# Leveraging Information as Power: America's Pursuit of Cyber Security

**by**

**Seychelle Cushing**

B.A., Simon Fraser University, 2011

Project Submitted in Partial Fulfillment of the
Requirements for the Degree of
Master of Arts

in the
Department of Political Science
Faculty of Arts and Social Sciences



**SIMON FRASER UNIVERSITY**

**Fall 2014**

# Approval

**Name:** **Seychelle Cushing**

**Degree:** **Master of Arts (Political Science)**

**Title:** ***Leveraging Information as Power: America's Pursuit of Cyber Security***

**Examining Committee:** **Chair:** Rémi Léger
Assistant Professor

**Alexander Moens**
Senior Supervisor
Professor

**Douglas Ross**
Supervisor
Professor

**André Gerolymatos**
External Examiner
Professor
Hellenic Studies
Simon Fraser University

**Date Defended/Approved:** November 28, 2014

## Partial Copyright Licence

## Abstract

Acquiring and exploiting information is key to remaining competitive in cyberspace. Security seesaws between informational advantage and vulnerability and America, as all other cyber-powers, must consistently tip the seesaw towards the former. Optimally managing the short term vulnerabilities of a cyber advantage will best produce a long-term net gain in security for the US.

The Internet's lax architecture favours offensive over defensive information seeking. Finding and buying zero-days supplements America's security innovations to maintain a deployable cyber arsenal. Cyber deterrence is problematic so America relies on resilience to manage cyber attacks. Defence through attack absorption offers a better strategy than deterrence per se. Strategically sharing capabilities enables the United States to influence Five Eyes intelligence priorities while enabling its global cyber operations. Amassing an information advantage thus enables America to leverage information as power to enhance its net security posture.



**Keywords**: cyber security; American foreign policy; national security; cyber resilience; information seeking; The Five Eyes

## Acknowledgements

First, and foremost, I am indebted to Dr. Moens. His thoughtful critiques and questions made me push my arguments further while challenging me to become a better writer. The final project is a testament to his steadfast encouragement.

Likewise, I would like to thank Dr. Ross and Dr. Gerolymatos for their enthusiastic support and helpful feedback. Their diverse expertise pointed me towards new perspectives from which to consider my arguments. I am also grateful to my friends who let me bounce ideas off of them and who pushed me through the challenges of the past year.

Last, but not least, I would like to thank Cody for his unwavering support, encouragement, and patience. Words cannot fully express my appreciation but I hope my actions do.

# Table of Contents

Approval ..... ii
Partial Copyright Licence ..... iii
Abstract ..... iv
Acknowledgements ..... v
Table of Contents ..... vi
List of Figures ..... vii
List of Acronyms ..... viii

**Chapter 1. Introduction ..... 1**

**Chapter 2. Taking Advantage of Exploits ..... 5**
2.1. The Zero-Day Exploit ..... 6
2.2. The Vulnerabilities Market ..... 9
2.3. Use it or Lose it? ..... 12
2.4. One Attack, Multiple Vulnerabilities ..... 16
2.5. The Need for Innovation ..... 19

**Chapter 3. The Challenge of a Deterrence Strategy in Cyber ..... 23**
3.1. Deterrence as Denial ..... 24
3.2. Attribution and Active Defence ..... 25
3.3. Ambiguous Signalling ..... 29
3.4. The Problem of Unacceptable Costs ..... 31

**Chapter 4. Defence through Resilience ..... 34**
4.1. Information Extracted from Stolen Data ..... 34
4.2. Creating Defensive Obstacles ..... 36

**Chapter 5. Cyber Security through Alliance: The Case of the Five Eyes ..... 39**
5.1. Necessary Coverage ..... 40
5.2. Sharing Capabilities and Information ..... 41
5.3. Compromised from the Inside: The Problem with Insider Threats ..... 47
5.4. Maximizing the Impact of the Five Eyes ..... 51

**Chapter 6. Conclusion ..... 53**

**References ..... 56**

# List of Figures

Figure 1: The Cyber Security Seesaw ..... 3
Figure 2: The Attacker Spectrum ..... 8
Figure 3: Multiple Zero-Day Exploits ..... 18
Figure 4: Active Defence Illustration ..... 28
Figure 5: PRISM ..... 48

## List of Acronyms

| | |
|---|---|
| APT | Advanced Persistent Threat |
| CDN | Canadian Dollars |
| CSEC | Communications Security Establishment Canada |
| GBP | British Pound |
| GCHQ | Government Communications Headquarters (UK) |
| HUMINT | Human Intelligence |
| NSA | National Security Agency (USA) |
| PRISM | Planning Tool for Resource Integration, Synchronization, and Management |
| R&D | Research and development |
| SIGINT | Signals Intelligence |
| UK | United Kingdom |
| US | United States |
| USD | American Dollars |

# Chapter 1.

# Introduction

Information seeking in cyberspace is competitive – it matters which state acquires and exploits information first to advance its security interests.[1] Unlike the domains of land, sea, or air, cyberspace cannot be conquered using overwhelming power.[2] A competitive cyber advantage requires the United States (US) to consistently seek out information about its adversaries to gauge intent, action, and capabilities.[3] Cyber actions thus help prepare America for future conflicts by "identify[ing] potential threats and the best ways to defeat them" in cyberspace.[4]

The Internet was not designed for security but, rather, for accessibility.[5] States, including America, are largely dependent on cyber to support their national security and economic activities. While the Internet enhances a state's efficiency in accessing and transmitting information, it also comes with a corresponding increase in vulnerabilities.[6] Networks built around the architecture of the Internet are inherently exploitable. America

1 Joseph S. Nye, Jr., *The Future of Power* (New York: Public Affairs, 2011), 117.

2 Joseph Nye, "Nuclear Lessons for Cyber Security?," *Strategic Studies Quarterly* 5, no. 4 (2011): 20, http://www.au.af.mil/au/ssq/2011/winter/nye.pdf.

3 National Security Agency, "Signals Intelligence," *National Security Agency/Central Security Service*, September 9, 2011, http://www.nsa.gov/sigint/.

4 Frank J. Cilluffo and Sharon L. Cardash, "Cyber Domain Conflict in the 21st Century," *Journal of Diplomacy & International* Relations 14, no. 1 (2013): 46, http://web.a.ebscohost.com.proxy.lib.sfu.ca/ehost/pdfviewer/pdfviewer?sid=afc29b59-f544-41c0-9fc4-4ad4f453612%40sessionmgr4002&vid=2&hid=4201.

5 Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (2013): 375-376, DOI: 10.1080/09636412.2013.816122. See also: Nye, *Nuclear Lessons*, 21; Nye, *Future of Power*, 125.

6 Nye, *Nuclear Lessons*, 20.

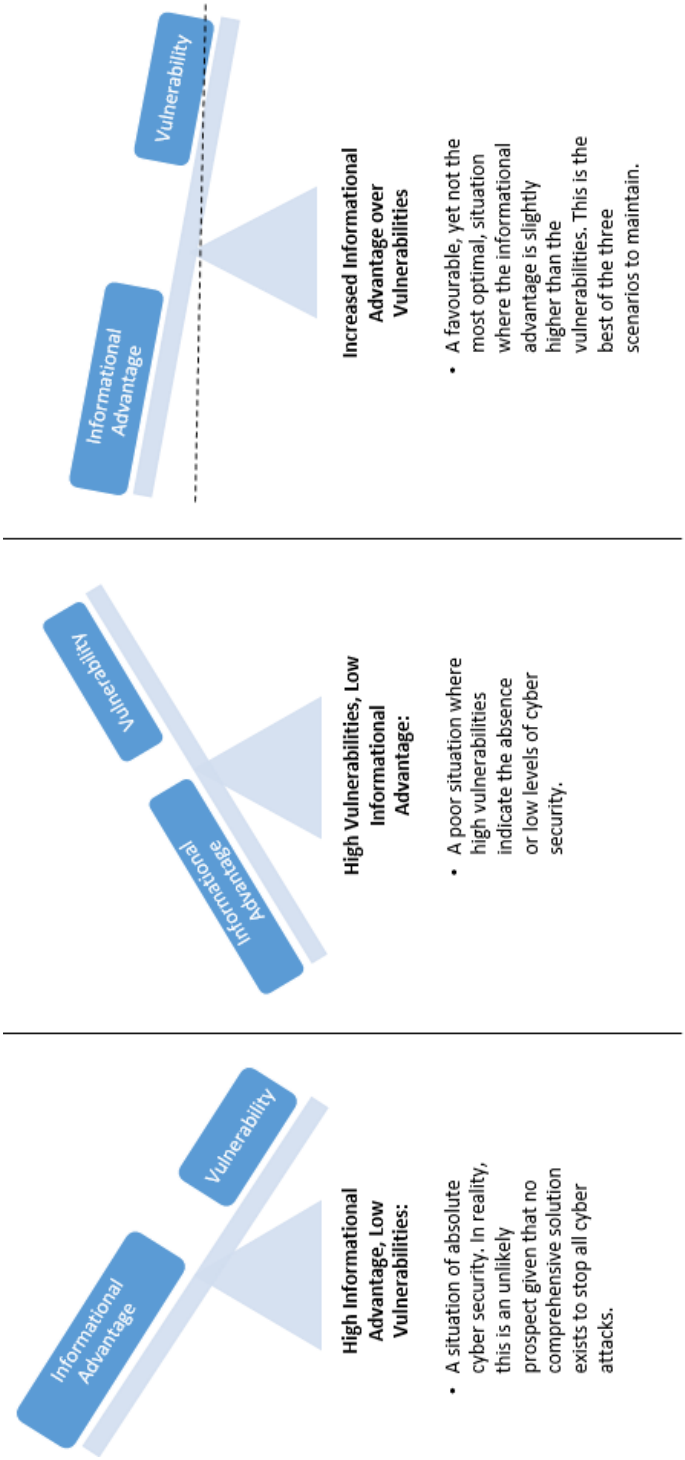
thus takes advantage of cyber's lax security architecture to seek out and extract information from its adversaries' networks[7] in innovative operations.

The once benign nature of the Internet has now given way to "a battleground, [and] a ground zero"[8] for political and military contests and conflicts. Yet, in cyber, there is no such thing as a clear-cut win – any actions undertaken can make the American security posture relatively better or worse. Security in cyberspace thus seesaws between advantage and vulnerability, as depicted below.

7 Ellen Nakashima and Joby Warrick, "For NSA chief, terrorist threat drives passion to 'collect it all,'" *The Washington Post*, July 14, 2013, http://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html.

8 Ronald J. Deibert, *Black Code: Surveillance, Privacy, and the Dark Side of the Internet* (Toronto: McClelland & Stewart, 2013), 17. Black describes the fact that so much of cyber is hidden and obscured. Responsibility for cyber is being delegated to secret national security agencies. Black Code refers to the growing influence of these agencies and the expanding network of companies they work with. See: Ibid., 7-8.

**Figure 1: The Cyber Security Seesaw**



Absolute cyber security, while desirable, is unlikely. Like the other domains of conflict, no comprehensive solution exists to ensure complete security. Conversely, a situation of high vulnerability is even more undesirable. Instead, America must constantly work to tip the security seesaw towards advantage over vulnerability. By optimally managing the short-term vulnerabilities inherent in seeking a cyber advantage, the United States can best produce a long-term net gain in security.

Using the security seesaw as a guide, this project will examine how information is acquired and leveraged in cyberspace at three levels: cyber attack, cyber strategy, and alliance relations in cyberspace. Information drives the acquisition and first-use of undetected vulnerabilities in a cyber attack. At the strategy level, a Cold War understanding of deterrence applied to cyber only creates incremental advantages. Instead, defence is acquired through resiliency by absorbing cyber strikes. In an alliance situation, America concedes part of its informational monopoly to strongly influence its allies' intelligence priorities. Initial vulnerabilities can subsequently be converted into strategic gains. Each section illustrates how the United States must constantly manipulate the security seesaw to obtain an improved security position.

# Chapter 2.

# Taking Advantage of Exploits

The core of cyber is built on code – sequences of letters, numbers, and symbols that tell a computer how to function.[9] Code is a product of human ingenuity with developers creating alphanumeric lines of code that, to a non-expert, appear to be little more than gibberish. Yet through this code, intelligence systems analyze data, fighter jets and drones strike at targets, and cyber attacks are activated.

Even with the successes of human ingenuity, code is liable to human error. Developers may miss vulnerabilities created in their code through coding errors.[10] Technology follows Moore's Law whereby every two years technology leaps forward exponentially.[11] Systems that once required a few thousand lines of code to operate now require millions of lines. Every time a change to the code is made, developers must read through millions of lines of code to check for unintended effects. The sheer volume of code creates more opportunities to unknowingly overlook these vulnerabilities. A single computer contains millions of lines of code with a number of undiscovered vulnerabilities. The vulnerabilities in one computer's code become multiplied when

9 Code can refer both to the infrastructure (electronic and physical) of cyberspace and the line of instruction that tells a computer how to act. In this instance, code refers to the lines of instruction to illustrate where vulnerabilities can be found. See: Ibid., 6.

10 Stefan Frei, *The Known Unknowns: Empirical Analysis of Publicly Unknown Security Vulnerabilities* (Austin, TX: NSS Labs, 2013), 16.

11 P.W. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century* (New York: Penguin Press, 2009), 97-98. Moore's Law is derived from Gordon Moore's 1965 prediction that computer chip transistors would double every two years. A similar trajectory following Moore's prediction can be seen in most aspects of information technology. See: Kenneth Geers, "The Challenge of Cyber Attack Deterrence," *Computer Law & Security Review* 26, no. 3 (2010): 302, http://dx.doi.org/10.1016/j.clsr.2010.03.003.

accounting for the millions of computers across the networks of America's national security organizations.[12]

## 2.1. The Zero-Day Exploit

These undetected vulnerabilities, called zero-day exploits,[13] create hidden access points to computer systems and networks – a way to sneak in through the backdoor. Finding a previously undiscovered vulnerability does not necessarily pose an immediate security concern. Vulnerabilities, on their own, present a latent threat – a part of the technological capabilities needed to build a cyber attack without actually doing so.[14] A zero-day used as a component of a cyber attack, however, does pose a

[12] To illustrate this point, the Windows XP operating system, used for millions of US government computers, has 45 million lines of code. Between July 2012 to July 2013, 45 vulnerabilities were discovered although many more vulnerabilities are assumed to exist. See: Cade Metz, "Facebook Says It's Now as Big as Windows (Literally)," *Wired Magazine*, April 30, 2013, http://www.wired.com/wiredenterprise/2013/04/facebook-windows/; Craig Timberg and Ellen Nakashima, "Government computers running Windows XP will be vulnerable to hackers after April 8," *The Washington Post*, March 16, 2014, http://www.washingtonpost.com/business/technology/government-computers-running-windows-xp-will-be-vulnerable-to-hackers-after-april-8/2014/03/16/9a9c8c7c-a553-11e3-a5fa-55f0c77bf39c_story.html; and Tim Rains, "The Risk of Running Windows XP After Support Ends April 2014," *Microsoft Security Blog*, August 15, 2013, http://blogs.technet.com/b/security/archive/2013/08/15/the-risk-of-running-windows-xp-after-support-ends.aspx.

In a single year, one computer operating Windows XP had 45 potential ways where its vulnerabilities could be exploited. Assume, for a moment, that the Pentagon has one million computers operating Windows XP and no patches were applied to address these vulnerabilities. A sophisticated state hacker could potentially have 45 different access points to enter one computer and subsequently affect a network of one million computers to carry out national security functions. Assuming an average of 45 undiscovered vulnerabilities each year creates 630 potential opportunities for a state hacker to exploit Windows XP, one system, over its lifetime. See: David Crookes, "RIP Windows XP: the 'zombie' operating system that came to haunt Microsoft," *The Independent*, March 25, 2014, http://www.independent.co.uk/life-style/gadgets-and-tech/features/goodbye-windows-xp-9213134.html.

[13] For the purposes of this paper, the term "zero-day" is equivalent to a "zero-day exploit." These exploits are called zero-days because they are discovered and used before the developer is aware of them. From the time the developer discovers the vulnerability (Day 1), the clock starts to develop a patch before the vulnerability is exploited further. Discovery and exploitation of the vulnerability thus takes place on the zeroth day. See: PC Tools by Symantec, "What is a Zero-Day Vulnerability?," *PC Tools*, http://www.pctools.com/security-news/zero-day-vulnerability/.

[14] Jacques E.C. Hymans, "The Threat of Nuclear Proliferation: Perception and Reality," *Ethics & International Affairs 27*, no. 3 (2013): 282, http://dx.doi.org.proxy.lib.sfu.ca/10.1017/S089267941300021X.

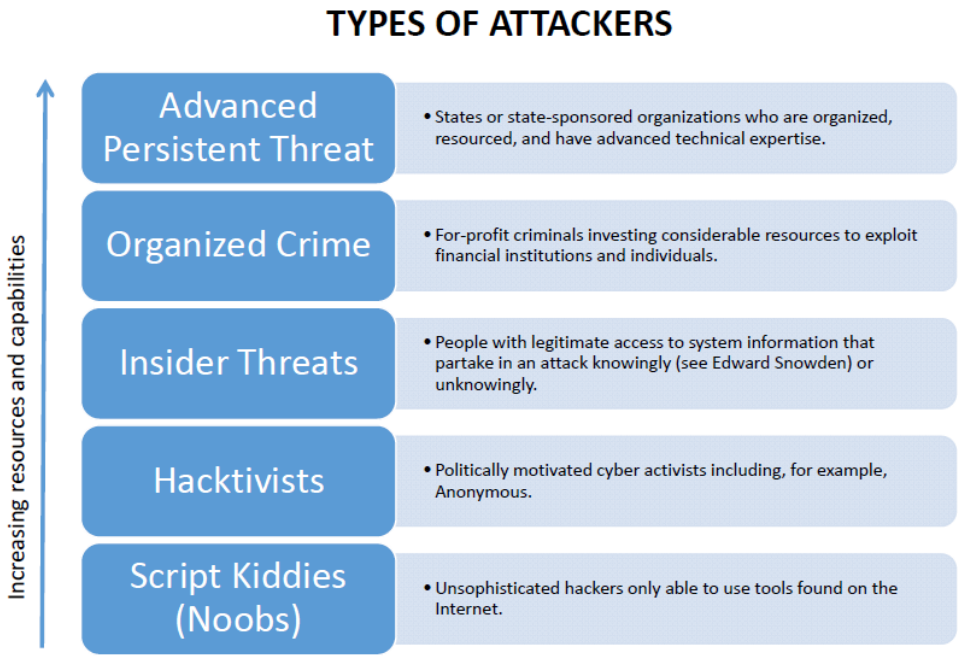
significant security threat. Converting a latent vulnerability into a cyber attack requires a high-level of coordination, resources, and, most importantly, technical expertise and capabilities.[15] Advanced Persistent Threats (APT) is the name given to states that possess this level of ability to execute sophisticated and unrelenting cyber attacks.[16] Cyber-capable states actively seek out these vulnerabilities to target their adversaries including, most often, other adversarial cyber capable states.

