THE SCHOOL OF PUBLIC POLICY

MASTER OF PUBLIC POLICY
CAPSTONE PROJECT

Developing a Cyberwarfare Capability for Canada: An Exploration of Seven Policy Rationales

Submitted by:

Erik Henningsmoen
September 8, 2017

Approved by Supervisor:

Dr. David J. Bercuson
September 13, 2017

Submitted in fulfillment of the requirements of PPOL 623 and completion of the requirements for the Master of Public Policy degree

UNIVERSITY OF CALGARY | THE SCHOOL OF PUBLIC POLICY

Capstone Approval Page

The undersigned, being the Capstone Project Supervisor, declares that

Student Name: Erik Henningsmoen

has successfully completed the Capstone Project within the

Capstone Course PPOL 623 A&B

David J. Bercuson

(Name of supervisor)

(Supervisor's signature)

Sept 13/2017

(Date)

UNIVERSITY OF CALGARY | THE SCHOOL OF PUBLIC POLICY

Acknowledgements

First of all, I would like to thank my supervisor Dr. David Bercuson for his mentorship and guidance during the writing of this capstone research project. Dr. Bercuson's expertise in defence policy and security issues were immensely helpful as I completed my research. When discussing anything cyber-related, every new development in the media can seem game-changing; a historian's perspective brings a degree of intellectual grounding when discussing issues such as cybersecurity and cyberwarfare.

I would also like to express my gratitude to Dr. Rei Safavi-Naini, Mr. Marc Kneppers, and Mr. Ryan Jepson for taking the time to share their thoughts and perspectives on Canadian cybersecurity issues with me.

I owe a special thank you to the faculty and staff at the School of Public Policy for creating such a challenging, yet supportive, and above all, stimulating environment to study public policy in. My classmates in the Master of Public Policy program have been fantastic colleagues and great friends. I could not have asked for a better group of people to "take the leap" and pursue graduate studies alongside.

Finally, I would like to thank my mother Sandra Henningsmoen for encouraging me to pursue university studies in the first place; and then for putting up with me over the years while I did so.

Table of Contents

TABLE OF CONTENTS

Capstone Executive summary ..... **v**

Part I – Introduction to Cybersecurity and Cyberwarfare **1-2**

Part II – Defining Cybersecurity and Cyberwarfare **2-9**
Cyberattacks 2-3
Actors and Motivations 4-5
The Nature of Cyberspace 5
Cyberwarfare 6-7
The Costs of Cyber Insecurity 7-9

PART III – Mapping Recent Canadian Cybersecurity Policy **10-23**
Canada's Cybersecurity Strategy 10-11
Digital Canada 150 12
The 2017 Public Consultation of Cybersecurity 12
Strategic Forecasting by Policy Horizons Canada 13
Coverage of Cybersecurity Issues in Canadian Politics 13
Coverage of Cybersecurity Issues in Parliament 13-14
Bill C-59 and Canadian Cyberwarfare Capabilities 14
Two Recent Canadian Senate Reports 15
Documented Cyberattacks on Federal Government IT Infrastructure 15-17
Communications Security Establishment Canadian Elections Cybersecurity Study 17
Communication and Security Establishment Cyber Capabilities? 18

Canada's Participation in the Budapest Convention 18-19
The 2017 Canadian Defence Policy Review 19-21
Operation REASSURANCE 21
Canadian Armed Forces Cyber Capabilities 21-22
Department of National Defence Cyber Procurement Activities 22-23

Part IV – Testing Theories of Cyberwarfare 23-34
Augment Conventional Military Capabilities 25-26
Cyber Confidence Game 26-28
Cyber Deterrence 28-30
Cyber Espionage and Cyber Sabotage 30-31
Tit-for-Tat Hacking 31-33
Keep Up with the Joneses 33-34

Part V – Legal Considerations 34-37
Cyberattacks during a State of Armed Conflict 35
Cyberattacks during the Absence of a State of Armed Conflict 35-37

Part VI – Conclusion 37-38

References 39-49

Capstone Executive Summary

In the past decade cybersecurity issues have progressed from being a niche technical area of public policy to a mainstream matter in public policy discourse. Concurrently, the specter of cyberwarfare has grown from being a speculative issue in the field of strategic studies, to common tool in international relations. States now pursue their national interests digitally through sophisticated hacking and cyberwarfare programs. Geopolitics has moved into cyberspace.

Canada has been a laggard in reacting to this new reality in strategic affairs. Both its domestic security and defence policies have been reactive to issues such as cybersecurity, critical infrastructure, and securing Canada's digital economy. Canadian policy in these areas has been developed in an incrementalist manner, and is naïve in the way it frames threats to Canadian security in cyberspace. Furthermore, it has been mute on the development Canadian cyberwarfare capabilities.

In June 2017 the Trudeau government published an updated defence policy white paper—named *Strong, Secure, Engaged: Canada's Defence Policy*—that will set the direction of the Canadian Armed Forces over the coming years. One of the most notable developments in this new defence policy is a new mandate for Canada's military to develop an offensive cyberwarfare capability. While the white paper provides few details on the specifics of such a capability, it does represent a leap in Canadian security thinking.

This paper will investigate whether such an offensive cyberwarfare capability, as called for in the 2017 defence white paper, will enhance Canada's national security. It does so by examining seven theories of why states develop cyberwarfare capabilities, and then tests these cyberwarfare rationales against Canada's unique strategic position in world affairs. The paper finds that an offensive cyberwarfare capability would enhance Canadian security by augmenting Canada's conventional military capabilities and signaling to Canada's allies that Canada is a sophisticated and dependable security partner. The paper concludes that the 2017 defence policy is a step in the right direction when it comes to defence and security policy.

PART I – INTRODUCTION TO CYBERSECURITY AND CYBERWARFARE

Cybersecurity, and the specter of cyberwarfare, are taking an increasingly prominent role in security policy discourse. Once considered a highly speculative and technical area of national security policy, cyberwarfare issues are manifesting themselves in geopolitical hotspots throughout the world. Cyberwarfare is no longer an emerging national security threat, but a geopolitical reality.

In recent high-profile cyberattacks over the past decade, state actors have used cyber-weapons to sabotage North Korea's ballistic missile program,[1] sabotage Iran's nuclear weapons program,[2] disrupt Syria's air defence system in preparation for an air attack on its nuclear weapons program,[3] cut off Estonia's Internet access,[4] and shut down Ukrainian power stations.[5] As cyber-weapons have proven their worth in contemporary conflict, it is reasonable to anticipate that further instances of state-on-state cyberattacks will take place in the near future.[6]

This paper will discuss Canada's cyberwarfare policy options and will explore the policy rationale for Canada to develop offensive cyberwarfare capabilities. The paper will do so by first discussing modern cyber issues and terminology such as *cybersecurity* and *cyberwarfare*. The paper will then map out current Canadian cybersecurity policy. Finally, the paper will explore seven theories on why states develop offensive cyberwarfare capabilities, and test these theories to determine if any of them fit Canada's unique security context.

---

[1] David E. Sanger and William J. Broad, "Hand of U.S. Leaves North Korea's Missile Program Shaken," *New York Times*, April 18, 2017, https://www.nytimes.com/2017/04/18/world/asia/north-korea-missile-program-sabotage.html; David E. Sanger and William J. Broad, "Trump Inherits a Secret Cyberwar Against North Korean Missiles," *New York Times*, March 4, 2017, https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html?_r=0.
[2] Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired*, November 3, 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.
[3] Sharon Weinberger, "How Israel Spoofed Syria's Air Defence System," *Wired*, October 4, 2007, https://www.wired.com/2007/10/how-israel-spoo/.
[4] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired*, August 21, 2007, https://www.wired.com/2007/08/ff-estonia/.
[5] "Hackers Behind Ukraine Power Cuts, Says US Report," *BBC News*, February 26, 2016, http://www.bbc.com/news/technology-35667989; "Ukraine power cut 'was cyber-attack'," *BBC News*, January 11, 2017, http://www.bbc.com/news/technology-38573074.
[6] For a good discussion on how states are increasingly turning cyberspace into a battlespace, see Alexander Klimburg, *The Darkening Web: The War for Cyberspace* (New York: Penguin, 2017).

The paper finds that Canada would benefit from developing a modest offensive cyberwarfare capability. The newfound emphasis on cyberwarfare in the Trudeau government's 2017 Canadian defence policy is both appropriate and timely in today's international security environment.

The paper argues that acquiring an offensive cyberwarfare capability would contribute to Canada's national security by enhancing and complimenting Canada's conventional military capabilities, and signalling to its allies that Canada is a reliable and modern security partner that takes national defence and international security issues seriously. The paper concludes by briefly exploring some of the legal questions involved in pursuing offensive cyberwarfare capabilities.

PART II – DEFINING CYBERSECURITY AND CYBERWARFARE

Defining the concepts and issues surrounding cybersecurity, cyberspace, and cyberwarfare is an important part of understanding public policy in this area. Policy debate is often jumbled by technical language. While technical jargon is important, as it helps information technology professionals and policy wonks to communicate effectively amongst one another, it can also make debate on cybersecurity difficult for non-specialists to understand.

Cyberattacks

A cyberattack can be defined as "directed intrusions into computer networks to steal or alter information or damage the system."[7] Malicious computer code (viruses); unauthorized access to an information system through stolen or fraudulent access credentials; and overburdening the system with data requests—referred to as a distributed denial-of-service attack (DDoS)—are just a few of the ways in which networked computers and information systems can be attacked.

Cyberattacks can also include a human element, where an attacker will attempt to socially manipulate, or con, individuals into giving up sensitive information, such as passwords, to

[7] Michael Vatis, "The Next Battlefield: The Reality of Virtual Threats," *Harvard International Review* 28, no. 3 (Fall 2016): 57.

facilitate the attack. This social element to a cyberattack is referred to by cybersecurity professionals as social engineering.[8]

Cyberattacks vary in qualitative terms on a spectrum of the relatively crude and unsophisticated on the low end, to highly sophisticated operations that use numerous points of attack against multiple, and often previously unknown, computer network vulnerabilities at the high end. Attacks that target such previously unknown vulnerabilities in a computer network are known as zero-day attacks by cybersecurity practitioners.[9] These zero-days tend to be the most effective cyberattacks and are the most difficult to defend against—after all, how do you go about defending against a vulnerability in your network that you do not know exists?

