1992)391-425

Wendt, Alexander, *Social Theory of International Politics* (Cambridge: Cambridge University Press: 1999)

WikiLeaks, “Spy Files,” retrieved from: https://wikileaks.org/spyfiles/

William Gibson, *Neuromancer*, (New York: Ace: 1984); 51-67

Yadron, Danny, “Ex-NSA Chief’s Cybersecurity Startup Draws Funding,” *The Wall Street Journal*, (2015, October 25), retrieved from: www.wsj.com/articles/ex-nsa-chiefs-cybersecurity-startup-draws-funding-1445819345

Yould, Rachel, “Beyond the American Fortress: Understanding Homeland Security in the Information Age.” In *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*, ed. Robert Latham. (The New Press, 2003)

Youtube, “Espionnage et cybersécurité, Bernard Barbier reçu par Symposium CentraleSupélec,” (2016, September 5), retrieved from: https://www.youtube.com/watch?v=s8gCaySejr4

YouTube, “Hackers Testifying at the United States Senate, May 19, 1998 (L0pht Heavy Industries),” retrieved from: https://www.youtube.com/watch?v=VVJldn_MmMY

Zetter, Kim, “Everything We Know About Ukraine’s Power Plant Hack,” *Wired,* (2016, January 20), Retrieved from: https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/

Zetter, Kim, “Hacking Team Leak Shows how Secretive Zero-day expoit sales work,” *Wired*, (2015, July 24), retrieved from: https://www.wired.com/2015/07/hacking-team-leak-shows-secretive-zero-day-exploit-sales-work.

Zetter, Kim, “How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History,” *Wired*, (201, November 7) retrieved from: https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/

Zetter, Kim, “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid,” *Wired,* (2016, March 3), retrieved from: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

Zetter, Kim, “Qatari Gas Company Hit with Virus in Wave of Attacks on Energy Companies,” *Wired,* (2012, August 30) Retrieved from: http://www.wired.com/2012/08/hack-attack-strikes-rasgas/

Zetter, Kim, “Suite of Sophisticated Nation-State attack tools found with connection to Stuxnet,” *Wired,* (2015), retrieved rom: www.wired.com/201502/kaspersky-discovers-equation-group/

Zetter, Kim, “We’re at Cyberwar: A global Guide to Nation-state Digital attacks,” *Wired*, (2015, September 1), retrieved from: https://www.wired.com/2015/09/cyberwar-global-guide-nation-state-digital-attacks/

Zetter, Kim, “Wiper Malware that Hit Iran left Possible Clues of its Origins,” *Wired*, (2012, August 29), retrieved from: https://www.wired.com/2012/08/wiper-possible-origins/

Zheng, Ye, “From Cyberwarfare to Cybersecurity in the Asia-Pacific and Beyond,” in Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (eds.), *China and Cybersecurity Espionage, Strategy, and Politics in the Digital Domain*, (Oxford: Oxford University Press: 2015)

ZimNet, “Zim gets deadly Iran Weapons to fight cyber ‘internet’ protests’” (unknown date), retrieved from: https://zimnews.net/zim-internet-computer-bill-iran-mnangagwa/