[15] See n. 60 for more information on constructing a cyber attack.

[16] Steve Winterfeld and Jason Andress, *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice* (Waltham, Mass: Syngress, 2012), 4, 8-10. Although resources matter, the most important factor for distinguishing between cyber-sophisticated states and other attackers is the high level of expertise an APT possesses. Within the APT category itself, there is a further hierarchy between states who possess superior capabilities, including the United States, Israel, Russia, China, France, and the United Kingdom and other states who possess cyber capabilities but have not yet reached the same level of superiority. The latter includes states such as Canada amongst others. See: James A. Lewis, *Conflict and Negotiation in Cyberspace* (Washington, DC: Centre for Strategic and International Studies, 2013), 4; Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (New York: The Penguin Press, 2011), 152; Richard Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What To Do About It* (New York: Ecco, 2010), 64-65; and Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld* (Senastopol, Calif.: O'Reilly Media, Inc., 2012), 243-262.

Some cyber capable states, such as China, sponsor proxies to carry out their cyber attacks. The Elderwood Gang (also called The Beijing Group), for example, is an organization with alleged links to the Chinese government that engages in cyber espionage. Elderwood primarily targets American companies "within the defence supply chain" using zero-day attacks. A secondary target vector are NGOs, "particularly ones connected to human rights activities related to Tibet and China." Unlike criminal organizations that attack a wide breadth of targets for profit, these state-sponsored organizations are selective and focus on specific targets of political or military value. See: Mark Clayton, "Stealing US Business Secrets: Experts ID Two Huge Cyber 'Gangs' in China," *The Christian Science Monitor*, September 14, 2012, http://www.lexisnexis.com.proxy.lib.sfu.ca/hottopics/lnacademic/?shr=t&csi=7945&sr= HLEAD(stealing%20us%20business%20secrets%3A%20experts%20id%20two%20huge%20cyber%20%27gangs%27%20in%20china)%20AND%20DATE%20IS%202012-09-14; Kim Zetter, "Sleuths Trace New Zero-Day Attacks to Hackers Who Hit Google," *Wired Magazine*, September 7, 2012, http://www.wired.com/2012/09/google-hacker-gang-returns/all/; Symantec Security Response, "The Elderwood Project," *Symantec Official Blog*, September 6, 2013, http://www.symantec.com/connect/blogs/elderwood-project; Anonymous, "Hackers Inc; Cybercrime," *The Economist*, July 12, 2014, http://search.proquest.com.proxy.lib.sfu.ca/docview/1544844816?accountid=13800.

**Figure 2: The Attacker Spectrum**[17]




A cyber attack targets three things: *confidentiality* (stealing information), *integrity* (manipulating data), or *availability* (denying access to information).[18] Targeting one facet, whether it be confidentiality, integrity, or availability, is sufficient to be considered a cyber attack. Precision targeting is necessary, given the Internet's networked nature, but useless unless sophisticated cyber states have a way to deliver their cyber attacks. Incorporating zero-days into a cyber strike provides a means to enter the target system undetected[19] to create disruptions.[20]

Searching for undetected vulnerabilities means that a cyber-capable state, like a developer, must examine or reverse engineer millions of lines of code in a system it is

17 Winterfeld and Andress, *Basics of Cyber Warfare*, 4, 8-10.

18 Ibid., 7.

19 Peter W. Singer, "The 'Oceans 11' of Cyber Strikes," *Brookings Institution*, May 2012, http://www.brookings.edu/research/articles/2012/05/21-cyber-threat-singer.

20 Thomas Rid, "Cyberwar and Peace," *Foreign Affairs* 96, no. 6 (2013), http://www.foreign affairs.com/articles/140160/thomas-rid/cyberwar-and-peace.

targeting.[21] The process is time-intensive and diverts valuable human and computational resources away from other activities in cyber.[22] Amassing a large enough arsenal of unused vulnerabilities through searching alone is inefficient. Instead, the US supplements its search by purchasing zero-days through private contractors in a "vulnerabilities market."[23]

## 2.2. The Vulnerabilities Market

The "vulnerabilities market" is a digital bazaar where hackers sell zero-day exploits amongst other illicit cyber goods. Corporations, such as Google, Microsoft, and Facebook, provide bounties to hackers who discover vulnerabilities in their security. The price a corporation pays for its bounty is low compared to the prices that can be charged in the "vulnerabilities market."[24] Instead of providing a corporation with information on where it is vulnerable,[25] professional hackers peddle this information in this digital marketplace to fetch a higher price. Through this marketplace, hackers can "fetch 10 to 100 times more" than what corporations are willing to pay.[26] Unless corporations start

21 Frei, *Known Unknowns*, 14.

22 Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND Corporation, 2009), 58.

23 Tom Gjelten, "First Strike: US Cyber Warriors Seize the Offensive," *World Affairs* 175, no. 5 (2013): 39, http://web.b.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=b33eb3d2-62d2-4cf8-97a9-0a85598d0ea6%40sessionmgr110&vid=2&hid=120.

24 Deibert, *Black Code*, 206.

25 These transactions, where hackers sell zero-days to the affected corporation, occur in a white vulnerabilities market. Hackers in the white market are largely motivated by the moral imperative to disclose vulnerabilities to enhance cyber security for the collective good. Financial gain is a secondary motivator. See: Paul N. Stockton and Michele Golabek-Goldman, "Curbing the Market for Cyber Weapons," *Yale Law and Policy Review* 32, no. 1 (2013): 248, http://web.a.ebscohost.com.proxy.lib.sfu.ca/ehost/pdfviewer/pdfviewer?sid=a6bc7e20-de4d-47de-b922-03c1d7b80b6d%40sessionmgr4005&vid=1&hid=4104.

26 Shane Harris, "Black Market for Malware and Cyber Weapons is Thriving," *Foreign Policy*, March 25, 2014, http://complex.foreignpolicy.com/posts/2014/03/24/black_market_for_malware_and_cyber_weapons_is_thriving.

paying market prices for exploits, they will not be able to convince hackers to stop selling in the vulnerabilities market.[27]

Although a cyber black market peddling illicit goods and services exists,[28] the US prefers to use the gray vulnerabilities market – a market that is hidden but not necessarily illegal.[29] The gray market can only be accessed through a trusted intermediary, usually a contractor operating within the market. Within the gray market, "large defense contractors [and…] smaller computer firms" act as intermediaries between the hackers who discovered the exploit and the buyers (who are most often state agencies).[30]

Reputation matters in this market not only for the hacker but for the intermediary contractors and buyers as well.[31] Hackers who provide exploits to contractors are able to leverage trustworthiness into a long-term income stream. Likewise, contractors want assurances that the vulnerability is legitimate whereas buyers want exclusive access to an unused product. Contractors (and hackers by extension) who sell an exploit to more than one client risk not only their reputation but, more importantly, their bottom line. States, especially America, are big buyers willing to pay handsomely for exploits. Profit is thus tied to trust. Selling the same vulnerability to others increases the likelihood that a state will take its business, and its millions of dollars, elsewhere without hesitation.[32]

27 Andy Greenberg, "Shopping for Zero-Days: A Price List For Hackers' Secret Software Exploits," *Forbes*, March 23, 2012, http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/.

28 Ibid.

29 Brian Fung, "The NSA hacks other countries by buying millions of dollars' worth of computer vulnerabilities," *The Washington Post*, August 31, 2013, http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/31/the-nsa-hacks-other-countries-by-buying-millions-of-dollars-worth-of-computer-vulnerabilities/. The Black Market exists to support cyber crime where "both the tools (e.g., exploit kits) and the take (e.g., credit card information)" are sold. The Grey Market, in comparison, is limited to the "exchange of vulnerabilities and exploits" – activities that are not prohibited since the discovery and development of such capabilities outside of this market are not necessarily illegal. See: Lillian Ablon, Martin C. Libicki, and Andrea A. Golay, *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar* (Santa Monica: RAND Corporation, 2014), iii, 1, 49.

30 Harris, *Black Market for Malware*.

31 Ablon et al., *Markets for Cybercrime Tools*, 26.

32 Ibid., 26-27.

Hackers, through private contractors, sell their undiscovered vulnerabilities to the highest bidder[33] with prices ranging from a few thousand dollars to $300,000 and, for a select few, up to $1 million per exploit. Google's bounty program, in comparison, typically pays up to $5,000 with rare payments of up to $150,000 for significant vulnerabilities.[34] These high prices mean that lower-order attackers (see Figure 2), who do not have the same resources as the United States, are priced out of the grey market. From there, America can mostly outspend its remaining competitors,[35] including other states, given its significant investment in cyber capabilities[36] and its willingness to pay market prices. In 2013, for example, the National Security Agency (NSA) spent more than $25 million to secure an arsenal of undetected vulnerabilities.[37] A fraction of budget spending[38] allowed the United States to take numerous undetected vulnerabilities off the market. Each undetected vulnerability added to the American cyber arsenal potentially means one less vulnerability for an adversarial cyber-capable state to purchase for use against America and its allies.

33 Gjelten, *First Strike*, 39.

34 Ablon et al., *Markets for Cybercrime Tools*, 26. The high price points are driven by: the difficulty of discovery, the level of difficulty in weaponizing an exploit, "the number of computers […] it provides access" [to…] and the value of those computers," and the fact that zero-days can only be used once. See also: Anonymous, "The Digital Arms Trade," *The Economist*, March 30, 2013, http://www.economist.com/news/business/21574478-market-software-helps-hackers-penetrate-computer-systems-digital-arms-trade; Harris, *Black Market for Malware*.

35 Gjelten, *First Strike*, 40. See n. 36 for more information on how the US can outbid its competitors.

36 Michael Hirsh, "Fear of Cyberwar Attack May Be Biggest Threat," *National Journal*, July 23, 2011. Academic Search Premier (03604217). Although China has the financial resources to compete with the US in a bidding war for vulnerabilities, the Chinese market for zero-days is saturated. Large number of hackers selling to the Chinese government pushes down the prices that can be charged for undetected vulnerabilities. The vulnerabilities market is profit-driven and hackers will sell to Western states where they can charge more for their product. Furthermore, "patriot hackers" regularly discover and supply vulnerabilities to the Chinese government thus lessening a dependence on the market. See: Greenberg, *Shopping for Zero-Days*; Nicole Perlroth and David E. Sanger, "Nations Buying as Hackers Sell Knowledge of Software Flaws," *The New York Times*, July 14, 2013, http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html.

37 Fung, *The NSA Hacks Other Countries*.

38 According to a Snowden leak, the NSA's (classified) 2013 Black Budget was $10.8 billion USD. Zero-day purchases total just 0.03% of the entire budget. See: Wilson Andrews and Todd Lindeman, "$52.6 billion: The Black Budget," *The Washington Post*, August 29, 2013, http://www.washingtonpost.com/wp-srv/special/national/black-budget/.

America's continuous quest to leverage vulnerabilities to stay ahead of its competitors has, perhaps unintentionally, created an invisible cyber arms race for zero-days.[39] Although the US is the dominant player in the vulnerabilities market,[40] it is not the only one – "Israel, Britain, Russia, India, and Brazil are [also…] big[…] spenders."[41] Smaller players include North Korea, "some Middle Eastern intelligence services [and] Countries in the Asian Pacific, including Malaysia and Singapore."[42]

The covert nature of cyber means that, unlike the acquisition of nuclear or conventional weapons, America cannot know with absolute certainty what exploits (and the subsequent potential for cyber weapons) competing states have acquired in the market.[43] On the one hand, American demand for zero-days invites competition from other states in the marketplace and potentially reduces the number of zero-days the US can exclusively buy. On the other hand, not all states that acquire zero-days will have the resources and technical expertise to convert a vulnerability into a sophisticated cyber weapon.[44] Despite the liabilities of a US-driven cyber arms race,[45] America still possesses the superior resources and expertise to stay ahead of most its market competitors (for now).

## 2.3. Use it or Lose it?

Most zero-days purchased through the grey market are specialized for specific software.[46] An undetected vulnerability for a system that is widely used both inside and

39 R. Scott Kemp, "Cyberweapons: Bold steps in a digital darkness?," *Bulletin of the Atomic Scientists*, June, 7, 2012, http://thebulletin.org/cyberweapons-bold-steps-digital-darkness.

40 Joseph Menn, "Special Report: U.S. cyberwar strategy stokes fear of blowback," *Reuters*, May 10, 2013, http://www.reuters.com/assets/print?aid=USBRE9490EL20130510.

41 Perlroth and Sanger, *Nations Buying as Hackers Sell*.

42 Ibid.

43 Libicki, *Nature of Strategic Instability*, 77.

44 Richard Betts, "The New Threat of Mass Destruction," *Foreign Affairs* 77, no. 1 (1998): 29, http://www.jstor.org.proxy.lib.sfu.ca/stable/20048360.

45 James Bamford, "NSA Snooping Was Only the Beginning. Meet the Spy Chief Leading Us Into Cyberwar," *Wired Magazine*, June 12, 2013, http://www.wired.com/2013/06/general-keith-alexander-cyberwar/all/.

46 Ablon et al., *Markets for Cybercrime Tools*, 26.

outside the American security architecture, such as Windows XP, creates a conundrum. On the one hand, the United States has purchased a vulnerability for a system that is most likely used by a number of its adversaries. The US could potentially convert one exploit into a multi-target cyber strike. On the other hand, America cannot patch the vulnerability in its own systems to protect itself. Alerting a corporation, such as Microsoft, to the existence of a vulnerability means that the corporation will issue a patch (a solution to the vulnerability). The patch issued will not be limited to users within American national security architecture but instead, will be released to all system users, including civilians, industry, or government. Once a patch is released and widely installed, the ability to successfully launch a cyber attack through that exploit is gone. The backdoor needed to access a system undetected has now closed.

The US thus faces a decision: save a zero-day and keep a vulnerability in its own system open or disclose the vulnerability and lose the ability to launch a cyber attack.[47] Purchasing an exploit, however, does not eliminate the possibility that a cyber-capable adversary will discover the same vulnerability through successful searching. An antagonistic state could then use the same zero-day America holds against the US. Rather than lose out on the opportunity to launch a cyber attack altogether, the United States collaborates with (and sometimes coerces) corporations to wedge open windows of opportunity to exploit vulnerabilities first.[48]

The Obama Administration's position (after years of secretly collecting and using zero-days)[49] is one of "responsible disclosure" where the government will alert an affected corporation of a vulnerability in their system to ensure a patch is issued.[50] Built into this position, however, was a significant loophole – zero-days that have "'a clear

47 Kemp, *Cyberweapons: Bold steps*.

48 Nicole Perlroth, Jeff Larson, and Scott Shane, "N.S.A Able to Foil Basic Safeguards of Privacy on Web," *The New York Times*, September 5, 2013, http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?hp&_r=1&&pagewanted=print.

49 Kim Zetter, "Obama: NSA Must Reveal Bugs Like Heartbleed, Unless They Help the NSA," *Wired Magazine*, April 15, 2014, http://www.wired.com/2014/04/obama-zero-day/.

50 Stockton and Golabek-Goldman, *Curbing the Market for Cyber Weapons*, 244; David E. Sanger, "Obama Lets N.S.A. Exploit Some Internet Flaws, Officials Say," *The New York Times*, April 12, 2014, http://nyti.ms/1gmYqOm.

national security or law enforcement need[…]'" are exempt from disclosure.[51] In principle, the Obama Administration is taking steps to increase the security of cyberspace while reducing the cyber arms race it, in effect, fueled. In practice, it seems that nothing has changed. As long as the US can "justify" that a zero-day has national security purposes, it can continue to discover and weaponize critical vulnerabilities to launch cyber attacks.[52]

Security in cyber depends on the ability to continually stay ahead of peer competitors.[53] The SIGINT Enabling Project, the NSA's $250 million a year program leaked by Edward Snowden, is part of America's effort to undermine encryption on the Internet to gain access to otherwise secret information. To do this, the US works with companies to knowingly covertly insert backdoors into their commercial products, including encryption software, to ensure sustained NSA access to information.[54] Although these vulnerabilities are only known to and exploited by the US,[55] a dedicated adversary could potentially discover and use the same backdoors against America.[56] Some corporations, such as Microsoft, disclose to the NSA in advance the patches they

51 Sanger, *Obama Lets N.S.A. Exploit Some Internet Flaws*.

52 Zetter, *NSA Must Reveal Bugs*.

53 Deibert, *Black Code*, 201.

54 Anonymous, "Secret Documents Reveal N.S.A. Campaign Against Encryption," *The New York Times*, September 5, 2013, http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html?ref=us; James Ball, Julien Borger, and Glenn Greenwald, "Revealed: how US and UK spy agencies defeat internet privacy and security," *The Guardian*, September 6, 2013, http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security. The SIGINT Enabling Project goes beyond inserting vulnerabilities into systems. It also seeks to work with industry to weaken encryption standards and push an "international encryption standard [the NSA…] can break." Combined, these tactics allow the NSA to access information that it would otherwise not be able to view. The industry organizations participating in this program have not been publicly named.

55 Anonymous, "Sigint – how the NSA collaborates with technology companies," *The Guardian*, September 5, 2013, http://www.theguardian.com/world/interactive/2013/sep/05/sigint-nsa-collaborates-technology-companies. The Guardian reports that companies, including Microsoft, are legally compelled to comply with the NSA's requests for access.

56 Perlroth et al., *NSA Able to Foil Basic Safeguards*.

will be issuing.[57] Advanced disclosure gives the US an opportunity to exploit the vulnerability before it is patched and the opportunity is lost.[58] America uses the opportunity in two ways: (1) at the frontend by inserting vulnerabilities that (in theory) only it can use and, (2) at the backend when it launches a cyber attack before the window of opportunity closes. Knowing the location of vulnerabilities helps manage the risk that the purchased zero-days could potentially be used against America first. Actively seeking to exploit and plant vulnerabilities helps the United States maintain a competitive advantage.