These zero-days are collected, or stockpiled, by attackers for their operational needs and are very valuable. A 2007 investigation by information security researcher Charlie Miller found that government and defence industry buyers of zero-days were willing to pay prices in the hundreds of thousands of dollars for these exploits in popular computer operating systems and other software.[10]

Attacks of the highest sophistication may take months or even years to coordinate, cost millions of dollars, and may include actions in physical space, such as social engineering, in support of attacks taking place in cyberspace. In the cybersecurity literature, an actor who develops attacks of the highest sophistication is often referred as an advanced persistent threat (APT).[11] These APTs can be well-resourced criminal enterprises, but they are often militaries, intelligence agencies, and paramilitary units controlled and financed by states.[12]

---

[8] A comprehensive introduction to social engineering, in the context of information security, is provided by Christopher Hadnagy, *Social Engineering: The Art of Human Hacking* (Indianapolis: Wiley Publishing, 2011).
[9] Kim Zetter, "Hacker Lexicon: What is a Zero Day?," *Wired*, November 11, 2014, https://www.wired.com/2014/11/what-is-a-zero-day/.
[10] Charlie Miller, *The Legitimate Vulnerability Market: Inside the Secretive World of 0-day Exploit Sales* (Independent Security Evaluators, 2007), http://www.econinfosec.org/archive/weis2007/papers/29.pdf.
[11] P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014), 55-60.
[12] For a captivating account of investigating an APT linked to a Chinese cyberespionage campaign, see Rafal Rohozinski and Ronald Deibert, *Tracking GhostNet: Investigating a Cyber Espionage Network,* SecDev Group and Citizen Lab, Munk Centre for International Studies, University of Toronto, March 29, 2009, https://citizenlab.ca/2009/03/tracking-ghostnet-investigating-a-cyber-espionage-network/.

Actors and Motivations

Actors vary in motivations and capabilities, and include states, criminal enterprises, activist groups, and terrorist organizations. Cyberattacks at the lowest levels of sophistication are usually criminal in nature and are motivated by economic gain. However, cyberattacks are also carried out by state actors and violent non-state actors with political and ideological motivations.[13] There are currently an estimated 60 countries that have access to cyberattack capabilities.[14]

By using cyberwarfare to accomplish their goals, states have moved geopolitical competition amongst one another to the Internet and the world's computer networks. As former United States Secretary of State and foreign policy scholar Henry Kissinger observes, "The emphasis of many strategic rivalries is shifting from the physical to the information realm, in the collection and processing of data, the penetration of networks, and the manipulation of psychology."[15]

While most cyberattacks take place in the shadows of international relations, and are typically considered sensitive information by state security agencies, in the most extreme cases, a major cyberattack could be interpreted as an act of war.[16] While international norms around what constitutes an act of war in cyberspace are still not well-established, a June 2016 statement by North Atlantic Treaty Organization (NATO) Secretary General Jens Stoltenberg expressed the possibility that a severe cyberattack against one of NATO's member states could trigger collective action by the security alliance.[17]

But cyberwarfare or cyberattacks should not be construed entirely as acts of state violence. To date, nobody has died in a cyberattack, and no state has ever responded to a cyberattack with a physical, kinetic response. So far, conflict in cyberspace has been confined to the Internet and the world's computer networks, and has not escalated beyond this. Even serious

---

[13] Eneken Tikk, "Ten Rules for Cyber Security," *Survival* 53, no.3 (June-July 2011): 119.
[14] Jennifer Valentino-DeVries and Danny Yadron, "Cataloging the World's Cyberforces," *Wall Street Journal*, October 11, 2015, https://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710.
[15] Henry Kissinger, *World Order* (New York: Penguin Press, 2014): 347
[16] John Stone, "Cyber War Will Take Place!" *Journal of Strategic Studies* 36, no. 1 (2013): 107.
[17] "Massive Cyber Attack Could Trigger NATO Response: Stoltenberg," *Reuters*, June 15, 2016, http://www.reuters.com/article/us-cyber-nato-idUSKCN0Z12NE.

attacks, such as the 2010 Stuxnet attack by the United States and Israel against Iran's uranium enrichment program was not responded to by the Iranian government with physical reprisals.[18]

However, as states continue to enhance their cyberwarfare capabilities and use them against their geopolitical rivals with more frequency, this gap between attacks in cyberspace and kinetic attacks in physical space, that lead to death and destruction, can be expected to narrow.

The Nature of Cyberspace

Cyberspace is an abstract, and almost ethereal, term used to describe the place in which cyberattacks take place within. Cyberspace should not be simply thought of as a technology buzzword, however. Cyberspace is a real place of military and strategic affairs. Currently, the United States Department of Defence treats cyberspace as an operational domain akin to land, sea, air, and space.[19] Political scientist Joseph S. Nye characterises this new cyberspace domain as "both a new and volatile human-made environment."[20]

Cyberspace exists as digital signals—encoded packets of information—travelling machine-to-machine at the speed of light. But cyberspace also physically manifests itself in the hardware and wiring that make the Internet and computer networks possible.[21] In this way, cyberspace exists in parallel digital and physical states of existence. And furthermore, as RAND Corporation analyst Benjamin Lambeth argues, cyberspace also interacts with the other domains of warfare, "It is qualitatively different from land, sea, air, and space domains, yet it both overlaps and continuously operates within all four."[22]

---

[18] For two comprehensive accounts of the Stuxnet attacks against Iran's uranium enrichment program, see David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, 2nd ed. (New York: Broadway Books, 2013): 189-225; and Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown, 2014).
[19] Department of Defense (United States), *Department of Defense Strategy for Operating in Cyberspace*, July 2011, http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.
[20] Joseph S. Nye, *The Future of Power* (New York: Public Affairs, 2011): 150.
[21] Cyberspace's dual existence in both the digital and physical realms is described most eloquently in Andrew Blum, *Tubes: A Journey to the Center of the Internet* (Toronto: HarperCollins, 2012).
[22] Benjamin S. Lambeth, "Airpower, Spacepower, and Cyberpower," *Joint Forces Quarterly* 60 (First Quarter 2011): 50.

Cyberwarfare

Cyberwarfare can be conceptualized as using computers and computer infrastructure to infiltrate, modify, steal from, or attack a rival's computer network for strategic and political gain. The key distinction between cybercrime and cyberwarfare is the political element and strategic aims of the hacking. To be effective cyberwarfare capabilities must be integrated with a state's grand strategy and national security policy.[23]

Cybersecurity scholars typically categorize states' operational capabilities in cyberspace as follows:[24]

- *Computer network operations (CNO)*—cyberwarfare or cyber-intelligence gathering operations against a rival state's computer network, or defensive operations on one's own computer network. This is an umbrella term that can encompass computer network exploitation, computer network attack, and computer network defence activities.
- *Computer network exploitation (CNE)*—penetrating a target's computer networks in order to map a network or collect intelligence on an opponent's capabilities or intentions. This is often the first step in a state's cyberwarfare campaign against a rival's information systems. CNE activities help prepare a battlefield in cyberspace for future cyberattacks, and collect needed intelligence.
- *Computer network attack (CNA)*—destroying or paralyzing a target's computer network, or assets linked to its network. At the most extreme, this could mean attacking physical assets, such as critical infrastructure, through cyberspace.
- *Computer network defence (CND)*—defending a state's own computer network against an enemy's CNE or CNA operations. This could take place during a time of war or during peacetime. CND is typically talked about in the context of a military or protecting its own computer networks, but state security organizations could also be called upon to help in defending private sector networks against cyberattacks.

---

[23] Paul Cornish, David Livingstone, Dave Clemente, Claire Yorke, *On Cyberwarfare* (London: Chatham House, November 2010), https://www.chathamhouse.org/publications/papers/view/109508.
[24] Myriam Dunn Cavelty, "Cyberwar: Concept, Status Quo, and Limitations," *CSS Analysis in Security Policy*, no. 71, (April 2010), http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSS-Analyses-71.pdf.

From a strategic standpoint, the technical method of cyberattack is not an important factor in policy planning. What is more important are the motivations or aims of the attacker, and how the attacks relate to an attacker's overall goals. For a state actor such as Canada, an offensive cyberwarfare capability must be synchronized with a larger defence policy. An isolated cyberattack (either CNE or CNA) that is not linked to a state's overarching goals would not be effective, and may even prove to be counterproductive.

The Costs of Cyber Insecurity

The Internet and other digital information systems are critical to Canada's economy. According to Statistics Canada's 2012 *Canadian Internet Use Survey*, 83 per cent of Canadian households have access to the Internet.[25] This high rate of Internet use means that Canadians rely on the Internet to carry out daily activities such as dealing with their finances and filing taxes, going shopping, and communicating with one another.

According to the Canadian Bankers Association, 68 per cent of Canadian use online and mobile banking.[26] During the 2014 tax season, Canadian taxpayers filed 78 per cent of tax returns electronically with the Canadian Revenue Agency.[27] A 2014 market study conducted by market research firm Forrester Research forecasts that by 2019, e-commerce will represent 9.5 per cent of retail transactions in Canada.[28] And according to Sherpa Marketing, 64 per cent of Canadians are active on social media; with 50 per cent of Canadians regularly using more than one social media platform.[29] Canadians depend on the Internet in living their day-to-day lives.

The Internet is seen by many commentators as a key technology to drive global economic growth over the coming decades. The McKinsey Global Institute estimates that the Internet

[25] Statistics Canada, "Canadian Internet Use Survey, 2012" last modified November 26, 2013, http://www.statcan.gc.ca/daily-quotidien/131126/dq131126d-eng.htm.
[26] Canadian Bankers Association, "How Canadians Bank," February, 2017, https://www.cba.ca/Assets/CBA/Files/Article%20Category/PDF/bkg_technology_en.pdf.
[27] "Tax time 2015: How to file your tax return online," *CBC News*, March 2, 2015, http://www.cbc.ca/news/business/taxes/tax-time-2015-how-to-file-your-tax-return-online-1.2960477.
[28] Forrester Research, "Canadian Online Retail Forecast, 2014 to 2019," October 14, 2014, https://www.forrester.com/report/Canadian+Online+Retail+Forecast+2014+To+2019/-/E-RES115497.
[29] Stewart Moffatt, "Canadian Social Media Statistics," July 1, 2014, Sherpa Marketing, https://www.sherpamarketing.ca/blogs/canadian-social-media-statistics-.

can be attributed to 21 per cent of GDP growth in post-industrial economies.[30] Globally, USD $8 trillion is exchanged each year over Internet-based e-commerce platforms.[31]

However, despite this great economic potential, the Internet is a digital Wild West in some respects. A 2014 Center for Strategic and International Studies report commissioned by cybersecurity firm McAfee estimates that cybercrime creates an annual global economic loss of between USD $375 billion and $575 billion.[32] The World Economic Forum's *Global Risks Report 2016* found that cyberattacks were the top perceived risk in North America.[33]

In Canada, a 2016 crime survey by consulting firm PricewaterhouseCoopers found that 28 per cent of Canadian businesses reported being victims of cyber-crimes in the past 24 months.[34] And a 2016 Ponemon Institute study found that data breaches cost Canadian companies USD $4.98 million/per incident on average.[35] In total, 0.17 per cent of Canadian GDP is estimated to be lost to cybercrime on an annual basis.[36] This compares to an estimated 5 per cent loss in Canadian GDP to all types of crime combined.[37] A 2014 report issued by the Royal Canadian Mounted Police warns that developments in technology and increased criminal cyber know-how means that opportunity for "Cybercrime is expanding."[38]

According to an investigation by the *Globe and Mail*, during a single high-profile cyberattack against the National Research Council in 2014 by Chinese hackers, "hundreds of millions" of

---

[30] James Manyika and Charles Roxburgh, *The Great Transformer: The Impact of the Internet on Economic Growth and Prosperity* (McKinsey Global Institute, October 2011), http://www.mckinsey.com/industries/high-tech/our-insights/the-great-transformer.
[31] Manyika and Roxburgh, *The Great Transformer*.
[32] Center for Strategic and International Studies, *Net Losses: Estimating the Global Cost of Cybercrime* (McAfee, June 2014), http://www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf.
[33] World Economic Forum, *The Global Risks Report 2016*, 11th ed. (World Economic Forum, 2016), http://www3.weforum.org/docs/Media/TheGlobalRisksReport2016.pdf.
[34] PricewaterhouseCoopers, "Global Economic Crime Survey 2016: Canadian Insights," 2016, https://www.pwc.com/ca/en/services/deals/publications/economic-crime-survey.html.
[35] Ponemon Institute, "Cost of Data Breach Study: Global Analysis, 2016," https://www-03.ibm.com/security/data-breach/.
[36] Center for Strategic and International Studies, *Net Losses.*
[37] Stephen Easton, Hilary Furness, and Paul Brantingham, *The Cost of Crime in Canada* (Fraser Institute, October 2014), https://www.fraserinstitute.org/sites/default/files/cost-of-crime-in-canada.pdf.
[38] Royal Canadian Mounted Police, "Cybercrime: An Overview of Incidents and Issues in Canada," last modified December 16, 2014, http://www.rcmp.gc.ca/en/cybercrime-an-overview-incidents-and-issues-canada.

dollars in critical research data were lost.[39] Such loss of critical research and development data constitute a threat to Canada's economic competitiveness in an increasingly fierce global economy. Over time, economic losses from such hacking can chip away at Canada's national power.