Nuclear or conventional weapons, once developed, can remain dormant yet functional until needed. In comparison, the zero-days used in cyber weapons require the US to constantly discover new vulnerabilities to maintain a deployable cyber arsenal. Holding a specific zero-day does not guarantee that the vulnerability will remain unpatched for a prolonged period of time by the targeted state.[59] Complicating this is the fact that undetected vulnerabilities, once acquired, are rarely used immediately given the time and resources it takes to construct a cyber attack.[60] In the time between acquisition

57 Fung, *The NSA Hacks Other Countries*. From Microsoft's perspective, advanced disclosures helps the government get "'an early start' on risk assessment and mitigation." On some level, the company is undoubtedly aware that the US government may exploit this information for offensive purposes. Having said that, a layer of deniability is built into this relationship – Microsoft "doesn't ask and can't be told how the government uses such tip-offs." See also: Michael Riley, "U.S. Agencies Said to Swap Data With Thousands of Firms," *Bloomberg*, June 15, 2013, http://www.bloomberg.com/news/print/2013-06-14/u-s-agencies-said-to-swap-data-with-thousands-of-firms.html.

58 Fung, *The NSA Hacks Other Countries*.

59 Libicki, *Cyberdeterrence and Cyberwar*, 55.

60 Singer, *Oceans 11*. The process for a cyber-capable state to develop and launch a cyber strike can take months to years to complete. On average, converting a zero-day into a cyber weapon takes about "500 person-days of work." See: Sandro Gaycken and Felix Fx Linder, "Zero-Day Governance: An (Inexpensive) Solution to the Cyber-security Problem," paper presented at the *Cyber Dialogue 2012: What is Stewardship in Cyberspace?,* Toronto, March 18-19, 2012, 7, http://www.cyberdialogue.citizenlab.org/wp-content/uploads/2012/2012 papers/CyberDialogue2012_gaycken-lindner.pdf.

and use, a patch for the vulnerability may be released, whether through routine patches or a specific identification of a security hole, rendering the vulnerability obsolete. To minimize this, America deploys several zero-days at once in a cyber attack to increase the odds that at least one (or more) of the vulnerabilities remains open to provide system access.[61]

## 2.4. One Attack, Multiple Vulnerabilities

Multiple backdoor entry points are preferable given that America cannot be absolutely certain of what vulnerabilities the target system will contain[62] despite extensive pre-launch cyber attack testing[63] and customization.[64] A successful cyber attack needs a minimum of one undetected vulnerability to gain access to the target system. Each successive zero-day that works adds to the strength and sophistication of a cyber assault.[65] As one vulnerability is patched, America can still rely on the other undetected vulnerabilities to continue its cyber strike. Incorporating multiple undetected vulnerabilities into a cyber attack reduces the need to create new cyber attacks after each zero-day fails.

The first step is to assemble and coordinate a team with diverse roles in the operation. From there, the team moves into the "reconnaissance and preparation" stage to understand the target system and its vulnerabilities. An attack is then developed to exploit a weak link in the system to gain access. Once access is secured, the state navigates through the system to override control, steal information, or ensure future access. The final step is to erase evidence of system intrusion. Singer's Ocean's 11 title is apt – to successfully launch a cyber attack, a state needs a large, well-resourced team taking on different roles (from target identification, reconnaissance, compromising weaknesses in the target, and technical exploitation) to get the "big score." See also: Lindsay, *Limits of Cyber Warfare*, 378-379.

61 Shane Harris, "The Cyberwar Plan," *National Journal*, November 14, 2009. EBSCOhost (45266379).

62 Gjelten, *First Strike*, 39-40.

63 Edward Hunt, "US Government Computer Penetration Programs and the Implications for Cyberwar," *IEEE Annals of the History of Computing* 34, no. 4 (2012): 16, http://muse.jhu.edu/journals/ahc/summary/v034/34.3.hunt.html.

64 Gaycken and Linder, *Zero-Day Governance*, 7.

65 Sean Collins and Stephen McCombie, "Stuxnet: The Emergence of a New Cyber Weapon and its Implications," *Journal of Policing, Intelligence, and Counter Terrorism* 7, no. 1 (2012): 86, DOI: 10.1080/18335330.2012.653198.

Stuxnet, a joint US-Israel operation, was a cyber attack designed to disrupt Iran's progress on its nuclear weapons program.[66] The attack was designed to alter the code of Natanz's computers and industrial control systems to induce "chronic fatigue," rather than destruction, of the nuclear centrifuges.[67] The precision of Stuxnet ensured that all other control systems were ignored except for those regulating the centrifuges.[68]

What is notable about Stuxnet is its use of four zero-day exploits (of which one was allegedly purchased)[69] in the attack.[70] That is, to target one system, Stuxnet entered through four different backdoors. A target state aware of a specific vulnerability in its system will enact a patch upon detection and likely assume that the problem is fixed. Exploiting multiple vulnerabilities creates variations in how the attack is executed given that different backdoors alter how the attack enters the target system.[71] One patch does not stop the cyber attack. The use of multiple zero-days thus capitalizes on a state's limited awareness of the vulnerabilities in its system.

66 Lindsay, *Limits of Cyber Warfare*, 379.

67 Ibid., 384.

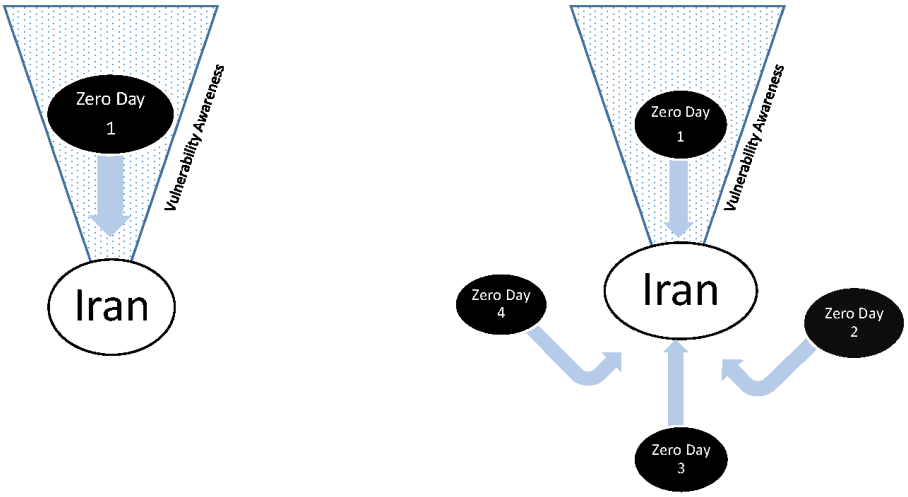
68 Martin Libicki, "The Nature of Strategic Instability in Cyberspace," *Brown Journal of World Affairs* 18, no. 1 (2011): 74, http://web.a.ebscohost.com.proxy.lib.sfu.ca/ehost/pdfviewer/pdfviewer?sid=45db41c8-21a1-486d-8613-deccbb90cfb4%40sessionmgr4002&vid=2&hid=4114.

69 Anonymous, *The Digital Arms Trade*; Menn, *Special Report: US Cyberwar Strategy*.

70 Sharon Weinberger, "Is This the Start of Cyberwarfare?," *Nature* 474, no. 7350 (2011): 143, DOI: 10.1038/474142a. In comparison, a regular malware attack only uses one zero-day exploit. See: Collins and McCombie, *Stuxnet: The Emergence of a New Cyber Weapon*, 86.

71 To illustrate this point, picture a burglar breaking into a house. The burglar could, for example, walk up a set of stairs and enter through the front door, enter through the garage at the back of the house, or walk around the side of the house and enter through the side door. The target (inside the house) is the same but the burglar can use different entry points to break in, each one requiring a variation (i.e. distance travelled, different types of doors, visibility to neighbours etc.) in how the burglar will act. Likewise, multiple zero-days provide different entry points into the target "house." Variance is created based on which door the attacker uses to break into the system.

**Figure 3: Multiple Zero-Day Exploits**




Each phase of Stuxnet was different from its previous phase which created confusion among the Iranians. Launched in 2009, Stuxnet was not discovered by the Iranians until 2010.[72] Yet even upon the initial discovery of the attack, who the attacker was remained unclear. The failures in the Natanz centrifuges were first attributed to insider error[73] and later to China[74] before finally discovering the true culprits.[75] The use of multiple undetected vulnerabilities helped to obscure the US and Israel as the actual attackers.[76]

The Stuxnet case helps illustrate the efficacy of zero-day attacks as a means of attaining political goals. Although Stuxnet did not produce immediate results in

72 Rid, *Cyberwar and Peace*.

73 David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *The New York Times*, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

74 Misha Glenny and Camino Kavanagh, "800 Titles but No Policy – Thoughts on Cyber Warfare," *American Foreign Policy Interests* 34, no. 6 (2012): 292, http://dx.doi.org/10.1080/10803920.2012.742410.

75 Noah Shachtman and Peter W. Singer, "The Wrong War," *Government Executive* 43, no. 10 (2011), http://web.ebscohost.com.proxy.lib.sfu.ca/bsi/detail?sid=580dc088-da1b-4cda-b35d-12363b5600b4%40sessionmgr114&vid=2&hid=122&bdata=JnNpdGU9YnNpLWxpdmUmc2NvcGU9c2l0ZQ%3d%3d#db=bth&AN=65089376.

76 David E. Sanger, *Confront and Conceal: Obama's Secret Wars and the Surprising Use of American Power* (New York: Crown Publishers, 2012), 208.

terminating Iran's nuclear program, it helped buy time for the Americans to consider other options against Iran. A nuclear Iran would not only threaten American security but possibly open a third conflict for America[77] in the Middle East given Israel's proclivity to strike a nuclear Iran first. Stuxnet allowed the United States to delay Iran's nuclear program without resorting to kinetic action.[78]

In response to Stuxnet, Iran launched a Distributed Denial of Service (DDOS) attack against US banks in 2012. The DDOS effects included intermittent Internet interruptions or website outages – minor disruptions rather than permanent, destabilizing damage. Iran also targeted Saudi Aramco, an oil and gas producer. The Aramco attacks included data wiping which disrupted part of its operating system for two weeks.[79] Launching Stuxnet, a cyber first-strike, ultimately incurred retaliation, albeit with less severity than the original attack.

## 2.5. The Need for Innovation

A zero-day exploit can only be used once.[80] Once an exploit is used, the targeted state is alerted to a vulnerability in its system. Compounding this problem is that when America launches a cyber attack, it has, in effect, send a clean copy of its attack code to its adversary. Unlike conventional or nuclear weapons, cyber weapons are not destroyed when they hit the target.[81] As R. Scott Kemp states, "It is as if with every bomb dropped, the blueprints for how to make it immediately follow."[82] Once detected, a cyber-capable adversary can dissect and reverse engineer the code for its own offensive purposes. Some estimates suggest that each cyber attack launched leads to a fivefold increase in

77 At the time of Stuxnet, the US was involved in military campaigns in Afghanistan and Iraq.

78 Sanger, *Confront and Conceal*, xi.

79 Lindsay, *Limits of Cyber Warfare*, 397; William D. Bryant, "Cyberspace Superiority A Conceptual Model," *Air & Space Power Journal* 27, no. 6 (2013): 40-42, http://web.ebscohost.com.proxy.lib.sfu.ca/ehost/pdfviewer/pdfviewer?sid=92b8dc2d-bb08-4d42-be5f-004da8873f2d%40sessionmgr110&vid=4&hid=122.

80 Clarke and Knake, *Cyber War*, 200.

81 Harris, *The Cyberwar Plan*.

82 Kemp, *Cyberweapons: Bold steps*.

the number of new attacks using variants of the original attack code.[83] While a cyber attack produces an initial advantage for America, the distance between cyber capabilities narrows if a cyber-sophisticated target state dissects and improves upon an American cyber attack.

Innovating on its own cyber attacks helps America maintain an advantageous capabilities gap against an adversarial cyber-capable state. From the Stuxnet code, the US produced two cyber attack variants, albeit with different zero-days, named Flame and Duqu.[84] Flame, used to spy on Iran's oil industry[85] and Iranian officials, could map out person-to-person relationships, collect information wirelessly, and digitally chart the locations of individual computers and networks[86] – capabilities that previously required an element of human intelligence (HUMINT). Duqu targeted specific computers in Iran's private sector to steal information on Iran's nuclear initiatives.[87] One attack code created three variants to gain information about how to best disrupt Iran's nuclear progress.

The discovery of one attack does not necessarily reveal the existence of other attacks with similar code. Stuxnet was discovered in 2010 but the Iranians did not discover its variants, Duqu and Flame, until 2011 and 2012 respectively.[88] The loss of Stuxnet did not terminate America's disruptive campaign against Iran's military

83 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): 834, DOI: 10.1145/2382196.2382284. A patch for a vulnerability can take days or months to develop and deliver to the affected users. In that time, other cyber attackers rush to exploit the recently discovered vulnerability before a patch is issued and the zero-day becomes obsolete.

84 Glenny and Kavanagh, *800 Titles*, 293.

85 Peter Beaumont and Nick Hopkins, "International: Obama ordered cyberwar against Iran: Nuclear programme main target of computer worms: Speculation grows over timing of revelations," *The Guardian (London)*, June 2, 2012, http://www.lexisnexis.com.proxy.lib.sfu.ca/hottopics/lnacademic/?shr=t&csi=138620&sr=HLEAD(international%3A%20obama%20ordered%20cyberwar%20against%20iran%3A%20nuclear%20programme%20main%20target%20of%20computer%20worms%3A%20speculation%20grows%20over%20timing%20of%20revelations)%20AND%20DATE%20IS%202012-06-02.

86 Mark Claydon, "Stuxnet cyberweapon set to stop operating," *Christian Science Monitor*, June 23, 2012. Academic Search Premier (77249946).

87 Ibid.

88 James P. Farewell and Rafal Rohozinski, "The New Reality of Cyber War," *Survival: Global Politics and Strategy* 54, no. 4 (2012): 107, DOI: 10.1080/00396338.2012.709391.

capabilities. Instead, America could fall back on Flame and Duqu to gather information to design another disruptive attack. Refining existing code at the outset of development and during the attack enables America to produce the next generation of cyber attacks quicker. With a shortened research and development phase, the United States can accelerate deployment of new attack variants into the networks it already penetrated. US-modified code ensures a continuity of specific objectives in cyberspace (such as disrupting Iran's nuclear capabilities) that serves its larger national security interests.

Adversaries study America's cyber tool and techniques "to capitalize on [US…] ideas" for their own strategic advantage.[89] On the one hand, innovating on its own code allows America to continue executing its security objectives in cyberspace. On the other hand, innovation allows the United States to speculate on how variations in its attack code may evolve to help anticipate potential attacks from its adversaries. While the United States may not be able to close all of its potential vulnerabilities,[90] it can at least flag the unpatched vulnerabilities most likely exploited in a cyber strike. Red-teaming cyber games further allow the US to test both anticipated attacks and potential responses to maintain an informational advantage.[91]

Cyber favours offense over defence given its lax security architecture. Sophisticated cyber states that are able to innovate first will enjoy a relative advantage.[92] Amassing an arsenal of undetected vulnerabilities does not necessarily produce an immediate, usable advantage. Instead, these vulnerabilities provide important information to gauge the strengths and weaknesses of America's offensive and defensive capabilities. Finding undetected vulnerabilities, and knowing how to exploit those, positions the US to capitalize on the offense-defence innovation cycle to preserve a cyber advantage. The strike methods of nuclear or conventional weapons are largely

89 Jan Kallberg and Bhavani Thuraisingham, "Cyber Operations: Bridging from Concept to Cyber Superiority," *Joint Force Quarterly* 1, no. 68 (2013): 55, http://web.a.ebscohost.com.proxy.lib. sfu.ca/ehost/pdfviewer/pdfviewer?sid=97a30f8e-0c55-449c-b007-ab718b40ff96%40sessionmgr4001&vid=2&hid=4114.

90 Libicki, *Cyberdeterrence and Cyberwar*, 50.

91 Nye, *Nuclear Lessons*, 26. See also: Libicki, *Nature of Strategic Instability*, 74.

92 Dave Clemente, "Cyber Security as a Wicked Problem," *The World Today* 67, no. 10 (2010): 17, http://web.a.ebscohost.com.proxy.lib.sfu.ca/ehost/pdfviewer/pdfviewer?sid=7660ec52-cf64-4e67-b87a-9d184245f62f%40sessionmgr4001&vid=2&hid=4114.

unchanged and can be used to great effect. Cyber weapons, in comparison, only successfully work once. Innovation is required to not only manage the "constant pressure to keep up,"[93] but to also tip the balance of informational advantage in your favour.

[93] Deibert, *Black Code*, 201.

# Chapter 3.

# The Challenge of a Deterrence Strategy in Cyber

During the Cold War, deterrence was the foundation of American security. The concept was straightforward: "an enemy will not strike if it knows the defender can defeat the attack or can inflict unacceptable damage in retaliation."[94] Deterrence dominated the thinking of policymakers during the latter half of the twentieth century[95] and, to a large extent, it continues today.[96] Applying a Cold War understanding of deterrence to cyber is akin to "trying to jam a new issue into the wrong historical framework."[97] Deterrence, as understood in Cold War terms of denial and retribution, does not confer a sizable advantage in cyber. When applied to the cyber security seesaw (see Figure 1), deterrence not only produces a smaller variance between advantage and vulnerability but also, creates more frequent oscillations between both sides.

94 Richard K. Betts, "The Lost Logic of Deterrence: What the Strategy That Won the Cold War Can – and Can't – Do Now," *Foreign Affairs* 92, no. 2 (2013), http://www.foreignaffairs.com/articles/138846/richard-k-betts/the-lost-logic-of-deterrence.

95 Shachtman and Singer, *The Wrong War*.

96 United States Senate Committee on Armed Services, "Advance Questions for Vice Admiral Michael S. Rogers, USN Nominee for Commander, United States Cyber Command," *United States Senate Committee on Armed Services*, March 11, 2014, http://www.armed-services.senate.gov/imo/media/doc/Rogers_03-11-14.pdf. See also: James A. Lewis, *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency* (Washington, DC: Center for Strategic and International Studies, 2008), 12.

97 Shachtman and Singer, *The Wrong War*. See also: Jean-Loup Samaan, "Cyber Command: The Rift in US Military Cyber-Strategy," *The Rusi Journal* 155, no. 6 (2010): 18, DOI: 10.1080/03071847.2010.542664.

## 3.1. Deterrence as Denial

The strategy of deterrence by denial aims to physically prevent adversaries from acquiring cyber weapons.[98] During the Cold War, a small number of states could possess nuclear weapons given the difficulty and cost of acquiring the technology.[99] Even the second-tier nuclear states who acquired the technology could not match the capabilities of the US and the Soviet Union. Cyber, in comparison, has over 100 states that possess cyber attack capabilities,[100] of which about 20 states have the ability to develop a Stuxnet-equivalent.[101] A strategy of denial in cyber is difficult given the low cost of entry needed to acquire cyber weapons.[102]

The start-up costs associated with building a cyber arsenal are initially quite low requiring only computational power and highly trained personnel. Developing nuclear weapons, in comparison, was resource intensive requiring a significant investment in infrastructure, equipment, and personnel.[103] States once relied on their own ingenuity, espionage, or other friendly states to acquire nuclear weapons technology. Cyber capabilities, in comparison, can be appropriated from states and non-state actors, including organized crime and hacktivists. While the US can take tools, such as undetected vulnerabilities, away from its adversaries, it cannot stop an opponent from acquiring cyber technology in the first place.

A cyber non-proliferation treaty to reinforce a deterrence by denial strategy is equally unlikely to be effective. The Non-Proliferation Treaty (NPT), for example, provided a verification regime to restrict the number of nuclear states. The entry of new nuclear powers did not happen simultaneously – there were often years between when the first and subsequent states acquired nuclear weapons. America had four years of being the sole nuclear power before the Soviets successfully detonated a nuclear bomb.

98 Geers, *Challenge of Cyber Attack Deterrence*, 299.

99 Ibid.

100 Shachtman and Singer, *The Wrong War*.

101 Peter W. Singer and Allan Friedman*, Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2013), 157.

102 Bryant, *Cyberspace Superiority*, 30.

103 Ibid.

Today, a corresponding gap of time between comparable cyber adversaries does not exist. Proliferation in cyber takes place at fiber optic speeds.[104]

Yet, even with the NPT, the "the size of the world's nuclear club has grown from five to nine."[105] Some states, including Iraq and North Korea, signed the NPT but later went ahead to disregard the treaty and develop their own nuclear weapons capability.[106] Applying a similar framework to cyber exacerbates these issues. Assuming there was enough political will[107] to get over 100 cyber capable states to sign on, verification remains problematic given the secrecy surrounding each state's cyber arsenal, the challenge of real-time attribution,[108] and competing conceptions of what constitutes a cyber attack.[109] Cyberspace is, unfortunately, far too conducive to cheating where measures of accountability can be circumvented.

## 3.2. Attribution and Active Defence

Where denial fails, according to classic deterrence thought, retaliation is a strategy for consideration. To prevent initial aggression, greater aggression is threatened through retribution.[110] For this strategy to work in cyber, an adversary must be convinced that launching a cyber attack against the US will not yield any strategic gains since greater retaliatory force will be returned.[111] The logic underpinning this strategy is from the Cold War where the threat of second-strikes was so unappealing that no state would dare employ a first strike. Retaliation during the Cold War, however, assumed that the

104 Singer and Friedman, *Cybersecurity and Cyberwar*, 161.

105 Kenneth Geers, "Cyber Weapons Convention," *Computer Law & Security Review* 26, no. 5 (2010): 549, DOI: 10.1016/j.clsr.2010.07.005.

106 Betts, *New Threat of Mass Destruction*, 35.

107 Geers, *Cyber Weapons Convention*, 549.

108 See section 3.2.

109 Nye, *Nuclear Lessons*, 35.

110 Geers, *Challenge of Cyber Attack Deterrence*, 301.

111 Betts, *New Threat of Mass Destruction*, 33.

deterring state would know who launched an attack and strike back.[112] In cyber, the immediate and certain attribution required for retaliation is problematic.

Near definitive attribution in cyber is possible just not in real time. Once an attack is detected, a process of forensic analysis and human intelligence[113] is required to trace back the origin of the attack and the perpetrator.[114] Since few states possess this level of cyber sophistication, the list of potential suspects can be narrowed.[115] Narrowing the suspects helps speed up the deductive component of attribution but it still does not get one any closer to identifying attackers in real time. In reality, it may take months[116] before an attacker is positively identified. Deterrence is weakened since the punishment enacted (if any) is so far away from the initial attack that it does little to dissuade the attacker from carrying out further strikes in the meantime.[117]

A nuclear launch gives 30 minutes of warning to formulate a response.[118] In that time, the American President could identify the attacker, consider options, and make a decision on retaliatory strikes. In contrast, the time from when a cyber attack is deployed to when it hits its target is approximately 300 milliseconds.[119] Since the President does not have the same luxury of time in cyber, a retaliatory response requires a level of automaticity. Active defence creates the capability to detect, trace back, and counterstrike a cyber attacker.[120] In this sense, an immediate response can help serve as a deterrent against attackers contemplating a strike against the United States.[121]

112 Ibid., 34.

113 In attribution, forensics can tell a state which machine launched an attack. Human intelligence helps to identify the individual or group that launched the attack and who they work for. See: Brenner, *America the Vulnerable*, 235.

114 Ibid., 50-51.

115 Clarke and Knake, *Cyber War*, 64-65.

116 Lindsay, *Limits of Cyber Warfare*, 377.

117 Libicki, *Cyberdeterrence and Cyberwar*, 41.

118 Nye, *Nuclear Lessons*, 27.

119 Ibid.

120 Jay P. Keysan and Carole M. Hayes, “Mitigative Counterstriking: Self-Defence and Deterrence in Cyberspace,” *Harvard Journal of Law & Technology* 25, no. 2 (2012): 433, http://jolt.law.harvard.edu/articles/pdf/v25/25HarvJLTech429.pdf.

121 Nye, *Nuclear Lessons*, 34.

The detection and trace back functions of active defence are necessary to enhance cyber security. The counterstrike component of active defence, however, is problematic. Counterstrikes can be both "retributive" to punish the attacker and "mitigative" to reroute the attack back to the assailant.[122] In both instances, active defence sends a cyber attack, albeit with varying degrees of severity, back to the attacker.[123]

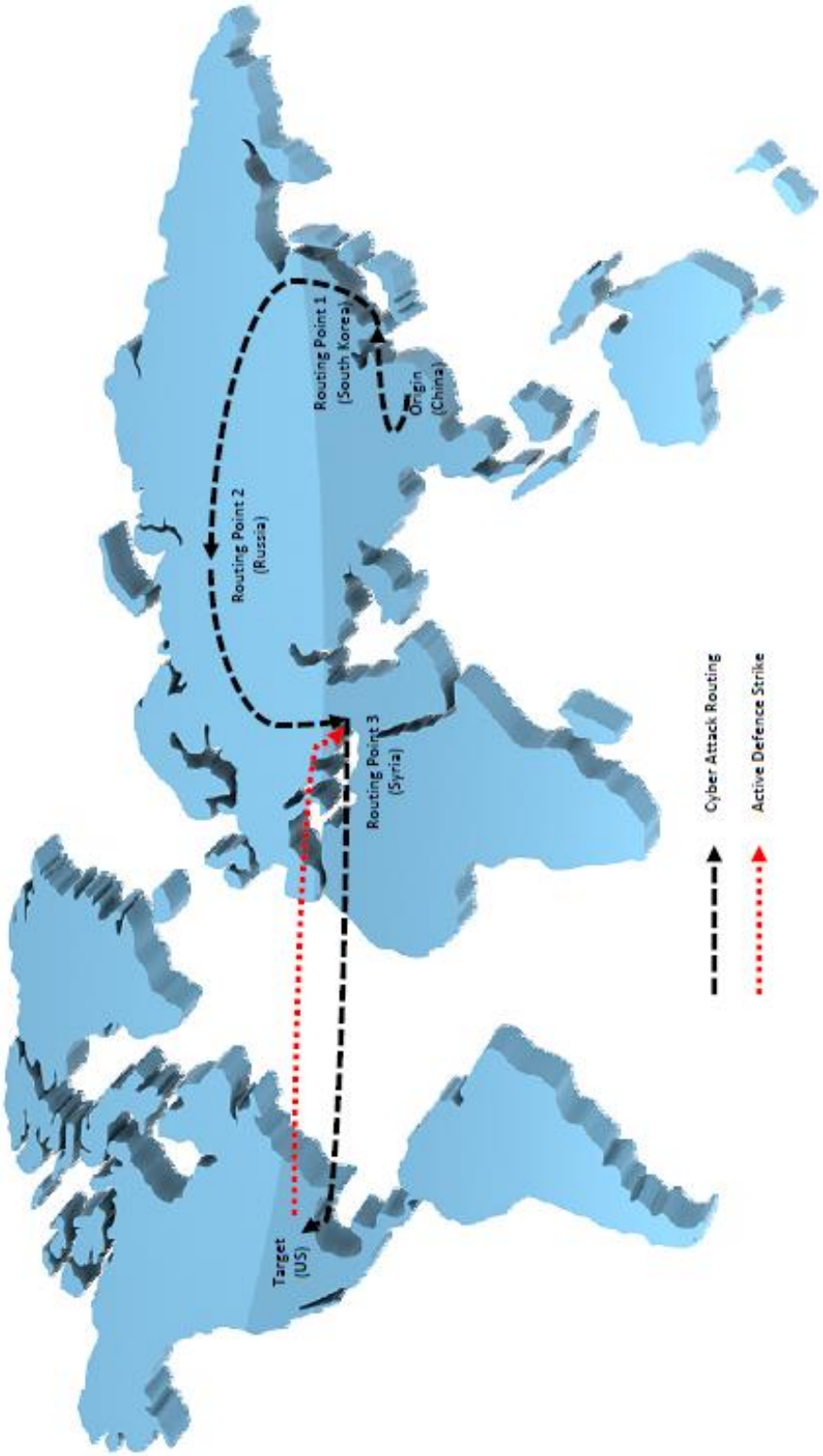
In practice, immediate retaliation is problematic for another reason. Sophisticated cyber attacks are rarely launched straight from state A to state B. Instead, a cyber strike is routed through multiple countries before reaching its intended target.[124] The problem with an automated reprisal is that it can hit back at a state that is a routing point for the attack rather than the originator. If a Chinese attack, for example, was routed through South Korea, Russia, and Syria, active defence could potentially target Syria instead of China, as illustrated below.

122 Kaysan and Hayes, *Mitigative Counterstriking*, 434-435, 476-477.

123 Active defence is a part of the Department of Defence (DOD) strategy for cyberspace but the extent of the DOD's counterstrike capabilities, its usage, and success rates remain classified. See: USA. Department of Defense. *Department of Defense Strategy for Operating in Cyberspace.* (Washington: Department of Defense, 2011), 6-7, http://www.defense.gov/news/d20110714cyber.pdf; Kaysan and Hayes, *Mitigative Counterstriking*, 476.

124 Geers, *Challenge of Cyber Attack Deterrence*, 301.

**Figure 4: Active Defence Illustration**



Automatic retaliatory strikes would thus target an innocent party whose networks were last exploited.[125] Active defence potentially opens up a conflict on two fronts in cyberspace: one against the original aggressor and another against the innocent state who was, in essence, pre-emptively attacked by the United States.[126] Attacks are often routed through states friendly and unfriendly to the US and an automatic strike against the former could damage cooperative relationships. Attribution needs a human element to be successful and taking a shortcut by using immediate counterstrikes weakens the potential security gains of employing deterrence. Time becomes the challenging variable since attribution needs months to enhance certainty while retaliation needs seconds to launch.

## 3.3. Ambiguous Signalling

Successful deterrence requires that there are no ambiguous signals about what the consequences will be for an attack.[127] To date, the Obama Administration has asserted that "The United States will ensure that the risks associated with attacking or exploiting our networks vastly outweigh the potential benefits."[128] Depending on the severity of a cyber attack, the US will "use all necessary means […] to defend [itself]" from diplomacy up to conventional and nuclear weapons as required.[129] Although the deterrence posture is public, the exact consequences of levelling a cyber attack against America remain unclear.

125 Libicki, *Cyberdeterrence and Cyberwar*, 41.

126 Ibid. As of 2013, the NSA, according to Edward Snowden, was purportedly developing an active defence capability named MonsterMind that could identify and block attacks, and automatically strike back "with no human involvement." However, it is unknown whether such a capability came to fruition or has successfully dealt the attribution problem in automatic reprisals. See: James Bamford, "The Most Wanted Man in the World," *Wired Magazine*, August 2014, http://www.wired.com/2014/08/edward-snowden/; Kim Zetter, "Meet MonsterMind, the NSA Bot That Could Wage Cyberwar Autonomously," *Wired Magazine*, August 13, 2014, http://www.wired.com/2014/08/nsa-monstermind-cyberwarfare/.

127 Ibid.

128 USA. *White House. International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, May 2011, 13, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

129 Ibid., 14.

Since the threshold of each response level remains ambiguous, adversaries may continue to attack the United States. Continued attacks, however, do not necessarily indicate that a deterrence posture has completely failed. Instead, adversaries may continue cyber strikes to "actively seek[…the] threshold [for retaliation] in order to avoid it."[130] In this sense, cyber strikes serve an intelligence gathering function. By deploying a wide array of cyber attacks, an attacker can flesh out the US response to determine its rigidity or flexibility. In addition, further attacks test America's resolve to actually retaliate when the time comes.[131] With this knowledge, an antagonistic state can either modify its cyber attacks to achieve strategic aims without assured retribution or find new ways to circumvent the threshold for attack. Neither outcome puts the United States in an optimal deterrence position.

If the United States revealed what retaliation would look like in cyberspace, it would, in effect, expose part of its cyber capabilities. One of China's longest intrusions, taking place over the better part of a decade, was within America's military networks and systems. Information on American weapons systems and other military technology was accessed according to a classified Defense Science Board report.[132] Assume for a moment that the United States makes its retaliation strategy explicit. For every instance of Chinese infiltration into Department of Defense networks to steal information, for example, the US will hack back into Chinese military networks to deny access to information. In this theoretical example, public disclosure reveals two things about American capabilities: (1) that it has access to Chinese military networks and, (2) that it has the capability to launch availability attacks. In doing so, the United States has essentially told the Chinese what part of its cyber capabilities are and the extent of penetration into Chinese networks. With this knowledge, the Chinese could shore up their networks and create better cyber strikes to circumvent an American retaliatory

130 Lindsay, *Limits of Cyber Warfare*, 401.

131 Libicki, *Cyberdeterrence and Cyberwar*, 71.

132 Mark Clayton, "Chinese cyberattacks hit key US weapons systems. Are they still reliable?," *The Christian Science Monitor*, May 28, 2013, http://www.csmonitor.com/USA/Military/2013/0528/Chinese-cyberattacks-hit-key-US-weapons-systems.-Are-they-still-reliable.

response.[133] American disclosure thus limits the usefulness of such retaliatory capabilities in the future.[134]

The clear signals required for deterrence places America in a catch-22 situation. To try and deter its adversaries, the US may inadvertently risk its own security by revealing its capabilities. If the United States remains ambiguous in how it applies deterrence, its adversaries may think the American deterrence posture is a bluff.[135] The signalling problem may create more vulnerabilities than advantages in cyber.

## 3.4. The Problem of Unacceptable Costs

The logic of deterrence relies on the fact that a state is willing to impose an unacceptable cost on its adversary.[136] During the Cold War, the unacceptable cost was a nuclear second strike – there was no worse weapon a state could launch.[137] In cyber, however, there are worse weapons that can be deployed in response. How a state reacts to a cyber attack could potentially create spillover effects outside of the cyber domain, including the domains of land, sea, or air.

Strictly speaking, cyber attacks alone have not yet produced an equivalent amount of destruction as nuclear or major conventional weapons.[138] Instead, cyber strikes target system and network disruption (over destruction).[139] Imposing an unacceptable cost in cyberspace is improbable given that cyber attacks, while expensive and troublesome, are survivable.[140] By this logic, a state would look to kinetic capabilities

133 Libicki, *Cyberdeterrence and Cyberwar*, 49.

134 Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38, no. 2 (2013): 59, http://muse.jhu.edu.proxy.lib.sfu.ca/journals/international_security/v038/38.2.gartzke.pdf.

135 Betts, *Lost Logic of Deterrence*.

136 Gartzke, *Myth of Cyberwar*, 46.

137 Libicki, *Cyberdeterrence and Cyberwar*, 49; Geers, *Challenge of Cyber Attack Deterrence*, 301.

138 Geers, *Challenge of Cyber Attack Deterrence*, 301.

139 Samaan, *Cyber Command*, 19, 16.

140 Libicki, *Cyberdeterrence and Cyberwar*, 71.

in order to effectively deter a cyber attack. The problem is that by doing so, a state potentially moves the conflict out of cyberspace and into the physical world where escalation and destruction become more likely.[141] Instead of cyber attack and counterattack, a response could include both cyber and kinetic means in domains both inside and outside of cyberspace. Cyber would no longer be confined to cyberspace.

A successful cyber attack requires covert conditions to create deniability on the part of the cyber attacker. A common assumption is that if a state cannot launch an attack covertly, it will be deterred from engaging in cyber strikes.[142] The credibility of deterrence is further challenged by states who launch attacks but do not care if they are caught.[143] In response to China's ongoing cyber attacks, the US has begun to publicly denounce China's intrusions into American systems.[144] Criticism and attribution notwithstanding, China has not slowed the rate at which it executes attacks. Given the breadth and persistence of attacks, it appears that deterrence at current levels may be ineffective against China in the long-term.[145]

Despite its drawbacks, deterrence in practice seems to have a mitigating effect on the behaviour of states outside of the military domain. Economic linkages between China and the US appear to have discouraged China from engaging in integrity attacks.[146] If the Chinese were to attack the American financial system, for example, China would not come out of such an attack in a strategically better position given that many of its assets are tied to Wall Street.[147] At the very least, it could be argued that an attack seriously affecting economic interests is counterproductive and seemingly

141 Ibid., 69.

142 Samaan, *Cyber Command*, 18.

143 Anonymous, "Masters of the cyber-universe; Cyber-hacking," *The Economist*, April 6, 2013, http://search.proquest.com.proxy.lib.sfu.ca/docview/1324420283?accountid=13800.