While these economic figures are shocking, in truth, we do not have a clear understanding of the overall level and economic effects of cyberattacks and cybercrime. This lack of clarity is due to reporting bias and data verification issues in cybercrime statistics.[40] Obtaining clearer data on losses from cybersecurity incidents is one of the key issues that must be addressed to create better public policy related to cybersecurity.

Furthermore, it is not just commerce that is vulnerable to cyberattacks. Recently, there have been allegations of Russian cyberattacks and information warfare operations during 2016 United States presidential elections.[41] These attacks may have influenced the results of the election, and as a result, the election's outcome is currently mired in controversy. Confidence in the American democratic process has been undermined.[42] Such attacks on democratic institutions illustrate modern states' complex cyber vulnerabilities.[43] The use of cyberattacks in support of information warfare activities is a particularly insidious threat to democratic countries such as Canada. Attacks on electoral institutions demonstrate how vulnerabilities in computer networks can be indirectly linked to larger strategic vulnerabilities for states.

---

[39] Colin Freeze, "China Hack Cost Ottawa 'Hundreds of Millions,' Documents Show," *Globe and Mail*, March 30, 2017, https://beta.theglobeandmail.com/news/national/federal-documents-say-2014-china-hack-cost-hundreds-of-millions-of-dollars/article34485219/?ref=http://www.theglobeandmail.com&.

[40] Dinei Florencio and Cormac Herley, "Sex, Lies and Cyber-crime Surveys," *10th Workshop on the Economics of Information Security*, Fairfax, VA, United States, June 1, 2011, available at: https://www.microsoft.com/en-us/research/publication/sex-lies-and-cyber-crime-surveys/.

[41] Zack Beauchamp, "The Key Findings from the US Intelligence Report on the Russia Hack, Decoded," *Vox*, January, 6, 2017, http://www.vox.com/world/2017/1/6/14194986/russia-hack-intelligence-report-election-trump.

[42] Eric Lipton, David E. Sanger, and Scott Shane, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.," *New York Times*, December 13, 2016, https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0.

[43] A study of how liberal democracies, such as the United States, are vulnerable to new methods of cyber- and information warfare is provided by Bill Gertz, *iWar: War and Peace in the Information Age* (New York: Threshold Editions, 2017).

PART III – MAPPING RECENT CANADIAN CYBERSECURITY POLICY

Recent cybersecurity policy in Canada has been produced through a series of government strategy documents and public consultations over the past ten years. Today, the resulting policy created through this process are in-flux, as they have been developed by successive Conservative and Liberal governments in fits and starts. As a result, rather than being a statement of political vision, Canada's cybersecurity policy development can readily be characterized as incrementalist in nature.

While the various government documents that have been tabled over the past decade do try to reference one another, they all have a standalone feel; with departments such as Public Safety Canada, Industry Canada, or the Department of National Defence producing their own content. The incremental development of Canadian cybersecurity policy is a classic case of "muddling through" policy development.[44]

Canada's Cybersecurity Strategy

The origins of recent Canadian cybersecurity policy can be found in the federal government's 2010 cybersecurity strategy document and implementation plan,[45] and a 2013 cyber incident management framework.[46] While this collection of strategy documents represent a first-try by the Canadian government in managing the modern challenges of cybersecurity in today's digital economy, these papers are now outdated, and express a degree of naivety about the kinds of threats Canada faces in cyberspace. Most critically, the documents fail to link cyber-capabilities to Canada's national power.

This first generation of strategy documents have a passive tone to them, and they do not give the kind of agency Canada requires to respond effectively to cyber-threats. Furthermore, the above-mentioned strategy documents are geared more towards dealing with low-level cybercrime and not state-on-state attacks (carried out by APTs). Finally, the documents tend

---

[44] Charles E. Lindblom, "The Science of 'Muddling Through,'" *Public Administration Review* 19, no. 2 (Spring 1959): 79-88; Charles E. Lindblom, "Still Muddling, Not Yet Through," *Public Administration Review* 39, no. 6 (November/December 1979): 517-526.

[45] Government of Canada, *Canada's Cyber Security Strategy* (Ottawa: Public Safety Canada, 2010), https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-en.aspx.

[46] Government of Canada, *Cyber Incident Management Framework for Canada* (Ottawa: Public Safety Canada, 2013), https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-ncdnt-frmwrk/index-en.aspx.

to frame cybersecurity as something that is done in reaction to events; government cybersecurity policy is framed as a way to respond to cyber-incidents. The strategy documents fail to discuss issues such as building resiliency in Canadian cyber-systems and monitoring rival computer networks for threat intelligence. Furthermore, these early cybersecurity strategy documents failed to recognize that cybersecurity also requires robust and demonstrated offensive capabilities.[47]

The federal government followed these strategy documents in 2014 with a critical infrastructure protection plan.[48] The infrastructure protection plan called for the government to work in cooperation with the private sector to protect Canadian critical infrastructure, yet it was vague on the types of actors who pose a danger to Canada's vital infrastructure. And aside from coordinating with various government departments and infrastructure operators, the plan was ambiguous on what the federal government could do to protect Canadians.[49]

One important initiative that has come out of Canada's muddled cybersecurity strategy is a Canadian Cyber Incident Response Centre (CIRC) operated under Public Safety Canada.[50] The mandate of the centre is to act as a clearing house of cyber-incident intelligence, and to partner with the private sector, as well as with municipal, territorial, and provincial levels of government to increase Canada's overall vigilance and resilience to major cyberattacks. Despite capacity issues in recent years that did not allow the CIRC to operate on a 24/7 continuous basis,[51] the development of such a unit within the federal government is a positive step in helping to secure Canadian cyberspace.

---

[47] Jeffrey Carr, *Inside Cyber Warfare* (Sebastopol: O'Reilly Media, 2012): 244-245.
[48] Government of Canada, *Action Plan for Critical Infrastructure: 2014-2017* (Ottawa: Public Safety Canada, 2014), https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pln-crtcl-nfrstrctr-2014-17/index-en.aspx.
[49] This coordination with government and industry in reaction to cybersecurity incidents is vital according to consultations held across Canada by the Public Policy Forum; see Public Policy Forum, *Securing Canada's Cyberspace* (Public Policy Forum, February 2017), http://www.ppforum.ca/publications/securing-canada%E2%80%99s-cyberspace.
[50] Public Safety Canada, "Canadian Cyber Incident Response Centre (CCIRC)," last modified April 4, 2016, https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-en.aspx.
[51] Office of the Auditor General of Canada, *2012 Fall Report of the Auditor General of Canada* (Ottawa: Government of Canada, 2012), Chapter 3, http://www.oag-bvg.gc.ca/internet/English/parl_oag_201210_e_37321.html.

Digital Canada 150

The federal government's 2014 *Digital Canada 150* strategy document, while mainly focused on digital cultural content, does include a section on cybersecurity.[52] The document advocated measures for "keeping with Canada's place in the world as a leading cybernation" by "protecting Canadians from online threats and the misuse of digital technology."[53] However, the phrasing contained within Digital Canada 150 on cybersecurity is more focused on cybercrime and issues such as cyber-bullying. While these are both worthy issues for government concern, Canada must also apply a national security lens to cybersecurity.

Canada, as a country with an advanced post-industrial economy, relies on networked information systems and the Internet to function. Threats towards Canada's digital economy, critical infrastructure, and information networks have national security implications. Due to the economic risks associated with cyber insecurity, Digital Canada 150 was a missed opportunity for Canada to proclaim the importance of cybersecurity as a core component of its national interest.

The 2017 Public Consultation of Cybersecurity

The federal government held public consultations on cybersecurity over the summer and fall of 2016,[54] and released a summary report on the consultations in January 2017.[55] Both the consultation document and the final report noted the challenge of protecting Canada's information systems and critical infrastructure from, what is phrased as, "Advanced Cyber Threats." Disappointingly, the final report did not include specific language on developing offensive cyber capabilities. Furthermore, cybersecurity was framed as a public safety issue rather than a geostrategic or national security issue.

---

[52] Government of Canada, *Digital Canada 150* (Ottawa: Industry Canada, 2014), http://www.ic.gc.ca/eic/site/028.nsf/eng/home.
[53] Ibid.
[54] Government of Canada, *Security and Prosperity in the Digital Age: Consulting on Canada's Approach to Cyber Security*, (Ottawa: Public Safety Canada, 2016), https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-scrty-prsprty/index-en.aspx.
[55] Nielsen, *Cyber Review Consultations Report* (Ottawa: Public Safety Canada, 2017), https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2017-cybr-rvw-cnslttns-rprt/2017-cybr-rvw-cnslttns-rprt-en.pdf.

Strategic Forecasting by Policy Horizons Canada

To complement recent government thinking on cybersecurity issues, Policy Horizons Canada—the federal government's a strategic foresight unit—listed cybersecurity as a critical emerging security challenge for Canada. In Policy Horizons' *Canada 2030* report on critical infrastructure, cybersecurity is identified as a "key infrastructure challenge" with "cross-cutting implications" for SMART infrastructure in the areas of public safety and national security, privacy, and economic development.[56] According to this forecast document, it is essential to secure Canada's cyber-assets to secure the country's future critical infrastructure. Securing and exploiting cyberspace is essential to Canada's economic future.