144 John Lee, "Cyber Kleptomaniacs: Why China Steals Our Secrets," *World Affairs* 173, no. 3 (2013): 74, http://web.a.ebscohost.com.proxy.lib.sfu.ca/ehost/pdfviewer/pdfviewer?sid=77656d24-1890-43fe-8870-d893bcbe6282%40sessionmgr4001&vid=2&hid=4114.

145 Ibid., 76.

146 It is possible, however, that a Chinese integrity attack on the US has occurred but has not been disclosed. Given what is currently known about China's attacks on America to facilitate espionage, an integrity attack appears unlikely for now.

147 Nye, *Nuclear Lessons*, 33.

unlikely.[148] Instead, to gain a strategic advantage, an attack on military or government structures, especially command and control systems, is the more attractive option.[149] Should tensions between China and the United States escalate further, integrity attacks on military or governmental systems could become more likely.

Adopting a position of credible deterrence is problematic in cyberspace. Deterrence works best when adversaries have a clear understanding of what one can do and will do if attacked.[150] Secrecy surrounding capabilities and objectives, however, is necessary to maintain a security advantage. Communicating an unambiguous deterrence posture erases the advantages secrecy confers in cyberspace.

How to attain a strategic advantage in cyberspace is much discussed but not well understood.[151] The newness of cyber causes America to frame cyber through existing concepts to enable an understanding of the complexity and difference of the cyber domain.[152] Politicians, in particular, appear to apply America's existing deterrence posture, crafted in the Cold War for nuclear conflict, to the electronic sphere.[153] A reformulation of deterrence is required for it to be effective in cyberspace – something that most likely will not happen until the US experiences a major cyber shock.[154] For now, the best strategy is for America to shore up the benefits of deterrence through better information that feeds defence, as detailed below.

148 Daniel K. Rosenfield, "Rethinking Cyber War," *Critical Review: A Journal of Politics and Society* 21, no. 1 (2009): 87, DOI: 10.1080/08913810902812156.

149 Ibid.

150 Martin C. Libicki, *Brandishing Cyberattack Capabilities* (Santa Monica: RAND Corporation, 2013), iii.

151 Singer and Friedman, *Cybersecurity and Cyberwar*, 4.

152 Ibid., 7.

153 Betts, *New Threat of Mass Destruction*, 34. Several reasons for this approach have been proposed including: forgetfulness of history, misapplication of concepts, and short-sighted policymaking. See also: Shachtman and Singer, *The Wrong War*; Betts, *Lost Logic of Deterrence.*

154 Exogenous shocks, notably from Pearl Harbour and the September 11 attacks, have precipitated policy and operational changes in the American security architecture. Cyber shocks may thus be required to not only put cyber threats in perspective but also necessitate a change in how cyber security is understood and applied. To date, there has not been significant shock sufficient to trigger comprehensive change. At present, American cyber policy can be considered a work in progress where policies are developed and reformulated incrementally. See: Shachtman and Singer, *The Wrong War*.

# Chapter 4.

# Defence through Resilience

Each year, the US government experiences volumes of cyber incidents. Department of Defence systems alone "are probed by unauthorized users approximately 250,000 times an hour, [and] over 6 million times a day" according to General Keith Alexander, the former Commander of the United States Cyber Command (USCYBERCOM) and former NSA Director.[155] Given the unrelenting cyber assaults it experiences, the American government now operates on the assumption that its networks and systems have been compromised.[156] No comprehensive solution exists to stop all attacks[157] and so, America must become resilient to absorb attacks. Cyber strikes do not yet pose an existential threat to the United States. Rather, these attacks provide an important source of information about America's attackers.

## 4.1. Information Extracted from Stolen Data

China is one of the largest perpetrators of cyber attacks against the United States targeting both commercial and military secrets.[158] Cyber theft is the chosen means to jumpstart security innovations that would otherwise lag behind American

[155] John Hamre, James Lewis, and Gen. Keith Alexander, "CSIS Cybersecurity Policy Debate Series: U.S. Cybersecurity Policy and the Role of U.S. CYBERCOM," *Centre for Strategic and International Studies,* June 3, 2010, http://csis.org/files/attachments/100603csis alexander.pdf.

[156] Brenner, *America the Vulnerable*, 91.

[157] Hunt, *US Government Computer Penetration Programs*, 12.

[158] Anonymous, Masters of the cyber-universe. China alone, by one estimate, is responsible for 70% of intellectual property theft according to a Commission on the Theft of American Intellectual Property report. See: The Commission on the Theft of American Intellectual Property, *The IP Commission Report* (Seattle, WA: The National Bureau of Asian Research, 2013), 2-3.

progress.[159] Secret information, the foundation of security superiority, is being pilfered at an alarming rate.[160] In spite of this, the United States is able to turn a loss of data into a strategic gain of information about its adversaries.

The Chinese commitment to modernizing its military has given rise to significant pilfering of American research and development for military systems. In 2007, for example, China exploited two vulnerabilities in Lockheed Martin's system to steal the plans for the F-35, a stealth fighter jet.[161] China saved itself years[162] in research and development (R&D) for a next generation fighter jet through this cyber attack.[163] Stolen data, however, can help point the United States towards what capabilities the Chinese are seeking but did not yet possess.

With each attack, America is able to enhance its situational awareness[164] to build a better picture of how the Chinese are developing their conventional capabilities based

159 Lee, *Cyber Kleptomaniacs*, 78.

160 Brenner, *America the Vulnerable*, 245.

161 Siobhan Gorman, August Cole, and Yochi Dreazen, "Computer Spies Breach Fighter-Jet Project," *The Wall Street Journal*, April 21, 2009, http://www.wsj.com/articles/SB124027491029837401.

162 Ellen Nakashima, "Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies," *The Washington Post*, May 27, 2013, http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html?hpid=z1. By some military estimates, China saved itself "25 years of research and development."

163 Ibid. The downside is that the US must now invest considerable time and effort to upgrade the weapons system compromised in the attack. While costly, it is a short term setback that will net a long-term advantage since vulnerabilities are easier to correct during development than after production. See: Clayton, *Chinese Cyberattacks Hit Key US Weapons Systems*.

164 Singer and Friedman, *Cybersecurity and Cyberwar*, 222. Situational awareness refers to an actor, in this case a state, understanding what happened, why it happened, and the effects of a cyber action. See: P. Barford et al., "Cyber SA: Situational Awareness for Cyber Defence," in *Cyber Situational Awareness: Issues and Research*, edited by Sushil Jajodia, Peng Liu, Vipin Swarup, and Cliff Wang (New York: Springer, 2010), 4.

on what information was taken.[165] Correspondingly, tracing back how and when China accessed military networks allows America to figure out the evolution of China's cyber capability. Having a clearer understanding of Chinese military development measured against America's current capabilities can help determine whether the United States remains superior in both cyber and conventional weapons. The information gathered thus provides a continual check on Chinese capabilities to ensure there are no "surprises" that threaten the predominance of American power.[166] The knowledge extracted from an attack is not only vital for intelligence but also provides information on how to improve American offence and defence.

## 4.2. Creating Defensive Obstacles

Cyber defence is an initially disadvantaged position[167] given that cyber barriers cannot stop all attacks from penetrating its systems. The ability to absorb a cyber attack, while inconvenient, helps America identify holes in its own security. Although America may be aware of a number of vulnerabilities, additional unaccounted for vulnerabilities will always exist in its systems. A cyber strike thus helps the United States identify where additional previously unknown vulnerabilities exist and, as a result, the US can direct its security apparatus to develop counter-capabilities.

The United States, through the Department of Homeland Security, has launched both passive and active cyber sensors to detect network intrusions. EINSTEIN 2, the

165 Similarly, states may also create attractive cyber targets, or "honeypots," to lure another state into an attack. Setting up such a decoy allows a state to determine what is or is not an attractive target to the adversaries. The larger gain come from counterintelligence – studying exactly how an adversary executes an attack and from where it originates from. Alternatively, such decoy can be used to distract an adversary from a more important attack. See: Tom Simonite, "Chinese Hacking Team Caught Taking Over Decoy Water Plant," *MIT Technology Review*, August 2, 2013, http://www.technologyreview.com/news/517786/chinese-hacking-team-caught-taking-over-decoy-water-plant/; Lior Div, "The Five Most Common Cyberattack Myths – Revealed," *Forbes*, September 11, 2014, http://www.forbes.com/sites/frontline/2014/09/11/the-five-most-common-cyberattack-myths-revealed/.

166 Brenner, *America the Vulnerable*, 53-54.

167 William J. Lynn III, "Defending a New Domain," *Foreign Affairs* 89, no. 5 (2010), http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain.

passive sensor, was launched in 2008 to detect network intrusions.[168] Building on the capabilities of EINSTEIN 2 was EINSTEIN 3, an active sensor designed to provide real-time threat detection capable of stopping known malware before it reaches the targeted government network.[169] Passive defences "scan, firewall, and patch" in an attempt to protect a system. These defences, however, have little utility against sophisticated cyber attacks, such as Stuxnet, or against attacks employing zero-days. Active defences, in comparison, build on passive defences to try and stop the cyber attack[170] but the success rates of such measures in the US security architecture remains unknown.[171] In reality, the EINSTEIN systems only detect and (in the case of EINSTEIN 3) stop known malware entering through known vulnerabilities.[172] Nevertheless, every vulnerability subsequently discovered through attack absorption allows EINSTEIN 3 to erect new cyber barriers in its systems.

A cyber-capable adversary may undertake multiple attempts to create sustained access to a target system or network.[173] Absorbing the initial attack becomes necessary to find and fix the exploited vulnerability to avert subsequent strikes. If only the first intrusion succeeds, the attacker will be forced to adjust its strike strategy to reopen the system access it once had. By erecting cyber obstacles, one is able to discourage weaker actors from exploiting the same vulnerability before it is patched. Adapting from vulnerabilities to defensive barriers may not stop cyber attacks altogether but it can frustrate cyber-capable states from "easily succeeding in […subsequent] attacks."[174]

168 USA. National Security Council. *The Comprehensive National Cybersecurity Initiative*. (Washington: Executive Office of the President of the United States, 2009), 2.

169 Ibid., 3.

170 Kaysan and Hayes, *Mitigative Counterstriking*, 432, 435.

171 Ibid., 476; USA. *Department of Defence. Department of Defence Strategy for Operating in Cyberspace.* (Washington: Department of Defence, 2011), 6-7.

172 William Jackson, "Einstein 3 goes live with automated malware blocking," *GCN*, July 24, 2013, http://gcn.com/Articles/2013/07/24/Einstein-3-automated-malware-blocking.aspx?Page=1.

173 USA. Defense Science Board. *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*, (Washington: Office of the Under Secretary of Defence for Acquisition, Technology and Logistics, 2013), 49. http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.

174 Lindsay, *Limits of Cyber Warfare*, 397.

Allowing a cyber attack, while counterintuitive, allows the US to gather valuable information on its attacker. By identifying how an attacker got into an American system or network and what information was sought, the US is positioned to better understand not only its vulnerabilities but also the capabilities and intentions of its adversaries. Resiliency through attack absorption diminishes the prospect of long-term disruption to American networks. As a result, the benefits to an attacker diminish.[175] What was an initial disadvantage can be converted into a long-term security gain.

[175] Nye, *Nuclear Lessons*, 34.

# Chapter 5.

# Cyber Security through Alliance: The Case of the Five Eyes

America, like other cyber capable states, has penetrated numerous foreign networks.[176] Strictly speaking, cyber espionage is a cyber attack on confidentiality.[177] Yet, the United States, as most other states, considers these types of cyber attacks acceptable given that the intrusions gather intelligence rather than steal "technolog[ical], trade, or financial secrets."[178] Unlike other cyber capable states, America stresses that its cyber espionage operations are a continuation of traditional state-to-state spying,[179] albeit in another domain.

Gains in cyber security then depend on America's ability to collect information first. America possesses cyber intelligence capabilities that are significantly more advanced than most states,[180] yet it is unable to gather the volume of intelligence it

176 Clarke and Knake, *Cyber War*, 123.

177 Winterfeld and Andress, *Basics of Cyber Warfare*, 7.

178 Michael Riley, "How the U.S. Government Hacks the World," *Bloomberg BusinessWeek*, May 23, 2013, http://www.businessweek.com/printer/articles/119394-how-the-u-dot-s-dot-government-hacks-the-world. In particular, America has drawn this distinction to demonstrate how China is on the wrong side of cyber espionage. The American perception is that the United States mainly uses cyber attacks for intelligence gathering whereas China uses cyber attacks to steal intellectual property. China's thefts of intellectual property, in the US' view, goes beyond the acceptable conduct of cyber espionage. See: Clarke and Knake, *Cyber War*, 123; Jacob Davidson, "China Accuses U.S. of Hypocrisy on Cyberattacks," *Time*, July 1, 2013, http://world.time.com/2013/07/01/china-accuses-u-s-of-hypocrisy-on-cyberattacks/.

179 Nakashima and Warrick, *For NSA Chief, Collect it All*.

180 Nye, *The Future of Power*, 117. In the same class as the United States in terms of advanced intelligence capabilities are "Russia, Britain, China, and France." Of this group, Britain is the only state in the Five Eyes. Despite the UK's advanced capabilities, it is still dependent on the United States for intelligence support. See: Nick Hopkins and Julian Borger, "Exclusive: NSA pays £100m in secret funding for GCHQ," *The Guardian*, August 1, 2013, http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden.

needs. This intelligence deficit is remedied by cooperating with its Five Eyes partners – Canada, the United Kingdom (UK), Australia, and New Zealand. Such a relationship, however, is not without drawbacks, as the US must manage competing interests within and threats to the alliance structure. Cooperation, while valuable, can be a double-edge sword to American interests and to its partners.

## 5.1. Necessary Coverage

During World War II, America established a cooperative signal intelligence (SIGINT) relationship with the United Kingdom and, by association, the "Dominions of Canada, Australia, and New Zealand."[181] The 1946 UKUSA Agreement[182] formalized this relationship into an intelligence sharing alliance that is still in force today. During the Cold War, the Five Eyes (the name given to the five partners of the UKUSA Agreement) predominantly targeted "the Soviet Union and its Warsaw Pact allies."[183] Each partner was responsible for collecting intelligence in a specific geographic area to cover the significant Soviet threat. The world was effectively carved up into five regional clusters – one for each member of the Five Eyes.[184]

181 National Security Agency, "UKUSA Agreement Release 1940-1956," *National Security Agency*, June 24, 2010, http://www.nsa.gov/public_info/declass/ukusa.shtml.

182 Ibid.

183 Martin Rudner, "Canada's Communications Security Establishment from Cold War to Globalization," *Intelligence and National Security* 16, no. 1 (2001): 98, DOI: 10.1080/714002836.

184 Jeffrey T. Richelson, "The Calculus of Intelligence Cooperation," *International Journal of Intelligence and CounterIntelligence* 4, no. 3 (1990): 308, DOI: 10.1080/08850609008435147. Unofficial accounts suggest that Canada covers the Arctic (with reach into Russia and China), Latin America, and the North Pacific and North Atlantic oceans. Australia and New Zealand cover South and East Asia, and the South Pacific and Southeast Asia respectively. The United Kingdom is responsible for Europe and Western Russia. The US covers "the Caribbean, China, Russia, the Middle East and Africa." See: James Cox, *Canada and the Five Eyes Intelligence Community* (Ottawa: Canadian Defense & Foreign Affairs Institute, 2012), 6; Rudner, *Canada's Communications Security Establishment*, 103.

The Five Eyes focused on the Soviet Union as the predominant intelligence target during the Cold War.[185] Post-Cold War, the threat is no longer confined to one state. The Five Eyes must now contend with a diffusion of threats given the low cost of entry[186] and the speed at which cyber attacks and counterattacks can occur.[187]

Without the Five Eyes, America could only "collect [information…] against a part of the target."[188] Incomplete information increases the risk of intelligence failures that affect American security inside and outside of cyberspace.[189] Intelligence collected from the Five Eyes allows the United States to enhance its situational awareness of the threats it directly faces, and the threats its partners face that could spillover to America. Ensuring adequate intelligence coverage through the alliance thus remains a necessity.

## 5.2. Sharing Capabilities and Information

A capabilities gap exists in the alliance between America, the primary, technologically sophisticated, and well-resourced partner, and the secondary partners of the UK and Canada, in particular, but also Australia and New Zealand.[190] As a result, the intelligence burden is unequally shared among the partners. The United States reinforces an asymmetric relationship that "bind[s] its all[ies…] more firmly to the [alliance]"[191] by perpetuating a continued dependence on American SIGINT capabilities.

185 Chris Clough, "Quid Pro Quo: The Challenge of International Strategic Intelligence Cooperation," *International Journal of Intelligence and CounterIntelligence* 17, no. 4 (2004): 607, DOI: 10.1080/08850600490446736.

186 Clemente, *Cyber Security as a Wicked Problem*, 17.

187 Cilluffo and Cardash, *Cyber Domain Conflict*, 46.

188 Stephen Lander, "International Intelligence Cooperation: An Inside Perspective," *Cambridge Review of International Affairs* 17, no. 3 (2004): 492, http://dx.doi.org/10.1080/0955757042000296964.

189 Ibid., 491.

190 Stéphane Lefebvre, "The Difficulties and Dilemmas of International Intelligence Cooperation," *International Journal of Intelligence and CounterIntelligence* 16, no. 4 (2003): 530, DOI: 10.1080/716100467.

191 Jennifer E. Sims, "Foreign Intelligence Liaison: Devils, Deals, and Details," *International Journal of Intelligence and CounterIntelligence* 19, no. 2 (2006): 198, DOI: 10.1080/08850600500483657.

Dependence, as a result of the capabilities gap, entrenches America's hegemonic position within the Five Eyes.[192]

The NSA shares its technologies and capabilities in exchange for strongly influencing the intelligence priorities of its partners.[193] Sharing occurs in two ways: (1) the NSA directly supplies computing resources to its partners[194] or, (2) the NSA funds a partner to "develop [specific] technologies."[195] Capabilities sharing becomes a strategic tool of America's larger efforts of guaranteeing partner cooperation to prioritize its own security interests within the alliance. [196]

The technology directly shared, reported to be mostly American in origin,[197] creates a level of interoperability between the Five Eyes' systems. Integration can help mitigate unexpected cyber shocks that would otherwise disrupt American intelligence gathering and processing functions. In 2000, for example, the NSA experienced a "'system overload'" where its computers were unable to process intelligence for four days.[198] During this time, the US reassigned the processing of American SIGINT to its partners.[199]

To carry out the Five Eyes mission – defending government systems in cyber and providing information to support governmental decision-making – access to high-

192 Zygmunt Bauman et al., "After Snowden: Rethinking the Impact of Surveillance," *International Political Sociology* 8, no. 2 (2014): 127, DOI: 10.1111/ips.12048.

193 Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (Toronto: Signal/McClelland & Stewart, 2014), 124.

194 Greg Weston, Glenn Greenwald, and Ryan Gallagher, "Snowden document shows Canada set up spy posts for NSA," *CBC News*, December 10, 2013, http://www.cbc.ca/news/politics/snowden-document-shows-canada-set-up-spy-posts-for-nsa-1.2456886.

195 Greenwald, *No Place to Hide,* 124. See also: Hopkins and Borger, *Exclusive: NSA pays £100m.*

196 Lefebvre, *Difficulties and Dilemmas*, 530.

197 Rudner, *Canada's Communications Security Establishment*, 112.

198 Walter Pincus, "NSA System Inoperative For Four Days; Computer Glitch Halted Data Interpretation," *The Washington Post*, January 30, 2000, http://www.lexisnexis.com.proxy.lib.sfu.ca/hottopics/lnacademic/?shr=t&csi=8075&sr=HLEAD(nsa%20system%20inoperative%20for%20four%20days%3B%20computer%20glitch%20halted%20data%20interpretation)%20AND%20DATE%20IS%202000-01-30.

199 Rudner, *Canada's Communications Security Establishment*, 113.

level intelligence is required.[200] The alliance partners, however, are dependent on American capabilities to produce comprehensive intelligence.[201] Rejecting an American-dictated reprioritization of its intelligence tasks could potentially jeopardize an alliance member's national interests. The partners, in a comparatively weaker position, acquiesced to American needs during the NSA's blackout to ensure future access to significant intelligence assets. [202]

Integrated systems allowed American intelligence efforts to carry on despite experience a significant systems blackout.[203] Although the NSA's systems overload resulted from a computer glitch rather than a cyber attack,[204] it nevertheless provides an example for future outages. Should the United States experience a significant cyber attack targeting availability in the future, America can still direct its alliance partners to collect intelligence and produce assessments. The US will still get the information it needs to make strategic security decisions.

Linked networks may also increase the prospect of a cyber attack against one partner spreading to another. Titan Rain, for example, was a series of coordinated cyber attacks from 2003 to 2005 that originated from China.[205] Although Titan Rain initially exfiltrated information from the US Department of Defence systems, it later spread to

200 Cox, *Canada and the Five Eyes*, 6.

201 Hopkins and Borger, *Exclusive: NSA pays £100m*. Sixty percent of the intelligence GCHQ produces, for example, "'is based on either NSA end-product or derived from NSA collection.'"

202 Rudner, *Canada's Communications Security Establishment*, 113.

203 Ibid.

204 Pincus, *NSA System Inoperative*.

205 John Markoff, David E. Sanger, and Thom Shanker, "In Digital Combat, U.S. Finds No Easy Deterrent," *The New York Times*, January 26, 2010, http://search.proquest.com.proxy.lib.sfu.ca/docview/1461079100?accountid=13800.

other “sensitive government and private-sector systems.”[206] By 2005, Titan Rain had infiltrated the systems of the Five Eyes governments, amongst other American allies.[207]

The converse, where an attack against a Five Eyes member spreads to America, could also occur. An adversarial cyber state may only need to penetrate one Five Eyes system to access American secrets through linked networks.[208] The technology America shares with the alliance potentially reduces the cyber obstacles that would otherwise be in place to frustrate a sophisticated cyber attacker. Interoperability increases the possibility that a cyber strike may not be contained within the networks on the original attacked state.

America’s willingness to share its advanced capabilities provides an incentive for the secondary Five Eyes partners to participate in the alliance. Shared US capabilities provides an avenue for the partners to access a multi-billion dollar intelligence apparatus without making an equivalent investment in their own capabilities. Canada’s Communication Security Establishment (CSEC), for example, has a budget of $460 million CDN.[209] The NSA, in comparison, has a budget of $10.8 billion USD.[210] Upgrading the capabilities of CSEC to NSA levels requires a roughly ten-fold increase in

206 Holly Porteous, *Cybersecurity and Intelligence: The U.S. Approach (Background Paper)* (Ottawa: Library of Parliament, 2011), 1.

207 Ibid.; Nathan Thornburgh et al., “The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them),” *Time Magazine*, September 2005, http://web.a.ebscohost.com.proxy.lib.sfu.ca/ehost/detail/detail?sid=21192193-4446-4831-a689-832a617141b4%40sessionmgr4002&vid=4&hid=4206&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=aph&AN=18065208.

208 Cox, *Canada and the Five Eyes*, 5.

209 Colin Freeze, “Spy agency’s budget to hit $460-million after ‘steady path’ of growth,” *The Globe and Mail*, November 12, 2013, http://www.theglobeandmail.com/news/politics/spy-agencys-budget-to-hit-460-million-after-steady-path-of-growth/article15385168/. CSEC’s 2013/2014 budget is roughly equivalent to 4% of the NSA’s budget. In 2014-2015, CSEC’s budget is anticipated to increase to $829 million largely to help pay for CSEC’s new state-of-the-art headquarters. See: Canada. Treasury Board of Canada Secretariat, *2014–15 Estimates: Parts I and II The Government Expenditure Plan and Main Estimates*, 2014, http://www.tbs-sct.gc.ca/ems-sgd/me-bpd/20142015/me-bpd-eng.pdf.

210 Barton Gellman and Greg Miller, “U.S. spy network’s successes, failures and objectives detailed in ‘black budget’ summary,” *The Washington Post*, August 29, 2013, http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_print.html.

CSEC's budget – an unlikely investment. Instead, Canada, through the Five Eyes, can "access […] a $15 billion global [information-sharing] partnership" that imparts vital intelligence on key "threats and […] technological challenges."[211] Cooperation is decidedly less expensive than developing independent and competitive intelligence capabilities.[212]

Such an arrangement, however, may have conditions imposed by the United States. While the partners can access American capabilities, they must, in return seriously consider US intelligence priorities. If they do not, America, for example, could hold the flow of shared capabilities, and the associated intelligence produced, hostage.[213] The independence of the secondary SIGINT agencies are further curtailed when America provides targeted funding for partner-produced technology.[214] Such an arrangement compels a partner to support American cyber advancements, possibly incurring a trade-off in its own priorities.[215]

A further complication arises when the United States essentially tasks its partners with leading SIGINT operations. CSEC, for example, led an operation named Olympia to gather intelligence on Brazil, specifically its government-regulated energy sector.[216] Similarly, the UK's Government Communications Headquarters (GCHQ) led an operation, codenamed Tempora, to tap into fibre-optic Internet cables to extract data in

211 Canada, Standing Senate Committee on National Security and Defence, *Transcript of Proceedings (Meeting No. 15).* 1st sess., 41st Parliament, Meeting No. 15, 2012. Testimony of John Forster.

212 Sims, *Foreign Intelligence Liaison*, 198-199.

213 Richelson, *Calculus of Intelligence Cooperation*, 317.

214 Greenwald, *No Place to Hide*, 124. Both Canada and the UK have been funded by the NSA. Britain's GCHQ, for example, has received at least $100 million GBP since 2009 from the NSA to fund the development of eavesdropping capacities, technology to tap into "transatlantic cables that carry internet traffic," and other sensitive capabilities. Canada, on the other hand, received under $500,000 from the NSA for technological development in 2012. Information on the NSA's financing of Canadian capabilities is incomplete but it is known that the NSA has provided software and cryptologic, technical, and information protection capabilities. See also: Hopkins and Borger, *Exclusive: NSA pays £100m*; Greenwald, *No Place to Hide*, 124; Weston, *Canada Set Up Spy Posts for NSA*; and USA. National Security Agency. *NSA Intelligence Relationship with Canada's Communications Security Establishment Canada* (National Security Agency, April 3, 2013), 2.

215 Richelson, *Calculus of Intelligence Cooperation*, 318.

216 Greenwald, *No Place to Hide*, 119-121.

transit.[217] In doing so, the United States can access information while insulating itself with a layer of deniability, assuming its adversary is not very cyber capable. Yet, the information collected from such operations cannot be for American eyes only given the partner's involvement. A liability arises where the partners could use the information collected "for unintended [non-US sanctioned] purposes."[218] While outsourcing helps spread the risks of conducting cyber espionage to its partners, it cannot overcome the inherent self-interest of states. Nevertheless, America's control over the allocation of capabilities and intelligence product may provide enough of an incentive to favourably tip the security seesaw to ensure the information is used in ways favourable to American interests.

Sharing ultimately means that America partially forfeits control of its advanced capacities to the alliance.[219] Vulnerabilities are further magnified if the partners cannot produce the expected intelligence innovations paid for by the United States. Increased cyber linkages potentially provides easier pathways for adversaries to attack America by exploiting the systems of a trusted partner. Despite the cascading vulnerabilities inherent in capabilities sharing, the Five Eyes provides an important avenue for America to expand its global surveillance reach.[220]

Cyberspace is large and complex – the US cannot watch it all and, as a consequence, partners are required. America thus employs a strategic trade-off. The US concedes part of its monopoly on advanced cyber capabilities, used in the production of high-value intelligence, to its partners. In return, America is able to influence the intelligence efforts of the Five Eyes. America can thus leverage its advanced capabilities to ensure its intelligence objectives are prioritized within the alliance.

217 Bauman et al., *After Snowden*, 122.
218 Lefebvre, *Difficulties and Dilemmas*, 536.
219 Sims, *Foreign Intelligence Liaison*, 197.
220 Bauman et al., *After Snowden*, 127.

## 5.3. Compromised from the Inside: The Problem with Insider Threats

External threats are always considered in national security calculations but focusing on these threats alone is not enough to comprehensively address cyber security vulnerabilities. Adding a complicating layer to cyber security is the possibility that states are not only vulnerable externally but also internally from within their own agencies. Intelligence for national security helps minimize the risks of "surprises"[221] so long as secrecy remains uncompromised.[222] Insider threats disrupt the standard of secrecy and, in doing so, undermine a state's informational advantages and invites increased public scrutiny.

Edward Snowden was a NSA contractor who stole volumes of confidential government surveillance documents and subsequently released them to the public.[223] Snowden, one individual acting alone, has released approximately 200,000 documents classified "top secret" or "special intelligence" to date and it is assumed that the leaks are unlikely to stop anytime soon.[224] His motivation for the leaks, as reported, stemmed from a personal dissatisfaction with the scope and covert nature of the NSA's surveillance program.[225] The Snowden leaks upset the national security structure where secrecy is valued over transparency[226] and, as a result, mobilized public distrust against the government over privacy concerns.[227]

221 Brenner, *America the Vulnerable*, 53-54.

222 Ibid., 207.

223 Ellen Nakashima, "U.S. officials dodge questions on scope of surveillance," *The Washington Post*, September 26, 2013, http://www.washingtonpost.com/world/national-security/nsa-leaks-extremely-damaging-national-intelligence-director-tells-senate-hearing/2013/09/26/a01b4e08-26d3-11e3-b75d-5b7f66349852_story.html.

224 Mark Hosenball, "NSA chief says Snowden leaked up to 200,000 secret documents," *Reuters*, November 14, 2013, http://www.reuters.com/article/2013/11/14/us-usa-security-nsa-idUSBRE9AD19B20131114.

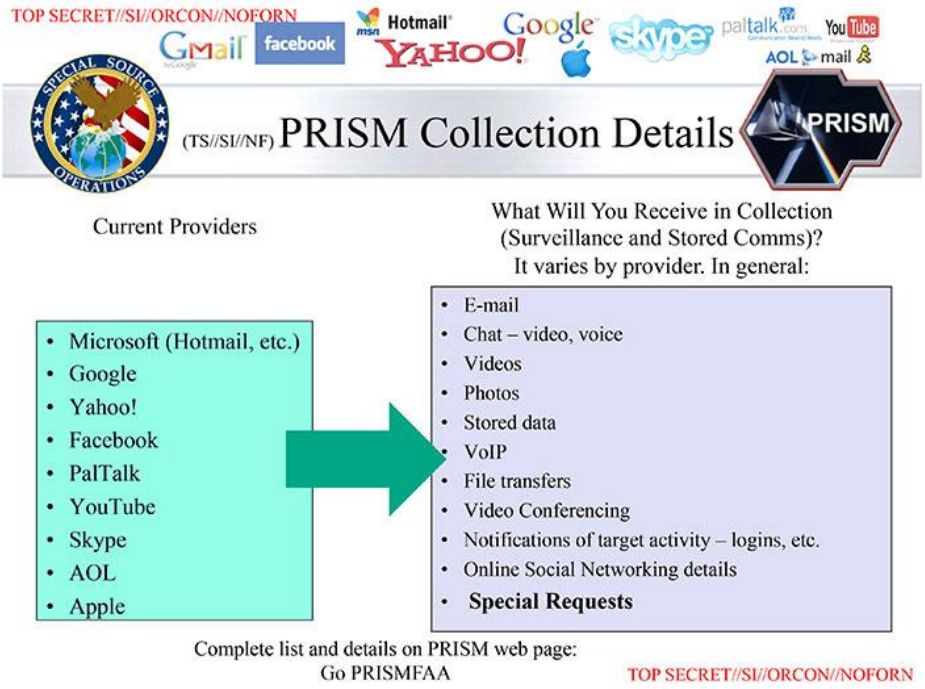
225 Ed Pilkington, "Edward Snowden: US would have buried NSA warnings forever," *The Guardian*, October 18, 2013, http://www.theguardian.com/world/2013/oct/18/edward-snowden-us-would-have-buried-nsa-warnings-forever.

226 Brenner, *America the Vulnerable*, 207.

227 Nakashima, *U.S. officials dodge questions on scope of surveillance*.

Covert conditions are a requirement for successful intelligence-gathering. When secrecy is compromised, access to important cyber intelligence sources are jeopardized. PRISM, for example, enabled the NSA to collect information directly from "nine of the biggest Internet companies," though the type of data extracted varied depending on each corporation's servers.[228]

**Figure 5: PRISM**[229]




The mine of "'user-generated content,'"[230] accessed through PRISM's corporate participants, enables the United States to search a wider breadth of information through

228 Anonymous, "NSA slides explain the PRISM data-collection program," *The Washington Post*, July 10, 2013, http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/. It is worth nothing that the corporations listed denied giving the NSA "unlimited access to their servers." Instead, information is only transmitted to the NSA as legally required under the Foreign Intelligence Surveillance Act (FISA) and court orders. The majority of these companies (except Twitter) have also cooperated with the US government to make secure information sharing between the companies and the government easier. See: Greenwald, *No Place to Hide*, 109; Claire Cain Miller, "Tech Companies Concede to Surveillance Program," *The New York Times*, June 7, 2013, http://www.nytimes.com/2013/06/08/technology/tech-companies-bristling-concede-to-government-surveillance-efforts.html?pagewanted=all.

229 Anonymous, Washington Post, *NSA Slides Explain PRISM*.

relatively uncomplicated means.[231] For counterterrorist efforts, PRISM is a valuable tool in mapping out the interactions of foreigners "engaged in terrorist activities" both outside and inside the United States.[232] Each of PRISM's corporate participants has a significant online presence in a number of states. PRISM thus enables America to identify and track highly mobile, potentially global threats that operate outside of formal political channels.[233]

On the one hand, America's cyber capabilities, and by extension, the extent to which its Five Eyes partners can access these capabilities, were revealed to its adversaries. Snowden revealed both the objectives and the tradecraft of cyber espionage – what information the US and the Five Eyes are after and how they collect that information. As targets become aware of America's surveillance methods, they will likely change their cyber behaviour to conceal their intentions and actions.[234] Information subsequently gained from pursuing a compromised intelligence operation may be incomplete. Likewise, the leaks may have provided adversaries with information to mirror American surveillance techniques or evade the cyber watch of the US and its allies in cyberspace. In either case, the utility of these intelligence operations decreases and America must reformulate its methods to achieve similar security goals.

A complicating factor occurs when the spotlight cannot be contained and spreads to the Five Eyes partners. [235] Although the agency was officially acknowledged in 1983,

230 Bauman et al., *After Snowden*, 142.

231 Riley, *U.S. Government Hacks the World*.

232 Charlie Savage, Edward Wyatt, and Peter Baker, "U.S. Confirms That It Gathers Online Data Overseas," *The New York Times*, June 6, 2013, http://www.nytimes.com/2013/06/07/us/nsa-verizon-calls.html?pagewanted=all&_r=0.

233 GCHQ also had access to the PRISM.

234 Bauman et al., *After Snowden*, 124, 138.

235 Greg Weston, Glenn Greenwald, and Ryan Gallagher, "New Snowden docs show U.S. spied during G20 in Toronto," *CBC News*, December 1, 2013, http://www.cbc.ca/m/touch/news/story/1.2442448. See also: Susan Ormiston, "Canada's spying touches nerve in Brazil: Susan Ormiston," *CBC News*, October 15, 2013, http://www.cbc.ca/news/world/canada-s-spying-touches-nerve-in-brazil-susan-ormiston-1.2054334.

CSEC has remained "one of the most secret and secretive organizations in Canada."[236] Snowden not only leaked secret information about American intelligence operations, he also leaked information about one of its closest allies. One of the most damming leaks that sparked public outrage provided information on CSEC's ability to track Canadian individuals through airports using metadata on behalf of the NSA.[237] The organization that once remained in the shadows now had the public glare on it.

Following the leaks, Canada undertook a review of its cyber security architecture to not only understand how an insider leak from the US could compromise Canadian security, but also figure out how such a leak affects its relationship to the alliance.[238] While the alliance is arguably too valuable to abandon, adaptation is needed to ensure the alliance continues to optimally perform in a post-Snowden era.