Coverage of Cybersecurity Issues in Canadian Politics

Cybersecurity issues played a noted but minor role in the 2015 federal election. While commentators have called for a more robust public debate on cyber-issues,[57] the cybersecurity has, so far, been one of relative unimportance in Canadian political debates. During the 2015 general election, all three mainstream federal parties included short commitments on cybersecurity as part of their campaign platforms.[58] The Liberal Party included a call for the federal government to conduct a policy review of Canada's current critical infrastructure and cybersecurity plan in its 2015 election campaign platform.[59]

Coverage of Cybersecurity Issues in Parliament

On March 7, 2016, the Senate Committee on National Security and Defence held a session in which the cybersecurity vulnerabilities of the federal government were discussed.[60] While the meeting produced no conclusive analysis on Canada's cybersecurity vulnerabilities, the

---

[56] Government of Canada, *Canada 2030: Scan of Emerging Issues* (Ottawa: Policy Horizons Canada, 2017): 4, http://www.horizons.gc.ca/eng/content/canada-2030-scan-emerging-issues-infrastructure.
[57] Amanda Connolly, "Experts say Munk Debate needs to include cybersecurity," *iPolitics*, September 23, 2015, http://ipolitics.ca/2015/09/23/experts-say-munk-debate-needs-to-include-cybersecurity/.
[58] Matthew Braga, "Where Canada's Three Political Parties Stand on Cybersecurity and Surveillance," *Vice Motherboard*, October 9, 2015, https://motherboard.vice.com/en_us/article/where-canadas-three-political-parties-stand-on-cybersecurity-and-surveillance.
[59] Liberal Party of Canada, *Real Change: A New Plan for a Strong Middle Class* (Liberal Party of Canada, 2015): 71, https://www.liberal.ca/wp-content/uploads/2015/10/New-plan-for-a-strong-middle-class.pdf.
[60] Senate of Canada, "Proceedings of the Standing Senate Committee on National Security and Defence," Issue 2, March 7, 2016, https://sencanada.ca/en/Content/Sen/Committee/421/SECD/02ev-52409-e.

testimony by senior bureaucrats from Public Safety Canada did inform Parliament of the serious nature of cybersecurity issues. These hearings were followed up on October 19, 2016 when the Liberal Senate Forum held additional public hearings on the state of cybersecurity in Canada.[61] During the hearings, expert witnesses testified on Canada's vulnerabilities to hacking and cyberattacks.

The issue of cybersecurity was briefly brought up again during Senate debates held on November 2, 2016, when Senator Art Eggleton inquired on the Liberal government's progress on updating Canada's 2010 cybersecurity strategy. In response to Eggelton's inquiry, Senator Peter Harder, the Leader of the Government in the Senate, stated that a new government cybersecurity strategy would be forthcoming after the conclusion of a series of public consultations.[62]

Bill C-59 and Canadian Cyberwarfare Capabilities

Bill C-59, the Liberal government's omnibus security and intelligence reform bill, is expected to better define the contours in which Canadian security and intelligence services can operate, and defend Canada in cyberspace. The bill has wide-ranging implications for the rollout of Canadian cybersecurity policy and the parameters governing the use of a Canadian cyberwarfare capability.[63] The bill is also intended to give the Communications and Security Establishment (CSE) a legislated mandate to pursue CNO in support of Canadian security interests.[64] At the time of this paper's writing, the bill is in second reading.[65]

---

[61] "The State of Cyber Security in Canada," Liberal Senate Forum, October 19, 2016, http://liberalsenateforum.ca/open-caucus/october-19-2016-state-cyber-security-canada/.
[62] Senate of Canada, *Debates of the Senate* 150, no. 69, November 2, 2016, https://sencanada.ca/Content/SEN/Chamber/421/Debates/pdf/069db_2016-11-02-e.pdf.
[63] David Mussington, "Bill C-59 – The Canadian National Security Act 2017: What You Need to Know," Centre for International Governance Innovation, July 2, 2017, https://www.cigionline.org/articles/bill-c-59-canadian-national-security-act-2017-what-you-need-know.
[64] Craig Forcese and Kent Roach, "The Roses and the Thorns of Canada's New National Security Bill," *Maclean's*, June 20, 2017, http://www.macleans.ca/politics/ottawa/the-roses-and-thorns-of-canadas-new-national-security-bill/.
[65] "Bill C-59: An Act Respecting National Security Matters," Open Parliament, June 20, 2017, https://openparliament.ca/bills/42-1/C-59/.

Two Recent Canadian Senate Reports

A two-part report published in spring 2017 by the Canadian Senate's Standing Senate Committee on National Security and Defence called for more attention to be paid by the Canadian government to cybersecurity issues, and framed cybersecurity as a national security issue. The Senate report recommended that Canada work with the United States on joint cyber-defence initiatives, including updating the North American Aerospace Defense Command (NORAD) Agreement to include a North American cyber-defence mission.[66] The Canadian Senate is the only parliamentary body that has consistently paid heed to Canada's cybersecurity vulnerabilities and provoked public discussion on the framing of cybersecurity as a national defence issue. As a place to debate and study issues of national importance, the Senate is serving Canadians well in the realm of cybersecurity policy.

Documented Cyberattacks on Federal Government IT Infrastructure

Federal government information technology (IT) systems are under daily cyberattack by a variety of actors.[67] A 2017 report prepared for Public Safety Canada by PricewaterhouseCoopers found that government systems are highly vulnerable to cyberattacks.[68] There has been a number of high-profile cyberattacks on Government of Canada IT infrastructure reported by the Canadian press in the past decade.

These high-profile cyberattacks have included the following:

- *January 2011*—hackers attack the Treasury Board of Canada, Department of Finance Canada, and Defence Research and Development Canada networks through spear-

[66] Senate of Canada, *Military Underfunded: The Walk Must Match the Talk*, report of the Standing Senate Committee on National Security and Defence, eds. Daniel Lang and Mobina S.B. Jaffer (Ottawa: Senate of Canada April 2017), https://sencanada.ca/content/sen/committee/421/SECD/Reports/DEFENCE_DPR_FINAL_e.pdf; Senate of Canada, *Reinvesting in the Canadian Armed Forces: A Plan for the Future*, report of the Standing Senate Committee on National Security and Defence, eds. Daniel Lang and Mobina S.B. Jaffer (Ottawa: Senate of Canada, May 2017), https://sencanada.ca/en/committees/secd.

[67] Stewart Bell, "Federal Government Facing 'Serious' Cyber Attacks from State-Sponsored Hackers and Terrorist Groups: CSIS," *National Post*, February 28, 2017, http://news.nationalpost.com/news/canada/federal-government-facing-serious-cyber-attacks-from-state-sponsored-hackers-and-terrorist-groups-csis.

[68] Nestor Arellano, "Government Computer Networks can't Standup to Cyberattacks: Report," *Vanguard*, January 12, 2017, http://www.vanguardcanada.com/2017/01/12/government-computer-networks-cant-standup-to-cyberattacks-report/.

phishing attacks on government email services. The attacks are believed to have originated in China.[69]

- *April 2014*—the Heartbleed virus attacks Canada Revenue Agency servers and forces the agency to take its online tax filing services off-line.[70]
- *July 2014*—hackers, believed to be based in mainland China, infiltrate the National Research Council's networks.[71]
- *Summer 2015*—the Canadian Security and Intelligence Service (CISIS) website is attacked by an organization known as Aerith.[72]
- *June 2015*—the Government of Canada website is subjected to DDoS attack by a hacktivist group known as Anonymous in protest of the federal government's Bill C-51 anti-terrorism legislation.[73]
- *Summer/Fall 2016*—hackers target a number of Government of Canada websites related to the environment, energy, and natural resources in a series of attacks.[74]
- *March 2017*—Statistics Canada's website is hacked and then taken offline after officials identify security vulnerabilities in the websites for both Statistics Canada and the Canada Revenue Agency.[75]
- *June 2017*—Canadian Parliament information technology decide to staff shut down Parliament's email and network services as a preventative measure in the face of the

[69] Greg Weston, "Foreign Hackers Attack Canadian government," *CBC News*, February 16, 2011, http://www.cbc.ca/news/politics/foreign-hackers-attack-canadian-government-1.982618.
[70] "Heartbleed Bug May Shut Revenue Canada Website until Weekend," *CBC News*, April 9, 2014, http://www.cbc.ca/news/business/heartbleed-bug-may-shut-revenue-canada-website-until-weekend-1.2603742.
[71] Rosemary Barton, "Chinese Cyberattack Hits Canada's National Research Council," *CBC News*, July 29, 2017, http://www.cbc.ca/news/politics/chinese-cyberattack-hits-canada-s-national-research-council-1.2721241.
[72] Wesley Wark, "The Summer of Cyber Attacks," *Ottawa Sun*, July 3, 2015, http://www.ottawasun.com/2015/07/03/the-summer-of-cyber-attacks.
[73] Jason Fekete and Ian Macleod, "Hacker Group 'Anonymous' Claims Credit for Federal Cyber Attacks," *Ottawa Citizen*, June 17, 2015, http://ottawacitizen.com/news/politics/federal-computer-servers-cyber-attacked-clement; Wark, "The summer of cyber attacks."
[74] Colin Freeze, "Hackers Target Canadian Government's Energy and Resource Departments," *Globe and Mail*, November 17, 2016, http://www.theglobeandmail.com/news/politics/hackers-target-governments-energy-and-resource-departments/article32890960/.
[75] Alex Ballingall, "StatsCan Hacked after Government Sites Made Vulnerable: Officials," *Toronto Star*, March 13, 2017, https://www.thestar.com/news/canada/2017/03/13/statscan-hacked-after-government-sites-made-vulnerable-officials.html.

threat that hackers were attempting to gain unauthorized access to Parliament's IT systems.[76]

These high-profile attacks that become stories in the news are just a small sample of the millions of low-level attacks and dozens of major cybersecurity incidents a Canadian government department will deal with in any given year. For example, an investigation by the *Financial Post* found that the Bank of Canada is bombarded with over 15 million potential attacks every month, and is subjected to dozens of major cyber incidents annually.[77]

Communications Security Establishment Canadian Elections Cybersecurity Study

In 2017 the Liberal government tasked the CSE to conduct a "risk assessment" of Canadian elections to foreign information operations and hacking.[78] This tasking came in the wake of fears of hacking and manipulation of the United States presidential election in November 2016, and the French presidential election in May 2017.[79] CSE's report on the matter found that "cyber threat activity" targeting elections had increased globally in recent years.

Furthermore, CSE reported that Canadian elections in 2015 had been targeted in low-level cyberattacks. CSE asserted that Canadian democratic institutions were vulnerable to cyberattacks, and that such attacks could be expected to take place during the upcoming federal election in 2019.[80] CSE's study underscores the ways in which state institutions can be undermined by cyberattacks.

---

[76] Althia Raj, "Canadian Parliament Shuts Down Emails over Fears Of Hacking," *Huffington Post*, June 25, 2017, http://www.huffingtonpost.ca/2017/06/25/canadian-government-emails-shut-down-over-fears-of-hacking_a_23000911/.

[77] Claire Brownell, "Hackers are Bombarding the Bank of Canada with Cyber Attacks and the Crack in the Bank's Armour is its Employees," *Financial Post*, January 26, 2017, http://business.financialpost.com/technology/hackers-bombard-the-bank-of-canada-with-cyberattacks.