A cyber attack occurs when the confidentiality, integrity, or accessibility of a network or system is compromised.[239] In the Snowden case, classified information was stolen and made available to unauthorized individuals compromising the secrecy (confidentiality) of the system. Although no government systems were damaged, these leaks highlight the fact that insiders need to be a consideration when assessing cyber security vulnerabilities. Constant scans and audits of government systems not only provides information on the types of external attacks and attackers,[240] it can also detect

236 Philip Rosen, "The Communications Security Establishment – Canada's Most Secret Intelligence Agency," *Parliamentary Information and Research Service, Library of Parliament,* September 1993, http://www.parl.gc.ca/Content/LOP/researchpublications/bp343-e.htm.

237 Greg Weston, Glenn Greenwald, and Ryan Gallagher, "Exclusive: CSEC used airport Wi-Fi to track Canadian travellers: Edward Snowden documents," *CBC News*, January 30, 2014, http://www.cbc.ca/news/politics/csec-used-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881. John Forster, CSEC Chief, vehemently argued that this leak was nothing more than a model, but sources have told CBC that this capability is indeed operational.

238 Canada, Standing Senate Committee on National Security and Defence, *Transcript of Proceedings (Meeting No. 4)*, 2nd sess., 41st Parliament, Meeting No. 4, 2013. http://www.parl.gc.ca/Content/SEN/Committee/412/secd/02ev-51162-e.htm?Language=E&Parl=41&Ses=2&comm_id=76. Testimony of Stephen Rigby, Security Advisor to the Prime Minister, Privy Council Office. See also: The Canadian Press, "Canadian cyberspy agency CSEC fretted about staff after Snowden leaks," *CBC News*, April 7, 2014, http://www.cbc.ca/news/politics/canadian-cyberspy-agency-csec-fretted-about-staff-after-snowden-leaks-1.2601410.

239 Winterfield and Andress, *The Basics of Cyber Warfare*, 101.

240 The White House, *Foreign Policy Cyber Security*.

unusual patterns of activity internally.[241] If governments direct their attention towards only detecting external threats, insiders can continue their activities undetected to compromise system confidentiality over a prolonged period of time.[242] Not every government worker or contractor will become an insider threat but attentiveness to this possibility enhances a state's situational awareness to better defend its networks and systems.

Insiders who compromise confidentiality weaken the ability of a state to execute covert intelligence operations by mobilizing increased public scrutiny. The objectives of a cyber strategy must include protection against cyber vulnerabilities in networks and systems used in government. Insiders who leak secret information compromise the ability of a state to implement the necessary measures to enhance cyber security. As a result, the unimpeded execution of cyber strategy, action, and cooperation in an alliance situation becomes challenged.

## 5.4. Maximizing the Impact of the Five Eyes

State-to-state espionage is an enduring activity[243] made easier in cyberspace. Sharing information, while necessary, is also a strategy to ensure America can collect and act on intelligence it needs to maintain a consistent competitive edge in cyber. Holding information back allows the US to unilaterally act on its national security objectives without impediment.[244] At the same time, collecting more data and assessments from its partners enables a fuller understanding of the threat yet sidelines decisive action.[245] Likewise, increased partner access to US intelligence undermines America's monopoly on the valuable information it independently collected[246] and creates cascading effects when compromised. Yet, despite these initial disadvantages,

241 Winterfield and Andress, *The Basics of Cyber Warfare*, 102-104.

242 Freeze and Taber, *Mole Had Access to Wealth of CSIS, RCMP, Privy Council Files*.

243 Nye, *Future of Power*, 148.

244 Lander, *International Intelligence Cooperation*, 493.

245 Ibid., 491-492.

246 Sims, *Foreign Intelligence Liaison*, 197.

the opportunities for accessing more information increase once the US leverages the "regional access or specialist exper[tise]"[247] of each partner. The US must thus navigate the security and vulnerability implications of sharing information.

America can leverage cooperative sharing by prioritizing a threat (or an intelligence target) within the Five Eyes by sharing information first. In doing so, the United States can structure the intelligence sharing process in a way that mobilizes its partners against an American-dictated "collective" threat. As a result, the US is able to influence the alliance's intelligence agenda to benefit American security interests. Strategically sharing information with the Five Eyes thus enables America to exert influence over its partners' intelligence activities[248] to create long-term conditions that further American security interests. While each alliance member operates on self-interest, America can structure the relationship so that it likely benefits the most from sharing information.[249]

247 Clough, *Quid Pro Quo*, 604.

248 Sims, *Foreign Intelligence Liaison*, 199.

249 Richelson, *Calculus of Intelligence Cooperation*, 307.

# Chapter 6.

# Conclusion

Finding and using information first is key to remaining competitive in cyberspace. Security in cyber is not absolute. Instead, it requires a careful tipping of security away from a position of vulnerability into a position of informational advantage. Such a seesaw requires that the US manage short term insecurity to support a long term security gain – a challenge given that information proliferates and changes at fibre optic speeds in cyber.

The Internet has made information seeking easier given its lax security structure that privileges offense over defence. Where the US once relied on its own ingenuity to support its national security innovations, it can now also purchase the necessary tools keep up with its peer competitors in cyberspace. Buying zero days in the vulnerabilities market thus serves a dual purpose: it takes away potential attack tools from its adversaries while building America's own cyber arsenal. The problem, however, is that zero days may not work when you need them. Unlike nuclear or conventional weapons, there is no guarantee that an acquired zero-day can remain dormant yet functional. As a result, the US must consistently discover and collect zero-days to maintain a deployable cyber arsenal.

America, despite its cyber superiority, cannot credibly threaten to use crushing cyber power to defeat its adversaries without revealing part of its capabilities. Compounding this problem is the fact that a cyber attack alone, while disruptive, is survivable at this time. America is thus experiencing a shift in its security strategy, albeit incrementally. What previously worked in the physical domain does not necessarily translate into successful primacy in the electronic domain. Although Cold War models of deterrence by denial and retribution may help frame the cyber problem, these models

will eventually need to give way to new thinking about security in cyberspace. Deterrence, despite its Cold War successes, is not enough to stop your adversaries from attacking you in cyberspace.

Instead, resiliency to absorb a cyber attack will carry America further in securing a net security advantage. While absorbing attacks seems counterintuitive, it is a short term risk that will garner important information. Resiliency then is as much about learning about your adversaries, their capabilities, and targets, and it is about comparatively measuring your own vulnerabilities and strengths in cyber offense and defence. The more information America can acquire, the better equipped it will be to face the cyber threat.

Preparations for kinetic conflict are likely to begin in cyberspace as states collect vast information about their adversaries. Tapping into the millions of gigabytes of data that passes through the Internet is necessary to help America build a better picture of its adversaries' actions and intent, including "the readiness of foreign militaries."[250] America, despite its cyber sophistication, cannot undertake such a task alone.[251] Instead, the United States strategically shares information and capabilities with its partners to influence the intelligence priorities of the Five Eyes.[252] Sharing initially puts the United States in a vulnerable position – exclusive control over a part of its cyber capabilities are conceded to its partners. From a vulnerable position, American cyber power can nevertheless influence conditions necessary to execute innovative, albeit high risk, intelligence operations.

Information gathered from cyber can both reflect the strengths and weaknesses of America's (and by extension, its adversaries') offensive and defensive capabilities both within and outside cyberspace. Amassing an informational advantage to use against its adversaries will enable the US to enhance its security posture. Information, as the new realm of cyber security illustrates, is still a growing foundation of power.

250 Riley, *U.S. Government Hacks the World*.

251 Cox, *Canada and the Five Eyes*, 6.

252 Sims, *Foreign Intelligence Liaison*, 199.

Leveraging information in cyberspace is key to producing a long-term net gain in security. In seeking a cyber advantage, the United States must endure short-term cyber insecurity. Tipping the security seesaw may not produce immediate advantages but instead, can be understood as a step towards long-term security. Consistently working to tip the seesaw towards advantage, while managing the associated vulnerabilities, helps produce a long-term advantage. The US' ability to enhance its cyber posture while managing the associated vulnerabilities ultimately produces a net gain in national security.

# References


Ablon, Lillian, Martin C. Libicki, and Andrea A. Golay. *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar.* Santa Monica: RAND Corporation, 2014.

Anonymous. "Hackers Inc; Cybercrime." *The Economist*, July 12, 2014. http://search.proquest.com.proxy.lib.sfu.ca/docview/1544844816?accountid=13800.

Anonymous. "Masters of the cyber-universe; Cyber-hacking." *The Economist*, April 6, 2013. http://search.proquest.com.proxy.lib.sfu.ca/docview/1324420283?accountid=13800.

Anonymous. "NSA slides explain the PRISM data-collection program." *The Washington Post*, July 10, 2013. http://www.washingtonpost.com/wpsrv/special/politics/prism-collection-documents/.

Anonymous. "Secret Documents Reveal N.S.A. Campaign Against Encryption." *The New York Times*, September 5, 2013. http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html?ref=us.

Anonymous. "Sigint – how the NSA collaborates with technology companies." *The Guardian*, September 5, 2013. http://www.theguardian.com/world/interactive/2013/sep/05/sigint-nsa-collaborates-technology-companies.

Anonymous. "The Digital Arms Trade." *The Economist*, March 30, 2013. http://www.economist.com/news/business/21574478-market-software-helps-hackers-penetrate-computer-systems-digital-arms-trade.

Andrews, Wilson, and Todd Lindeman. "$52.6 billion: The Black Budget." *The Washington Post*, August 29, 2013. http://www.washingtonpost.com/wp-srv/special/national/black-budget/.

Ball, James, Julien Borger, and Glenn Greenwald. "Revealed: how US and UK spy agencies defeat internet privacy and security." *The Guardian*, September 6, 2013. http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

Bamford, James. "NSA Snooping Was Only the Beginning. Meet the Spy Chief Leading Us Into Cyberwar." *Wired Magazine*, June 12, 20113. http://www.wired.com/2013/06/general-keith-alexander-cyberwar/all/.

---. “The Most Wanted Man in the World,” *Wired Magazine*, August 2014, http://www.wired.com/2014/08/edward-snowden/.

Barford, P., M. Dacier, T.G. Dietterich, M. Fredrikson, J. Giffin, S. Jajodia, S. Jha, J. Li, P. Liu, P. Ning, X. Ou, D. Song, L. Strater, V. Swarup, G. Tadda, C. Wang, and J. Yen. “Cyber SA: Situational Awareness for Cyber Defence.” In *Cyber Situational Awareness: Issues and Research*, edited by Sushil Jajodia, Peng Liu, Vipin Swarup, and Cliff Wang, 3-14. New York: Springer, 2010.

Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jarbi, David Lyon, and R.B.J. Walker. “After Snowden: Rethinking the Impact of Surveillance.” *International Political Sociology* 8, no. 2 (2014): 121-144. DOI: 10.1111/ips.12048.

Beaumont, Peter, and Nick Hopkins. “International: Obama ordered cyberwar against Iran: Nuclear programme main target of computer worms: Speculation grows over timing of revelations.” *The Guardian (London)*, June 2, 2012. http://www.lexisnexis.com.proxy.lib.sfu.ca/hottopics/lnacademic/?shr=t&csi=138620&sr=HLEAD(international%3A%20obama%20ordered%20cyberwar%20against%20iran%3A%20nuclear%20programme%20main%20target%20of%20computer%20worms%3A%20speculation%20grows%20over%20timing%20of%20revelations)%20AND%20DATE%20IS%202012-06-02.

Betts, Richard K. “The Lost Logic of Deterrence: What the Strategy That Won the Cold War Can – and Can’t – Do Now.” *Foreign Affairs* 92, no. 2 (2013). http://www.foreignaffairs.com/articles/138846/richard-k-betts/the-lost-logic-of-deterrence.

---. “The New Threat of Mass Destruction.” *Foreign Affairs* 77, no. 1 (1998): 26-41. http://www.jstor.org.proxy.lib.sfu.ca/stable/20048360.

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. DOI: 10.1145/2382196.2382284.

Brenner, Joel. *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. New York: The Penguin Press, 2011.

Bryant, William D. “Cyberspace Superiority: A Conceptual Model.” *Air & Space Power Journal* 27, no. 6 (2013): 25-44. http://web.b.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=14c3f4cd-cefb-4649-999c-9af8fe8a5129%40sessionmgr198&vid=2&hid=120.

Canada. Parliament. Senate. Standing Senate Committee on National Security and Defence. *Transcript of Proceedings*. 1st sess., 41st Parliament, Meeting No. 15, 2012. http://www.parl.gc.ca/Content/SEN/Committee/411/secd/10ev-49784-e.htm?Language=E&Parl=41&Ses=1&comm_id=76.

Canada. Parliament. Senate. Standing Senate Committee on National Security and Defence. *Transcript of Proceedings*. 2nd sess., 41st Parliament, Meeting No. 4, 2013. http://www.parl.gc.ca/Content/SEN/Committee/412/secd/02ev-51162-e.htm?Language=E&Parl=41&Ses=2&comm_id=76.

Canada. Treasury Board of Canada Secretariat, *2014–15 Estimates: Parts I and II The Government Expenditure Plan and Main Estimates*, 2014, http://www.tbs-sct.gc.ca/ems-sgd/me-bpd/20142015/me-bpd-eng.pdf.

Carr, Jeffrey. *Inside Cyber Warfare: Mapping the Cyber Underworld*. Senastopol, Calif.: O'Reilly Media, Inc., 2012.

Cilluffo, Frank J., and Sharon L. Cardash. "Cyber Domain Conflict in the 21st Century." *Journal of Diplomacy & International Relations* 14, no. 1 (2013): 41-47. http://web.a.ebscohost.com.proxy.lib.sfu.ca/ehost/pdfviewer/pdfviewer?sid=afc29b59-f544-41c0-9fc4-4ad4f4533612%40sessionmgr4002&vid=2&hid=4201.

Clarke, Richard, and Robert K. Knake. *Cyber War: The Next Threat to National Security and What To Do About It*. New York: Ecco, 2010.

Clayton, Mark. "Chinese cyberattacks hit key US weapons systems. Are they still reliable?." *The Christian Science Monitor*, May 28, 2013. http://www.csmonitor.com/USA/Military/2013/0528/Chinese-cyberattacks-hit-key-US-weapons-systems.-Are-they-still-reliable.

---. "Stealing US Business Secrets: Experts ID Two Huge Cyber 'Gangs' in China." *The Christian Science Monitor*, September 14, 2012. http://www.lexisnexis.com.proxy.lib.sfu.ca/hottopics/lnacademic/?shr=t&csi=7945&sr=HLEAD(stealing%20us%20business%20secrets%3A%20experts%20id%20two%20huge%20cyber%20%27gangs%27%20in%20china)%20AND%20DATE%20IS%202012-09-14.

---. "Stuxnet cyberweapon set to stop operating." *Christian Science Monitor*, June 23, 2012. Academic Search Premier (77249946).

Clemente, Dave. "Cyber Security as a Wicked Problem." *The World Today* 67, no. 10 (2010): 15-17. http://web.a.ebscohost.com.proxy.lib.sfu.ca/ehost/pdfviewer/pdfviewer?sid=7660ec52-cf64-4e67-b87a-9d184245f62f%40sessionmgr4001&vid=2&hid=4114.

Clough, Chris. "Quid Pro Quo: The Challenge of International Strategic Intelligence Cooperation." *International Journal of Intelligence and CounterIntelligence* 17, no. 4 (2004): 601-613. DOI: 10.1080/08850600490446736.

Collins, Sean, and Stephen McCombie. "Stuxnet: The Emergence of a New Cyber Weapon and its Implications." *Journal of Policing, Intelligence, and Counter Terrorism* 7, no. 1 (2012): 80-91. DOI: 10.1080/18335330.2012.653198.

Cox, James. *Canada and the Five Eyes Intelligence Community*. Ottawa: Canadian Defense & Foreign Affairs Institute, 2012.

Crookes, David. “RIP Windows XP: the ‘zombie’ operating system that came to haunt Microsoft.” *The Independent*, March 25, 2014. http://www.independent.co.uk/life-style/gadgets-and-tech/features/goodbye-windows-xp-9213134.html.

Davidson, Jacob. “China Accuses U.S. of Hypocrisy on Cyberattacks.” *Time*, July 1, 2013. http://world.time.com/2013/07/01/china-accuses-u-s-of-hypocrisy-on-cyberattacks/.

Deibert, Ronald J. *Black Code: Surveillance, Privacy, and the Dark Side of the Internet*. Toronto: McClelland & Stewart, 2013.

Div, Lior. “The Five Most Common Cyberattack Myths – Revealed.” *Forbes*, September 11, 2014. http://www.forbes.com/sites/frontline/2014/09/11/the-five-most-common-cyberattack-myths-revealed/.

Farewell, James P., and Rafal Rohozinski. “The New Reality of Cyber War.” *Survival: Global Politics and Strategy* 54, no. 4 (2012): 107-120. DOI: 10.1080/00396338.2012.709391.

Freeze, Colin. “Spy agency’s budget to hit $460-million after ‘steady path’ of growth.” *The Globe and Mail*, November 12, 2013. http://www.theglobeandmail.com/news/politics/spy-agencys-budget-to-hit-460-million-after-steady-path-of-growth/article15385168/

Frei, Stefan. *The Known Unknowns: Empirical Analysis of Publicly Unknown Security Vulnerabilities*. Austin, TX: NSS Labs, 2013.

Fung, Brian. “The NSA hacks other countries by buying millions of dollars’ worth of computer vulnerabilities.” *The Washington Post*, August 31, 2013. http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/31/the-nsa-hacks-other-countries-by-buying-millions-of-dollars-worth-of-computer-vulnerabilities/.

Gartzke, Erik. “The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth.” *International Security* 38, no. 2 (2013): 41-73. http://muse.jhu.edu.proxy.lib.sfu.ca/journals/international_security/v038/38.2.gartzke.pdf.

Gaycken, Sandro, and Felix Fx Linder. “Zero-Day Governance: An (Inexpensive) Solution to the Cyber-security Problem.” Paper presented at the *Cyber Dialogue 2012: What is Stewardship in Cyberspace?*, Toronto, March 18-19, 2012. http://www.cyberdialogue.citizenlab.org/wp-content/uploads/2012/2012papers/CyberDialogue2012_gaycken-lindner.pdf.

Geers, Kenneth. “The challenge of cyber attack deterrence.” *Computer Law & Security Review* 26, no. 3 (2010): 298-303. http://dx.doi.org/10.1016/j.clsr.2010.03.003.

---. “Cyber Weapons Convention.” *Computer Law & Security Review* 26, no. 5 (2010): 547-551. DOI: 10.1016/j.clsr.2010.07.005.

Gellman, Barton, and Greg Miller. “U.S. spy network’s successes, failures and objectives detailed in ‘black budget’ summary.” *The Washington Post*, August 29, 2013. http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_print.html.

Gjelten, Tom. “First Strike: US Cyber Warriors Seize the Offensive.” *World Affairs* 175, no. 5 (2013): 33-43. http://web.b.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=b33eb3d2-62d2-4cf8-97a9-0a85598d0ea6%40sessionmgr110&vid=2&hid=120.

Glenny, Misha, and Camino Kavanagh. “800 Titles but No Policy – Thoughts on Cyber Warfare.” *American Foreign Policy Interests* 34, no. 6 (2012): 287-294. http://dx.doi.org/10.1080/10803920.2012.742410.

Greenberg, Andy. “Shopping for Zero-Days: A Price List For Hackers’ Secret Software Exploits.” *Forbes*, March 23, 2012. http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/.

Greenwald, Glenn. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. Toronto: Signal/McClelland & Stewart, 2014.

Gorman, Siobhan, August Cole, and Yochi Dreazen. “Computer Spies Breach Fighter-Jet Project.” *The Wall Street Journal*, April 21, 2009. http://www.wsj.com/articles/SB124027491029837401.

Hamre, John, James Lewis, and Gen. Keith Alexander. “CSIS Cybersecurity Policy Debate Series: U.S. Cybersecurity Policy and the Role of U.S. CYBERCOM.” *Center for Strategic and International Studies*, June 3, 2010. http://csis.org/files/attachments/100603csis-alexander.pdf.

Harris, Shane. “Black Market for Malware and Cyber Weapons is Thriving.” *Foreign Policy*, March 25, 2014. http://complex.foreignpolicy.com/posts/2014/03/24/black_market_for_malware_and_cyber_weapons_is_thriving.

---. “The Cyberwar Plan.” *National Journal*, November 14, 2009. EBSCOhost (45266379).

Hirsh, Michael. “Fear of Cyberwar Attack May Be Biggest Threat.” *National Journal*, July 23, 2011. Academic Search Premier (03604217).

Hopkins, Nick, and Julian Borger. “Exclusive: NSA pays £100m in secret funding for GCHQ.” *The Guardian*, August 1, 2013. http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden.

Hosenball, Mark. “NSA chief says Snowden leaked up to 200,000 secret documents.” *Reuters*, November 14, 2013. http://www.reuters.com/article/2013/11/14/us-usa-security-nsa-idUSBRE9AD19B20131114.

Hunt, Edward. “US Government Computer Penetration Programs and the Implications for Cyberwar.” *IEEE Annals of the History of Computing* 34, no. 4 (2012): 4-21. http://muse.jhu.edu/journals/ahc/summary/v034/34.3.hunt.html.

Hymans, Jacques E.C. “The Threat of Nuclear Proliferation: Perception and Reality.” *Ethics & International Affairs* 27, no. 3 (2013): 281-298. http://dx.doi.org.proxy.lib.sfu.ca/10.1017/S089267941300021X.

Jackson, William. “Einstein 3 goes live with automated malware blocking.” *GCN*, July 24, 2013. http://gcn.com/Articles/2013/07/24/Einstein-3-automated-malware-blocking.aspx?Page=1.

Kallberg, Jan, and Bhavani Thuraisingham. “Cyber Operations: Bridging from Concept to Cyber Superiority.” *Joint Force Quarterly* 1, no. 68 (2013): 53-58. http://web.a.ebscohost.com.proxy.lib.sfu.ca/ehost/pdfviewer/pdfviewer?sid=97a30f8e-0c55-449c-b007-ab718b40ff96%40sessionmgr4001&vid=2&hid=4114.

Kemp, R. Scott. “Cyberweapons: Bold steps in a digital darkness?.” *Bulletin of the Atomic Scientists*, June, 7, 2012. http://thebulletin.org/cyberweapons-bold-steps-digital-darkness.

Keysan Jay P., and Carole M. Hayes. “Mitigative Counterstriking: Self-Defence and Deterrence in Cyberspace.” *Harvard Journal of Law & Technology* 25, no. 2 (2012): 429-543. http://jolt.law.harvard.edu/articles/pdf/v25/25HarvJLTech429.pdf.

Lander, Stephen. “International Intelligence Cooperation: An Inside Perspective.” *Cambridge Review of International Affairs* 17, no. 3 (2004): 481-493. http://dx.doi.org/10.1080/0955757042000296964.

Lee, John. “Cyber Kleptomaniacs: Why China Steals Our Secrets.” *World Affairs* 173, no. 3 (2013): 73-79. http://web.a.ebscohost.com.proxy.lib.sfu.ca/ehost/pdfviewer/pdfviewer?sid=77656d24-1890-43fe-8870-d893bcbe6282%40sessionmgr4001&vid=2&hid=4114.

Lefebvre, Stéphane. “The Difficulties and Dilemmas of International Intelligence Cooperation.” *International Journal of Intelligence and CounterIntelligence* 16, no. 4 (2003): 527-542. DOI: 10.1080/716100467.

Lewis, James A. *Conflict and Negotiation in Cyberspace*. Washington, DC: Centre for Strategic and International Studies, 2013.

---. *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency*. Washington, DC: Center for Strategic and International Studies, 2008.

Lindsay, Jon R. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* 22, no. 3 (2013): 365-404. DOI: 10.1080/09636412.2013.816122.

Libicki, Martin C*. Brandishing Cyberattack Capabilities*. Santa Monica: RAND Corporation, 2013.

---. *Cyberdeterrence and Cyberwar*. Santa Monica: RAND Corporation, 2009.

---. "The Nature of Strategic Instability in Cyberspace." *Brown Journal of World Affairs* 18, no. 1 (2011): 71-79. http://web.a.ebscohost.com.proxy.lib.sfu.ca/ehost/pdfviewer/pdfviewer?sid=45db41c8-21a1-486d-8613-deccbb90cfb4%40sessionmgr4002& vid=2&hid=4114.

Lynn III, William J. "Defending a New Domain." *Foreign Affairs* 89, no. 5 (2010). http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain.

Menn, Joseph. "Special Report: U.S. cyberwar strategy stokes fear of blowback." *Reuters*, May 10, 2013. http://www.reuters.com/assets/print?aid=USBRE9490EL20130510.

Markoff, John, David E. Sanger, and Thom Shanker. "In Digital Combat, U.S. Finds No Easy Deterrent." *The New York Times*, January 26, 2010. http://search.proquest.com.proxy.lib.sfu.ca/docview/1461079100?accountid=13800.

Metz, Cade. "Facebook Says It's Now as Big as Windows (Literally)." *Wired Magazine*, April 30, 2013. http://www.wired.com/wiredenterprise/2013/04/facebook-windows/.

Miller, Claire Cain. "Tech Companies Concede to Surveillance Program." *The New York Times*, June 7, 2013. http://www.nytimes.com/2013/06/08/technology/tech-companies-bristling-concede-to-government-surveillance-efforts.html?pagewanted=all.

Nakashima, Ellen. "Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies." *The Washington Post*, May 27, 2013. http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html?hpid=z1.

---. “U.S. officials dodge questions on scope of surveillance.” *The Washington Post*, September 26, 2013. http://www.washingtonpost.com/world/national-security/nsa-leaks-extremely-damaging-national-intelligence-director-tells-senate-hearing/2013/09/26/a01b4e08-26d3-11e3-b75d-5b7f66349852_story.html.

Nakashima, Ellen, and Joby Warrick. “For NSA chief, terrorist threat drives passion to ‘collect it all.’” *The Washington Post*, July 14, 2013. http://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html.

National Security Agency. “Signals Intelligence.” *National Security Agency/Central Security Service.* September 9, 2011. http://www.nsa.gov/sigint/.

National Security Agency. “UKUSA Agreement Release 1940-1956.” *National Security Agency*. June 24, 2010. http://www.nsa.gov/public_info/declass/ukusa.shtml.

Nye, Joseph. “Nuclear Lessons for Cyber Security?.” *Strategic Studies Quarterly* 5, no. 4 (2011): 18-38. http://www.au.af.mil/au/ssq/2011/winter/nye.pdf.

Nye, Jr., Joseph S. *The Future of Power*. New York: Public Affairs, 2011.

Ormiston, Susan. “Canada's spying touches nerve in Brazil: Susan Ormiston.” *CBC News*, October 15, 2013. http://www.cbc.ca/news/world/canada-s-spying-touches-nerve-in-brazil-susan-ormiston-1.2054334.

PC Tools by Symantec, “What is a Zero-Day Vulnerability?,” *PC Tools*, http://www.pctools.com/security-news/zero-day-vulnerability/.

Perlroth, Nicole, Jeff Larson, and Scott Shane. “N.S.A Able to Foil Basic Safeguards of Privacy on Web.” *The New York Times*, September 5, 2013. http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?hp&_r=1&&pagewanted=print.

Perlroth, Nicole, and David E. Sanger. “Nations Buying as Hackers Sell Knowledge of Software Flaws.” *The New York Times*, July 14, 2013. http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html.

Pilkington, Ed. “Edward Snowden: US would have buried NSA warnings forever.” *The Guardian*, October 18, 2013. http://www.theguardian.com/world/2013/oct/18/edward-snowden-us-would-have-buried-nsa-warnings-forever.

Pincus, Walter. “NSA System Inoperative For Four Days; Computer Glitch Halted Data Interpretation.” *The Washington Post*, January 30, 2000. http://www.lexisnexis.com.proxy.lib.sfu.ca/hottopics/lnacademic/?shr=t&csi=8075&sr=HLEAD(nsa%20system%20inoperative%20for%20four%20days%3B%20computer%20glitch%20halted%20data%20interpretation)%20AND%20DATE%20IS%202000-01-30.

Porteous, Holly. *Cybersecurity and Intelligence: The U.S. Approach (Background Paper)*. Ottawa: Library of Parliament, 2011.

Rains, Tim. “The Risk of Running Windows XP After Support Ends April 2014.” *Microsoft Security Blog*, August 15, 2013. http://blogs.technet.com/b/security/archive/2013/08/15/the-risk-of-running-windows-xp-after-support-ends.aspx.

Richelson, Jeffrey T. “The Calculus of Intelligence Cooperation.” *International Journal of Intelligence and CounterIntelligence* 4, no. 3 (1990): 307-323. DOI: 10.1080/08850609008435147.

Rid, Thomas. “Cyberwar and Peace,” *Foreign Affairs* 96, no. 6 (2013). http://www.foreignaffairs.com/articles/140160/thomas-rid/cyberwar-and-peace.

Riley, Michael. “How the U.S. Government Hacks the World.” *Bloomberg BusinessWeek*, May 23, 2013. http://www.businessweek.com/printer/articles/119394-how-the-u-dot-s-dot-government-hacks-the-world.

---. “U.S. Agencies Said to Swap Data With Thousands of Firms.” *Bloomberg*, June 15, 2013. http://www.bloomberg.com/news/print/2013-06-14/u-s-agencies-said-to-swap-data-with-thousands-of-firms.html.

Rosen, Philip. “The Communications Security Establishment – Canada’s Most Secret Intelligence Agency.” *Parliamentary Information and Research Servic*e, *Library of Parliament,* September 1993. http://www.parl.gc.ca/Content/LOP/researchpublications/bp343-e.htm.

Rosenfield, Daniel K. “Rethinking Cyber War.” *Critical Review: A Journal of Politics and Society* 21, no. 1 (2009): 77-90. DOI: 10.1080/08913810902812156.

Rudner, Martin. “Canada’s Communications Security Establishment from Cold War to Globalization.” *Intelligence and National Security* 16, no. 1 (2001): 97-128. DOI: 10.1080/714002836.

Samaan, Jean-Loup. “Cyber Command: The Rift in US Military Cyber-Strategy.” *The Rusi Journal* 155, no. 6 (2010): 16-21. DOI: 10.1080/03071847.2010.542664.

Sanger, David E. *Confront and Conceal: Obama’s Secret Wars and the Surprising Use of American Power*. New York: Crown Publishers, 2012.

---. “Obama Lets N.S.A. Exploit Some Internet Flaws, Officials Say.” *The New York Times*, April 12, 2014. http://nyti.ms/1gmYqOm.

---. “Obama Order Sped Up Wave of Cyberattacks Against Iran.” *The New York Times*, June 1, 2012. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

Savage, Charlie, Edward Wyatt, and Peter Baker. “U.S. Confirms That It Gathers Online Data Overseas.” *The New York Times*, June 6, 2013. http://www.nytimes.com/2013/06/07/us/nsa-verizon-calls.html?pagewanted=all&_r=0.

Shachtman, Noah, and Peter W. Singer. “The Wrong War.” *Government Executive* 43, no. 10 (2011). http://web.ebscohost.com.proxy.lib.sfu.ca/bsi/detail?sid=580dc088-da1b-4cda-b35d-12363b5600b4%40sessionmgr114&vid=2&hid=122&bdata=JnNpdGU9YnNpLWxpdmUmc2NvcGU9c2l0ZQ%3d%3d#db=bth&AN=65089376.

Simonite, Tom. “Chinese Hacking Team Caught Taking Over Decoy Water Plant.” *MIT Technology Review*, August 2, 2013. http://www.technologyreview.com/news/517786/chinese-hacking-team-caught-taking-over-decoy-water-plant/.

Sims, Jennifer E. “Foreign Intelligence Liaison: Devils, Deals, and Details.” *International Journal of Intelligence and CounterIntelligence* 19, no. 2 (2006): 195-217. DOI: 10.1080/08850600500483657.

Singer, Peter W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press, 2013.

Singer, Peter W. “The "Oceans 11" of Cyber Strikes.” *Brookings Institution*. May 2012. http://www.brookings.edu/research/articles/2012/05/21-cyber-threat-singer.

---. *Wired for War: The Robotics Revolution and Conflict in the 21st Century.* New York: Penguin Press, 2009.

Stockton, Paul N., and Michele Golabek-Goldman. “Curbing the Market for Cyber Weapons,” *Yale Law and Policy Review* 32, no. 1 (2013): 239-266. http://web.a.ebscohost.com.proxy.lib.sfu.ca/ehost/pdfviewer/pdfviewer?sid=a6bc7e20-de4d-47de-b922-03c1d7b80b6d%40sessionmgr4005&vid=1&hid=4104.

Symantec Security Response. “The Elderwood Project.” *Symantec Official Blog*, September 6, 2013. http://www.symantec.com/connect/blogs/elderwood-project.

The Canadian Press. “Canadian cyberspy agency CSEC fretted about staff after Snowden leaks.” *CBC News*, April 7, 2014. http://www.cbc.ca/news/politics/canadian-cyberspy-agency-csec-fretted-about-staff-after-snowden-leaks-1.2601410.

The Commission on the Theft of American Intellectual Property, *The IP Commission Report.* Seattle, WA: The National Bureau of Asian Research, 2013.

Thornburgh, Nathan, Matthew Forney, Brian Bennett, Timothy J. Burger, and Elaine Shannon. “The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them).” *Time Magazine*, September 5, 2005. http://web.a.ebscohost.com.proxy.lib.sfu.ca/ehost/detail/detail?sid=21192193-4446-4831-a689-832a617141b4%40sessionmgr4002&vid=4&hid=4206&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=aph&AN=18065208.

Timberg, Craig, and Ellen Nakashima. “Government computers running Windows XP will be vulnerable to hackers after April 8.” *The Washington Post*, March 16, 2014. http://www.washingtonpost.com/business/technology/government-computers-running-windows-xp-will-be-vulnerable-to-hackers-after-april-8/2014/03/16/9a9c8c7c-a553-11e3-a5fa-55f0c77bf39c_story.html.

United States Senate Committee on Armed Services. “Advance Questions for Vice Admiral Michael S. Rogers, USN Nominee for Commander, United States Cyber Command.” *United States Senate Committee on Armed Services*, March 11, 2014. http://www.armed-services.senate.gov/imo/media/doc/Rogers_03-11-14.pdf.

USA. Defense Science Board. *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*, 2013. http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.

USA. Department of Defense*. Department of Defense Strategy for Operating in Cyberspace*, 2011. http://www.defense.gov/news/d20110714cyber.pdf.

USA. National Security Agency. *NSA Intelligence Relationship with Canada’s Communications Security Establishment Canada*, 2013. http://www.cbc.ca/news2/pdf/nsa-canada-april32013.pdf.

USA. National Security Council. *The Comprehensive National Cybersecurity Initiative*, 2009. http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf.

USA. White House. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, 2011. http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

Weinberger, Sharon. “Is This the Start of Cyberwarfare?.” *Nature* 474, no. 7350 (2011): 142-145. DOI: 10.1038/474142a.

Weston, Greg, Glenn Greenwald, and Ryan Gallagher. “Exclusive: CSEC used airport Wi-Fi to track Canadian travellers: Edward Snowden documents.” *CBC News*, January 30, 2014. http://www.cbc.ca/news/politics/csec-used-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881.

---. “New Snowden docs show U.S. spied during G20 in Toronto.” *CBC News*, December 1, 2013. http://www.cbc.ca/m/touch/news/story/1.2442448.

---. “Snowden document shows Canada set up spy posts for NSA.” *CBC News*, December 10, 2013. http://www.cbc.ca/new s/politics/snowden-document-shows-canada-set-up-spy-posts-for-nsa-1.2456886.

Winterfeld, Steve and Jason Andress. *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice.* Waltham, Mass: Syngress, 2012.

Zetter, Kim. “Meet MonsterMind, the NSA Bot That Could Wage Cyberwar Autonomously,” *Wired Magazine*, August 13, 2014, http://www.wired.com/2014/08/nsa-monstermind-cyberwarfare/.

---. “Obama: NSA Must Reveal Bugs Like Heartbleed, Unless They Help the NSA.” *Wired Magazine*, April 15, 2014. http://www.wired.com/2014/04/obama-zero-day/.

---. “Sleuths Trace New Zero-Day Attacks to Hackers Who Hit Google.” *Wired Magazine*, September 7, 2012. http://www.wired.com/2012/09/google-hacker-gang-returns/all/.