[78] Alex Boutilier, "Canada's Spies Examining 'Vulnerabilities' in Election System," *Toronto Star*, May 12, 2017, https://www.thestar.com/news/canada/2017/05/12/canadas-spies-examining-vulnerabilities-in-election-system.html.

[79] Andy Greenberg, "The NSA Confirms It: Russia Hacked French Election 'Infrastructure'," *Wired*, May 9, 2017, https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/; Eric Lipton, David E. Sanger, Scott Shane, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.," *New York Times*, December 13, 2016, https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0.

[80] Government of Canada, *Cyber Threats to Canada's Democratic Process* (Ottawa: Communications and Security Establishment, 2017), https://www.cse-cst.gc.ca/sites/default/files/cse-cyber-threat-assessment-e.pdf.

Communication and Security Establishment Cyber Capabilities?

While at an official level the Canadian government has deferred on discussing offensive responses to cybersecurity incidents, there is evidence in the form of leaked documents that government organizations such as the CSE may have CNE and CNA capabilities.[81]

These capabilities are said to include the ability to infiltrate and map target computer networks; download, modify, or delete a target's data; block a target's network/Internet connections; as well as the ability to directly attack against an opponent's networked critical infrastructure.[82] However, as these are leaked documents, it is difficult to paint a full picture on how advanced Canada's existing cyber capabilities actually are, and how and if these capabilities have been used.

Canada's Participation in the Budapest Convention

The *Budapest Convention on Cybercrime* is a global treaty intended to combat criminal activity in cyberspace. The Budapest Convention seeks to harmonize signatory countries' national cybercrime laws, and to coordinate cybercrime investigations across international borders.[83] The treaty is intended to help law enforcement and national security agencies of signatory states effectively prosecute criminal activity taking place transnationally over computer networks, including the Internet. The treaty covers issues around copyright infringement, computer fraud, distribution of child pornography, and network security violations.

Canada signed the convention in 2001, but the treaty was only ratified and brought into force under Canadian law in 2015.[84] While the treaty is the most comprehensive international framework agreement related to cybercrime and modern cybersecurity concerns, it is

---

[81] Amber Hildebrandt, Dave Seglins, and Michael Pereira, "Communication Security Establishment's Cyberwarfare Toolbox Revealed," *CBC News*, March 23, 2015, http://www.cbc.ca/news/canada/communication-security-establishment-s-cyberwarfare-toolbox-revealed-1.3002978.

[82] Hildebrandt, Seglins, and Pereira, "Communication Security Establishment's Cyberwarfare Toolbox Revealed."

[83] Council of Europe, *Explanatory Report to the Convention on Cybercrime* (Budapest: European Treaty Series, 2001), https://rm.coe.int/16800cce5b.

[84] Council of Europe, Chart of Signatures and Ratifications of Treaty 185: Convention on Cybercrime, last modified March 9, 2017, http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=tcrnNcYJ.

limited in its power as key international actors such as Russia have not signed the convention and have been openly hostile to the treaty's provisions. Furthermore, the treaty is proving to have a limited real-world effect on curbing cybercrime as pursuing transnational cybercriminal investigations and extraditions remains a complex activity. There are also concerns with how the Budapest Convention interfaces with domestic laws and free speech guarantees.

Since 2006, the Budapest Convention has included the *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*. The Additional Protocol seeks to criminalize the dissemination of hate speech, and racist or xenophobic materials distributed via computer networks, including the Internet.[85] Canada became a signatory to the Additional Protocol in 2005, but has yet to ratify it and bring it into force under Canadian law.[86]

The 2017 Canadian Defence Policy Review

In June 2017, the Trudeau government released Canada's 2017 defence policy review. This long-awaited white paper supplanted the *Canada First Defence Policy* released by the Harper government in 2008. The new white paper titled *Strong, Secure, Engaged: Canada's Defence Policy* included a number of new developments in the realm of Canadian cybersecurity and the Canadian Armed Forces' approach to cyberwarfare. Most critically, for the first time, the Government of Canada publicly tasked the military with "conducting active cyber operations" in defence of Canada.[87]

The white paper has called for the Canadian military to acquire "cyber security situational awareness projects, cyber threat identification and response," as well as develop "military-

[85] Council of Europe, *Additional Protocol to the Convention on Cybercrime Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems* (Strasbourg: European Treaty Series, 2003), https://rm.coe.int/168008160f.
[86] Council of Europe, Chart of Signatures and Ratifications of Treaty 189: Additional Protocol to the Convention on Cybercrime Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems, last modified March 9, 2017, http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p_auth=LGcvu24X.
[87] Department of National Defence (Canada), *Strong, Secure, Engaged: Canada's Defence Policy*, (Ottawa: Her Majesty the Queen in Right of Canada, 2017): 14, http://dgpaapp.forces.gc.ca/en/canada-defence-policy/index.asp.

specific information operations and offensive cyber operations capabilities able to target, exploit, influence, and attack in support of military operations."[88]

Importantly, the new Canadian defence policy recognizes that some of the most sophisticated cyber threats come from state actors. These APTs threaten Canadian government and military IT systems, as well as private sector assets.[89] The new policy, as advocated in the white paper, understands how technically difficult it can be to positively attribute individual actors to specific network attacks, and the issues around legal interjurisdictionally when attempting to stop such hacks. The white paper also ties cybersecurity in with Canadian space security, citing a cyberattack as a possible means for a sophisticated actor to disrupt, or even destroy, Canadian space assets.[90]

As part of the new defence policy, the Canadian Armed Forces now recognizes cyberspace as a separate domain of warfare. The policy also calls for Canadian cyber capabilities to be used actively in both defensive and offensive roles. Such operations will require the establishment of a Cyber Mission Assurance Program and the creation of a new Cyber Operator military occupation within the Canadian Armed Forces.[91]

Finally, the white paper recognizes the threat of cyberattacks on Canadian interests, and how important cyber operations have become in "hybrid warfare" operations by rival states and violent non-state actors.[92] The white paper characterizes this new emergent form of warfare as taking place in a "grey zone" between war and peace, and as a dangerous development in the global security environment.[93] Of particular concern for the Canadian government is hybrid warfare's tendency to create mistrust and misunderstanding amongst rival states.[94]

In international security affairs, misunderstandings can quickly lead to miscalculations and exacerbated tensions between rivals. Political scientist Ben Buchanan theorizes that the global increase in cyber-operations will push the international system towards further

[88] Department of National Defence (Canada*), Strong, Secure, Engaged*: 41.
[89] Ibid., 56.
[90] Ibid., 71.
[91] Ibid., 73.
[92] Ibid., 53.
[93] Ibid.
[94] Ibid.

instability as states become enmeshed in security dilemmas originating from their aggressive activities in cyberspace.[95]

Operation REASSURANCE

The Canadian Armed Forces are currently facing cyber-threats in its current theaters of operation. According to the *National Post*, the 450 troops currently being deployed to Latvia under Operation REASSURANCE will be accompanied by "cyber warriors" to provide force protection from Russian cyberwarfare capabilities and information warfare operations.[96,97] While the deployment of this relatively new capability is sure to be of use to field commanders, it is still defensive in nature and is being implemented in reaction to local theater-level threats. The use of this novel cyber warrior asset may take on a more offensive orientation over time as the Canadian Armed Forces implement the new 2017 defence strategy.

Canadian Armed Forces Cyber Capabilities

Despite recent developments with the 2017 defence strategy, Canada's military does not currently have any known offensive cyberwarfare capabilities. However, the Canadian Armed Forces is beginning to explore the use of cyberweapons and developing a corps of cyberwarfare operations personnel to support these operations, as called for in the 2017 defence white paper.[98] These discussions on Canada's future approach to cyberwarfare are taking place at the highest levels of the defence community.[99]

The Department of National Defence's *Centre for Operational Research and Analysis* is supporting this evolution of cyberwarfare capabilities by providing analytical support in the area of doctrine development and linking cyber to other Canadian Armed Forces

---

[95] Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations* (New York: Oxford University Press, 2017).
[96] Matthew Fisher, "Canada's Forces Deployed in Latvia to Include 'Cyber Warriors' to Counter Russians," *National Post*, March 9, 2017, http://news.nationalpost.com/news/world/matthew-fisher-canadas-forces-deployed-in-latvia-to-include-cyber-warriors-to-counter-russian-attacks.
[97] Department of National Defense (Canada), Operation REASSURANCE, last modified May 9, 2017, http://www.forces.gc.ca/en/operations-abroad/nato-ee.page.
[98] Alex Boutilier, "Canada Developing Arsenal of Cyber-Weapons," *Toronto Star*, March 16, 2017, https://www.thestar.com/news/canada/2017/03/16/canada-developing-arsenal-of-cyber-weapons.html.
[99] Justin Ling, "Cyber war," *Vice News Canada*, January 18, 2017, https://news.vice.com/story/canada-is-deciding-whether-it-wants-to-get-into-the-business-of-cyberwar.

capabilities.[100] This emphasis on the development of doctrine and the linking of cyber-capabilities to other Canadian military assets is critical to ensuring that Canada develops a robust cyberwarfare program.[101]

In a recent *CBC News* interview, Richard Fadden, a national security advisor under Prime Ministers Stephen Harper and Justin Trudeau, and former director of the Canadian Security Intelligence Service (CSIS), has argued that the Canadian Armed Forces must have the ability to conduct both defensive and offensive cyber-operations during deployments.[102]

There is also publically available evidence to suggest that the Canadian Security Establishment has played active roles in both Afghanistan and Northern Iraq in supporting the Canadian Armed Forces with CNE missions.[103]

Department of National Defence Cyber Procurement Activities

The Department of National Defence is currently working with Canadian industry to develop tactical-level cyber-operations capabilities. Through Public Works and Government Services Canada, Canada's military is currently soliciting a call for letters of interest (LOI) in the development of a digital platform for the *Tactical Edge Cyber Command and Control (TEC3) Program*.[104] While specifics on the Canadian Tactical Edge Program are not well-defined at this point in time, a similar pilot program is currently being implemented by the United States Army with the goal of collecting tactical intelligence on computer networks and electromagnetic spectra; and even giving local commanders low-level CNA capabilities.[105]

---

[100] For example, see Melanie Bernier and Joanne Treurniet, *CF Cyber Operations in the Future Cyber Environment Concept* (Ottawa: Defence R&D Canada, December 2009), http://cradpdf.drdc-rddc.gc.ca/PDFS/unc92/p532776.pdf.

[101] For an in-depth discussion on the linking of cyber capabilities to national power, see David J. Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power* (London: The International Institute for Strategic Studies, 2011).

[102] Murray Brewster, "Former CSIS Head Says Canada Should Have its Own Cyber-Warriors," *CBC News*, June 22, 2016, http://www.cbc.ca/news/politics/military-cyber-wars-fadden-1.3648214.

[103] Murray Brewster, "Canada's Electronic Spy Service to Take More Prominent Role in ISIS Fight," *CBC News*, February 18, 2016, http://www.cbc.ca/m/touch/politics/story/1.3454617.

[104] Public Works and Government Services Canada, "Tactical Edge Cyber Command and Control," call for letters of interest, *Buyandsell.gc.ca*, last modified May 12, 2017, https://buyandsell.gc.ca/procurement-data/tender-notice/PW-15-00668957.

[105] Mark Pomerleau, "Army Takes Strategic Cyber Capabilities to the Tactical Edge," *C4ISRNET*, February 9, 2017, http://www.c4isrnet.com/articles/army-takes-strategic-cyber-capabilities-to-the-tactical-edge.

Public Works and Government Services Canada has also recently closed a call for industry input into a Department of National Defence *Defensive Cyber Operations Decision Support Project* (DCODSP). This project is intended to enhance the Canadian Armed Forces capacity to partake in CND operations, both domestically and in support of international deployments.[106] Like the TEC3 Program, a review of the DCODSP's tender document suggests that the Canadian military is unclear how to deal with cybersecurity issues, and needs industry input and analytical thinking on how derive the most benefit from its novel cyber-capabilities.

PART IV – TESTING THEORIES OF CYBERWARFARE

The previous sections of this paper have articulated the threat of cyberwarfare to Canada's interests, and have mapped the Canadian government's policy actions on cyber-issues to date. However, to rigorously understand why Canada requires a cyberwarfare capability, theories of cyberwarfare must be used to characterize and logically link Canada's national security interests with the development of an offensive cyberwarfare capability.

In international relations, capabilities can be thought of as assets that states use in their foreign relations to advance their national interests. In the international relations literature, capabilities are the expression of a state's power in the international arena in pursuit of its goals.[107] In the realm of cyberwarfare, a cyber capability provides a new means for states to pursue security and foreign policy goals in cyberspace.[108] A review of cybersecurity literature suggests that there are seven theories to explain why states would acquire cyberwarfare capabilities. By exploring these seven theories in detail, they can be tested to determine if they apply to Canada's specific security needs.

---

[106] Public Works and Government Services Canada, "Defensive Cyber Operations Project," call for letters of interest, *Buyandsell.gc.ca*, last modified January 26, 2017, https://buyandsell.gc.ca/procurement-data/tender-notice/PW-QE-049-26100.
[107] K.J. Holsti, "The Concept of Power in the Study of International Relations," *Background* 7, no. 4 (1964): 192.
[108] Franklin D. Kramer, et al., "Frameworks and Insights Characterizing Trends in Cyberspace and Cyberpower," *12th International Command and Control Research and Technology Symposium*, June 2007, Newport, Rhode Island, available at: https://www.semanticscholar.org/paper/Frameworks-and-Insights-Characterizing-Trends-in-C-Kramer-Starr/5eb231cdb687265a0099cf498165a17a66fd012f.

These seven theories are as follows:

- *Augment conventional military capabilities*—States develop cyberwarfare capabilities to augment their conventional forces during an armed conflict.[109] This augmentation could include using cyberweapons to attack a rival state's armed forces, or shut down strategic infrastructure such as the power grid during a time of war.
- *Cyber confidence game*—States develop cyberwarfare capabilities to dissuade rival states, who enjoy lesser technological prowess, from bothering to take the time and expense to develop high-technology capabilities.[110] This will degrade rivals' competitive military advantages over time and put their conventional forces at a qualitative disadvantage.
- *Cyber deterrence*—States develop cyberwarfare capabilities to deter rival states from attacking their computer networks for fear of a fierce and overwhelming counterattack.[111] This theory of cyberwarfare has its roots in nuclear deterrence theory developed during the Cold War.
- *Cyber espionage*—States develop cyberwarfare capabilities to break into their rivals' information systems to collect strategic and economic intelligence.[112]
- *Cyber sabotage*—States develop cyberwarfare capabilities to launch covert sabotage missions against a rival state's computer networks or critical infrastructure.[113]
- *Keep up with the Joneses*—States develop cyberwarfare capabilities to signal to their allies that they are useful, sophisticated, and dedicated security partners who are worth maintaining security partnerships and agreements with.[114]

---

[109] Russia augmented its conventional warfare capabilities with a series of DDoS attacks on Georgian government websites during its August 2008 invasion of Georgia; see John Markoff, "Before the Gunfire, Cyberattacks," *New York Times*, August 12, 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html.
[110] Martin C. Libicki, "Cyberwar as a Confidence Game," *Strategic Studies Quarterly* (Spring 2011): 132-146.
[111] David Elliott, "Deterring Strategic Cyberattack," *IEEE Security & Privacy*, September/October 2011: 36-40; Joseph S. Nye, "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly*, Winter 2011: 18-38.
[112] For a description of China's industrial espionage program, see David Talbot, "Cyber-Espionage Nightmare," *MIT Technology Review*, June 10, 2015, https://www.technologyreview.com/s/538201/cyber-espionage-nightmare/.
[113] Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown Publishers, 2014).
[114] Alexander Moens, Seychelle Cushing, and Alan W. Dowd, *Cybersecurity Challenges for Canada and the United States* (Vancouver: Fraser Institute, March 2015): 20-23, https://www.fraserinstitute.org/sites/default/files/cybersecurity-challenges-for-canada-and-the-united-states.pdf.

- *Tit-for-tat hacking*—Private sector organizations are constrained by law from taking offensive actions against hackers in most countries.[115] States develop cyberwarfare capabilities to launch small-scale retaliatory cyberattacks against identified hackers when government or corporate interests are attacked in cyberspace.

Augment Conventional Military Capabilities

The first theory of cyberwarfare that this paper will explore is that states will develop offensive cyberwarfare capabilities to augment their conventional military capabilities. By using cyberattacks, militaries can increase their operational effectiveness by targeting enemy forces or critical infrastructure. Such cyberwarfare capabilities could also be used by militaries to screen and defend their own forces in cyberspace by attacking an opponent's cyberwarfare forces. Under this theory, cyberspace becomes another domain for military action to take place in; just like land, sea, air, and space.

Force augmentation using cyberweapons has been effectively used by both Russia and Israel in the recent past. In the weeks prior to its August 2008 invasion of Georgia, Russia launched a series of DDoS attacks on Georgian government websites and the National Bank of Georgia's website.[116] These attacks can be interpreted as a part of the Russian's information warfare campaign in support of kinetic attacks on Georgian military forces. Likewise, during a September 2007 Israeli air attack on Syria's al-Kibar nuclear facility, the IDF used electronic warfare equipment to feed false data into Syrian anti-aircraft defenses, preventing them from tracking and firing on Israeli combat aircraft during the attack.[117]

The Canadian Armed Forces could greatly benefit from such capabilities during future operations. Equipping Canada's military to operate in cyberspace, alongside its air, land, sea, and space assets would provide commanders with additional options for planning missions. Under such a concept, dedicated cyber-operations personnel, or cyber-warriors, would

---

[115] Hannah Kuchler, "Cyber Insecurity: Hacking back," *Financial Times*, July 27, 2015, https://www.ft.com/content/c75a0196-2ed6-11e5-8873-775ba7c2ea3d.
[116] John Markoff, "Before the Gunfire, Cyberattacks"; "Marching Off to Cyberwar," *Economist*, December 4, 2008, http://www.economist.com/node/12673385.
[117] Sharon Weinberger, "How Israel Spoofed Syria's Air Defence System," *Wired*, October 4, 2007, https://www.wired.com/2007/10/how-israel-spoo/; David Makovsky, "The Silent Strike: How Israel Bombed a Syrian Nuclear Installation and Kept it a Secret," *The New Yorker*, September 17, 2012, http://www.newyorker.com/magazine/2012/09/17/the-silent-strike.

support a combat force during assigned missions. Such cyberwarfare units would be integrated into battle plans just like any other military asset.[118]

Under such a cyberwarfare concept, a Canadian cyberwarfare capability could complete the following three types of missions:[119]

- Physically destroy an opponent's computer network;
- Manipulate the data on an opponent's computer network;
- Negate an opponent's access to his own computer network.

For a modest investment in cyberwarfare capability, Canada's military would be equipped with a vital offensive asset to use during future missions. It would augment the Canadian Armed Forces' other assets, and allow Canada to work effectively with its allies. This augmentation theory is the strongest rationale for Canada to develop offensive cyberwarfare capabilities.

Cyber Confidence Game

Proposed by information warfare scholar Martin Libicki, the cyber confidence game argues that states will be dissuaded from pursuing advanced military technologies, such as digitally networked military hardware, for fear of leaving their militaries vulnerable to hacking by technologically sophisticated and powerful opponents.[120]

The premise of the cyber confidence game rests on the assumption that states who enjoy access to advanced technologies and the ability to digitally network their military hardware enjoy an immense advantage on the battlefield. Through digital networking, conventional military assets such as land forces, navies, and fighter and bomber aircraft can be linked in real-time with advanced information technology assets such as digital communications networks, computerized logistics systems, sensor equipment, and global navigation satellite systems.

---

[118] Melanie Bernier and Joanne Treurniet, "Understanding Cyber Operations in a Canadian Strategic Context: More than C4ISR, More than CNO," in *Conference on Cyber Conflict Proceedings 2010*, eds. C. Czosseck and K. Podins (Tallinn, Estonia: COE Publications, 2010): 227-243.
[119] Frances Allen, *CN(EH?): Should the CF Adopt Computer Network Exploitation and Attack Capabilities?* (Master's thesis, Canadian Forces College, 2002): 3, http://www.cfc.forces.gc.ca/259/181/74_allen.pdf.
[120] Libicki, "Cyberwar as a Confidence Game."

Often referred to in defence policy circles by names such as the Revolution in Military Affairs and Network-Centric Warfare,[121] this high-technology advantage has proven decisive on the battlefield in the recent past; and therefore, states would prefer to have a digital networking capability that would allow their militaries to remain competitive. State-on-state conflicts in the 1990s such as the Persian Gulf War (1990-91) and the Kosovo War (1998-99) demonstrate the immense qualitative advantage militaries enjoy by digitally networking their forces.

However, by digitally networking military hardware, states leave their armed forces vulnerable to an opponent's cyberattacks. It is feared that a rival state with advanced cyberwarfare capabilities could disrupt or disable military assets and negate any advantage created by digitally networking military hardware. In other words, the introduction of digital networking introduces a new vulnerability to the hardware and a new complication for military commanders to deal with.

States facing this dilemma may decide that they have the capacity to defend their networked forces in cyberspace. With this confidence, they can go ahead and digitally network their militaries and gain a critical advantage. However, states that are not confident in their ability to defend their networked forces in cyberspace may decide to forgo pursuing advanced military technologies, and put themselves at a military disadvantage.[122] This military disadvantage will manifest itself over time in a reduction in military capability; and ultimately, a relative decline in national power.

Libicki's confidence game is an interesting theory, which pushes forward the thinking on how cyberpower could be used in the future. However, it has no real relevance for a medium power such as Canada. This is because Canada's potential geopolitical rivals are made up of large and military-capable states. Canada lacks the capacity to generate the kind of force necessary to dissuade its rivals from developing high-technology capabilities for their armed forces.

[121] Elinor C. Sloan, *The Revolution in Military Affairs: Implications for Canada and NATO* (Montreal & Kingston: McGill-Queen's University Press, 2002): 3-17.
[122] Libicki, "Cyberwar as a Confidence Game."

Furthermore, the incentives for digitally networking military hardware are so compelling that risking cyber-vulnerabilities is probably a worthwhile trade-off for most states that can afford to upgrade. For this reason, the cyber confidence game theory does not present a compelling rationale for Canada to develop a cyberwarfare capability.

Cyber Deterrence

The idea behind deterrence theory is for a state to be well-armed enough, that if it were to be attacked by a rival state, it would be able to launch a fierce and overwhelming counterattack. This fear of a counterattack will deter and dissuade rival states from launching attacks. Deterrence was a major piece of Cold War-era strategic thinking, and was used by both the Soviet Union and the United States in an attempt to dissuade the other from attacking. This line of reasoning has been extended into the cybersecurity realm and is actively being debated by policy makers—particularly in the United States.[123]

Under deterrence theory, the fear of counter attack will dissuade states from attacking in the first place, and thus create a strategic stability where it is in nobody's interest to attack their rivals in a first strike and risk starting an escalating conflict. Thus stability can be maintained even if neither party trusts one another. On the face of it, cyber deterrence sounds like a good reason to develop cyber-weapons: "*I have this malicious computer code. I'm not interested in fighting, but if you attack my computer network, I will use it on you! Therefore, you better not attack and just leave me alone.*"

But there are major problems with cyber deterrence. First, under deterrence, you need to communicate your intentions to your rival and prove your credibility for him to believe you. Without communicating one's intentions to attack, and without demonstrating your ability to do so, you will not be perceived by an opponent as credible; and thus, no deterrent effect will be created.

However, in cyberwarfare scenarios, attacks must be planned well in advance. Computer code and methods of attack must be pre-developed for CNE and CNA operations, and

[123] P.W. Singer, "How the United States Can Win the Cyberwar of the Future," *Foreign Policy*, December 18, 2015, http://foreignpolicy.com/2015/12/18/how-the-united-states-can-win-the-cyberwar-of-the-future-deterrence-theory-security/.

customized for use against targeted information networks. This is particularly true if dealing with complex information systems or critical infrastructure that is protected by a rival state's CND capabilities. When dealing with well-defended government information systems, the cyberspace battlefield must be prepared in advance through meticulous computer network mapping and by identifying zero-day vulnerabilities to exploit on an opponent's information networks.

Because of this credibility issue with cyberweapons, it is difficult to make credible threats that are detailed enough to have a deterrent value. If a state communicates its capability to do a cyber-operation on a rival state's systems, it must be detailed enough to be considered credible. But if the threat is communicated in such detail, the rival state can simply add extra security protection to its systems and identify and fix its zero-day security vulnerabilities.

This may be one reason why states' CNE and CNA capabilities are currently such closely guarded secrets. In cyberwar, once a cyberattack capability is communicated, it may also be lost in short order. This dynamic of cyberweapons becoming ineffective as soon as an opponent becomes aware of their existence also creates a "use-if-or-lose-it" incentive structure that favours offensive action in cyber-operations.[124]

A second issue for a medium power such as Canada is that rivals that would threaten Canada with cyber-weapons are unlikely to be deterred by a meek Canadian counterattack. While the threat of such a Canadian cyber counter-attack would increase the costs for a rival to attack, Canada would not be able to generate the kind of fierce and overwhelming counterattack against a rival state that deterrence theory demands to work properly.

If such a threat were to escalate into a conflict in the physical domain, Canada would be truly outclassed in most situations due to its small military force, and its limited ability to project power and go on the offensive. Even in the physical realm, Canada would not be able to generate the kind of fierce and overwhelming counterattack that deterrence theory requires. In fact, it would be difficult for any state—even a great power such as the United States—to

[124] Wade L. Huntley, "Strategic Implications of Offense and Defense in Cyberwar," *49th Hawaii International Conference on System Sciences* (Koloa: IEEE, 2016): 5593.

generate the kind of force in cyberspace that would have a definite deterrent effect against a rival power.[125]

While deterrence theory served the United States and its NATO allies well during the Cold War, cyberwarfare should not be conflated with nuclear warfare.[126] Cyberweapons and nuclear weapons have different characteristics and are very different strategic assets. Nuclear weapons represent the ultimate weapon, while cyberweapons are at best a useful tools of espionage and sabotage and conventional force-enhancers.

But, while classical Cold War-era deterrence will not work in cyberspace, having a cyberwarfare capability could shape a rival state's strategic calculations and provide a marginal degree of security.[127] While not a totally useless concept in cyberwarfare, cyber deterrence theory does not present a good policy rationale for Canada to develop an offensive cyberwarfare capability.

Cyber Espionage and Cyber Sabotage

Cyber espionage and cyber sabotage are similar concepts and will be dealt with together in this paper. Cyber espionage is the exploitation of targeted computer networks for the purpose of collecting intelligence on a target's capabilities, plans, and intentions. Under the parlance of cybersecurity jargon, cyber espionage would fall under CNE. Cyber espionage is the digital equivalent of classic spying on rival state, with the key difference being that it is much less risky to spy in cyberspace, as it is done at a distance.[128]

Cyber sabotage is taking cyber espionage one step further and using this access into a target's digital systems to conduct limited attacks. The key difference between cyber espionage and cyber sabotage is that rather than just observing and mapping a target, in a cyber sabotage

---

[125] Richard Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Ecco, 2010): 193.
[126] P.W. Singer and Noah Shachtman, "The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity Is Misplaced and Counterproductive," Brookings Institution, August 15, 2011, https://www.brookings.edu/articles/the-wrong-war-the-insistence-on-applying-cold-war-metaphors-to-cybersecurity-is-misplaced-and-counterproductive/.
[127] Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (Winter 2016/17): 44-71.
[128] Jason Andress and Steve Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, 2nd ed. (Waltham: Syngress, 2014): 169-179.

mission an attacker will attempt to cause harm to an information network by doing things such as shutting it down, deleting or modifying critical data, damaging the physical network infrastructure, or depriving an opponent of its use.

Cyber espionage and cyber sabotage activities are probably common occurrences in international relations. The United States has been particularly successful using cyber sabotage operations as counter-proliferation tools against Iran's nuclear weapons program and North Korea's ballistic missile program.

CNE and CNA operations within the context of cyber espionage and sabotage are particularly useful to states as they have, so far, not provoked a conventional armed response by those who have been attacked. In this way, cyber espionage and cyber sabotage allow for states to conduct cyber-operations that fall short of armed conflict, but that can still help states pursue their national interests by affecting geopolitical outcomes.

The development of a Canadian cyberwarfare capability would allow Canada to conduct CNE- and CNA-missions in support of cyber espionage and sabotage operations. Cyber espionage and cyber sabotage could be a rationale for Canada to develop offensive cyberwarfare capabilities. However, in light of revelations that the CSE already has cyber capabilities, and is actively using cyberattacks in support of its intelligence-gathering activities, a Canadian CNE and CNA capability for the purposes of spying most certainly already exists.

Tit-for-Tat Hacking

In most countries in the world, private companies are prohibited by law from counter-attacking if they suffer a cyberattack.[129] While there has been discussion in the United States on allowing, under certain circumstances, organizations under cyberattack to "hack back,"[130] under Canadian law, Section 342.1 of the Criminal Code prohibits unauthorized access to computer systems or data transfers between computer systems.[131] This would make it illegal

[129] Kuchler, "Cyber Insecurity: Hacking back."
[130] Josephine Wolff, "When Companies Get Hacked, Should They Be Allowed to Hack Back?," *The Atlantic*, July 14, 2017, https://www.theatlantic.com/business/archive/2017/07/hacking-back-active-defense/533679/.
[131] Donna Simmons, *Laws of Canada as they pertain to Computer Crime* (SANS Institute, May 2002), https://www.sans.org/reading-room/whitepapers/legal/laws-canada-pertain-computer-crime-673.

for a Canadian company or government agency to launch a retaliatory attack against a hacker—even if such an attack was only intended to gather information on an attacker's systems or take back sensitive data that has been stolen.

Under the tit-for-tat hacking theory of cyberwarfare, when a corporation or government agency is attacked in cyberspace, a state will use its cyberwarfare capability to go on the offensive and launch a limited retaliatory strike against the attacker.

Rather than aiming to cause large-scale damage to an opponent's computer networks and critical infrastructure, the goal of such tit-for-tat hacking would be to signal to one's opponent that you are aware of their transgressions on your state's computer networks; and that this transgression is not appreciated. Beyond mere retribution, the aim of such a counterattack would be to raise the cost for an opponent to launch an attack, and help the victim of the hacking recover its assets and strengthen its cyber-defences.

Under this theory, a cyberattack would not really constitute cyberwar in a conventional sense, it would be something less than war. A state following a tit-for-tat hacking strategy would demonstrate that its cyber-operations forces are prepared to meet cyberattacks in-kind, but would not necessarily escalate the situation. Like cyber deterrence, this would hopefully dissuade hackers from targeting a state's information systems. However, in contrast to deterrence, the response would be limited and would end at a single and proportional retaliatory cyberattack. Escalating to using physical force would be disallowed under a tit-for-tat strategy.

Just as cyber deterrence, tit-for-tat hacking at first glance may seem like a reasonable way to protect Canadians and their information networks in cyberspace. However, in practice, tit-for-tat hacking is not a useful rationale for Canada to develop an offensive cyberwarfare capability. In a tense geopolitical environment, such tit-for-tat hacking could quickly and unexpectedly escalate into serious conflict. Such an escalating conflict, precipitated from tit-for-tat hacking to defend a government or private sector computer network from foreign cyberattack, could take Canada in diplomatic and military directions that it did not intend to go.

As stated previously in this paper, a Canadian cyberwarfare capability by necessity must be aligned with Canadian policy and national strategy. A reactive tit-for-tat response to cyberattacks would not produce such alignment. And furthermore, it would put Canada's long-term security interests at risk for short-term computer network security.

Keep Up with the Joneses

In the context of cyberwarfare, to keep up with the Joneses refers to the idea that if one's allies are acquiring cyberwarfare capabilities, your state must do so as well. After all, you do not want your state to be perceived as falling behind in the development of a critically important new security asset. Rival states will take note of this perceived gap in your national defence capabilities, while allies will note this same deficiency and question if your state is pulling its own weight in the alliance.

While the idea of Keeping up with the Joneses is a poor way to run a household—or to live one's life in general—it does have value as an argument for Canada to develop cyberwarfare capabilities. This is because Canada has traditionally relied on its allies in the United States, the United Kingdom, and Western Europe for collective defence. Canada has greatly benefited from having a robust network of international security alliances throughout its history.

This alliance structure has held up over the First World War, the Second World War, the Cold War, and remains in place today. Canada's recent role in Afghanistan, and its current missions in Northern Iraq and Eastern Europe, are a direct result of Canada's membership in this alliance structure. Canada takes on such missions as it strives to meet its security obligations.

Through security cooperation arrangements such as NORAD, NATO, and the "Five Eyes" intelligence-sharing network—which consists of the United States, the United Kingdom, Canada, Australia, and New Zealand—Canada gains an immense amount of security at a bargain-basement price.[132] In 2016, Canada spent $20.3 billion on defence, or just under 1

[132] Steve Saideman, "Canada and NATO, NATO and Canada," *OpenCanada.org*, May 20, 2012, https://www.opencanada.org/features/canada-and-nato-nato-and-canada/; James Cox, *Canada and the Five Eyes Intelligence Community* (Canadian International Council and the Canada Defence & Foreign Affairs Institute, 2012),

per cent of its GDP.[133] To maintain these partnerships, Canada could develop a modest cyberwarfare capability to signal to allies that Canada is a useful, sophisticated, and dedicated security partner.

While the keeping up with the Joneses argument of cyberwarfare may seem suspect at first glance, it may be one of the best policy rationales to develop cyberwarfare capabilities. It would fit in well with a body of Canadian defence and security policy that has worked to keep Canadians secure in the past. The signalling of Canada's commitment to collective security through the development of cyberwarfare capabilities is of critical importance at a time where the relevance of collective security is being openly questioned in the United States under the Trump administration.[134]

PART V – LEGAL CONSIDERATIONS

Like any other military capability, the development of a Canadian cyberwarfare capability would produce a thorny nest of legal issues under international law that would need to be addressed. There is no current treaty or body of international law that bans or regulates offensive cyber-operations in the international system. And there is currently no such thing as a "cyberwarfare treaty" to govern state behavior.[135]

The specific areas of international law that would pertain to the use of cyberwarfare capabilities would be dependent on the diplomatic status shared by Canada and the belligerent actor (and whether an opponent is a state or non-state actor), and the nature of the targets of such a cyberattack.

---

http://cdfai.org.previewmysite.com/PDF/Canada%20and%20the%20Five%20Eyes%20Intelligence%20Community.pdf.

[133] Murray Brewster, "Canada Ranks 23 out of 28 NATO Countries on Defence Spending," *CBC News*, July 4, 2016, http://www.cbc.ca/news/politics/canada-defence-spending-1.3664272.

[134] Simon Shuster, "Can NATO Survive a Donald Trump Presidency?," *Time*, November 14, 2016, http://time.com/4569578/donald-trump-nato-alliance-europe-afghanistan/.

[135] The Shanghai Cooperative Organization (SCO) has proposed an *International Code of Conduct for Information Security* that would include language to disallow the use of digital systems for hostile activities; see Sarah McKune, "Will the SCO states' Efforts to Address 'Territorial Disputes' in Cyberspace Determine the Future of International Human Rights Law?," *Citizen Lab*, September 28, 2015, https://citizenlab.org/2015/09/international-code-of-conduct/.

Cyberattacks during a State of Armed Conflict

In the case of the existence of an armed conflict between Canada and the belligerent, the principles of international humanitarian law (IHL) would apply.[136] IHL does not specifically address cyberwarfare or CNO.[137] But under IHL, a cyberwarfare capability would be subject to the same considerations and restrictions as other weapons of war. Namely, the use of cyberweapons would need to conform to IHL's principles of distinction, necessity, proportionality, humane treatment, and non-discrimination.[138]

According to the International Committee of the Red Cross, the interlinked nature of computer networks creates a risk that targeted information systems may support both legitimate military targets and civilian IT infrastructure.[139] Despite this potential legal issue created by dual-use IT systems, and the complexity of computer networks, the Red Cross also points out that cyber-operations could also be used to minimize collateral damage during wartime and help reduce civilian casualties.[140] As there are few known cases of cyberweapons being used on the battlefield outside of niche roles, how IHL would govern such arms is purely speculative in nature.

Cyberattacks during the Absence of a State of Armed Conflict

In the case that no state of armed conflict exists between Canada and the belligerent, a cyberattack may or may not constitute an act of war depending on the nature of the attack, and if it is perceived to have caused damage or death as a direct consequence. Bodies of customary international law, such as the United Nations (UN) Charter, did not foresee cyberwarfare as an issue when they were drafted.[141]

---

[136] Joseph S. Nye, *The Future of Power*: 145.
[137] Hugh M. Kindred, et al., *International Law Chiefly as Interpreted and Applied in Canada*, 8th ed. (Toronto: Emond Montgomery Publications, 2014): 561.
[138] Ibid., 537-543; Carr, *Inside Cyberwarfare*: 71.
[139] "What Limits Does the Law of War Impose on Cyber Attacks?" *International Committee of the Red Cross*, June 28, 2013, https://www.icrc.org/eng/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm.
[140] Ibid.
[141] Nils Melzer, *Cyberwarfare and International Law* (UNIDIR Resources, 2011): 9, http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.

Furthermore, while instances of cyberwarfare are becoming more and more common in the international system, there have not been enough incidents and overt responses to create international norms that would informally govern the use of cyberweapons.[142]

Under Article 51 of the UN Charter,[143] for states suffering a cyberattack to be permitted to militarily strike back, the attack must be serious and damaging enough to constitute an "armed attack" under the wording of the UN Charter.[144]

The threshold between what constitutes an armed attack under Article 2(4) of the UN Charter is not well understood as it has not yet been invoked in response to a cyberattack. However, the key issue in determining if a cyberattack would constitute an armed attack is the consequences, or effects, of such an attack.[145] As legal scholar Michael N. Schmitt observes, "it is seldom the instrument employed, but instead the consequences suffered, that matter to States."[146]

Cyberattacks that fall below the threshold of an armed attack—such as cyber intelligence operations, state-directed cybercrime and fraud, or disruption of non-essential services—[147] would fall outside of the purviews of international conflict management. These below-threshold attacks would need to be dealt with as a law enforcement issue; or, in the case of

---

[142] This being said, arms control experts such as Joseph S. Nye believe that the creation of norms through international dialogue as a potentially useful way to limit destructive cyberattacks between state actors; see Joseph S. Nye, "A Normative Approach to Preventing Cyberwarfare," *Project Syndicate*, March 13, 2017, https://www.project-syndicate.org/commentary/global-norms-to-prevent-cyberwarfare-by-joseph-s--nye-2017-03.

[143] United Nations, Charter of the United Nations, Chapter VII, Article 51, http://www.un.org/en/sections/un-charter/chapter-vii/.

[144] Charles J. Dunlap, "Perspectives for Cyber Strategists on Law for Cyberwar," *Strategic Studies Quarterly*, 5, no. 1 (Spring 2011): 81-99.

[145] Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," *Columbia Journal of Transnational Law* 37 (1998-99), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1603800.

[146] Michael N. Schmitt, "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts," in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington D.C.: National Research Council, 2010): 154.

[147] Jason Thelen, "Applying International Law to Cyber Warfare," *RSA Conference 2014*, San Francisco, CA, February 24-28, 2014, https://www.rsaconference.com/writable/presentations/file_upload/law-f03a-applying-international-law-to-cyber-warfare.pdf.

cyber-espionage, under a state's domestic espionage laws.[148] The Budapest Convention would help targeted states prosecute such below-threshold attacks.

While not considered to be a legally-binding document, the best publically available policy guidance on how cyberwarfare capabilities interface with international law can be found in the 2012/17 *Tallinn Manual on the International Law Applicable to Cyber Warfare.*[149] This academic manual, produced by NATO's Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia provides states with a comprehensive interpretation of existing international law as it applies to cyberwarfare, and is perhaps the most useful document currently available on the details of responding to cyberattacks and cyberwarfare.

PART VI – CONCLUSION

This paper has explored the policy challenge of cyberwarfare and Canada's evolving cybersecurity policy. It has attempted to define key issues in cybersecurity and cyberwarfare. It has also mapped out Canada's current approach to cybersecurity policy. The paper has found that in most instances, the Canadian government's strategy towards cybersecurity is out of date and lacking in vision.

Furthermore, this paper has offered seven theo, ries, or rationales, to explain why states would develop a cyberwarfare capability. It has then tested the seven theories to establish if any of them suggest that the acquisition of a Canadian cyberwarfare capability would enhance Canada's national security.

This theory testing suggests that developing a modest cyberwarfare capability would enhance Canada's national security in two ways:

- *Augment conventional military capabilities*—developing a cyberwarfare capability would enhance Canada's conventional military capabilities.

[148] Christopher S. Yoo, "Cyber Espionage or Cyberwar?: International Law, Domestic Law, and Self-Protective Measures," working paper, University of Pennsylvania Law School, 2015, http://scholarship.law.upenn.edu/faculty_scholarship/1540.
[149] NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, ed. Michael N. Schmitt, 2nd ed. (London: Cambridge University Press, 2017).

- *Keep up with the Joneses*—developing a cyberwarfare capability would signal to Canada's allies that Canada is a techniolgically sophisticated and reliable security partner who is worthwhile to maintain security alliances with.

Both the military enhancement and alliance signalling advantages of a Canadian cyberwarfare capability suggest that Canada would be able to enhance its national security by pursuing offensive cyberwarfare capabilities.

Such capabilities would provide Canadian policy makers additional strategic options with which to deal with national security issues. They would also enhance the effectiveness of the Canadian Armed Forces. And help Canada maintain its critical network of security partnerships such as the NORAD, the Five Eyes, and NATO. For these reasons, this paper advocates that Canada should develop a modest cyberwarfare capability. Canada's 2017 defence policy is a leap in the right direction.

REFERENCES

Allen, Frances. *CN(EH?): Should the CF Adopt Computer Network Exploitation and Attack Capabilities?* Master's thesis, Canadian Forces College, 2002. http://www.cfc.forces.gc.ca/259/181/74_allen.pdf.

Andress, Jason and Steve Winterfeld. *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. 2nd ed. Waltham: Syngress, 2014.

Arellano, Nestor. "Government Computer Networks can't Standup to Cyberattacks: Report." *Vanguard*, January 12, 2017. http://www.vanguardcanada.com/2017/01/12/government-computer-networks-cant-standup-to-cyberattacks-report/.

Ballingall, Alex. "StatsCan Hacked after Government Sites Made Vulnerable: Officials." *Toronto Star*, March 13, 2017. https://www.thestar.com/news/canada/2017/03/13/statscan-hacked-after-government-sites-made-vulnerable-officials.html.

Barton, Rosemary. "Chinese Cyberattack Hits Canada's National Research Council." *CBC News*, July 29, 2017. http://www.cbc.ca/news/politics/chinese-cyberattack-hits-canada-s-national-research-council-1.2721241.

BBC News. "Hackers behind Ukraine Power Cuts, Says US Report." February 26, 2016. http://www.bbc.com/news/technology-35667989.

———. "Ukraine Power Cut 'was Cyber-Attack'." January 11, 2017. http://www.bbc.com/news/technology-38573074.

Beauchamp, Zack. "The Key Findings from the US Intelligence Report on the Russia Hack, Decoded." *Vox*, January, 6, 2017. http://www.vox.com/world/2017/1/6/14194986/russia-hack-intelligence-report-election-trump.

Bell, Stewart. "Federal Government Facing 'Serious' Cyber Attacks from State-Sponsored Hackers and Terrorist Groups: CSIS." *National Post*, February 28, 2017. http://news.nationalpost.com/news/canada/federal-government-facing-serious-cyber-attacks-from-state-sponsored-hackers-and-terrorist-groups-csis.

Bernier, Melanie and Joanne Treurniet. "Understanding Cyber Operations in a Canadian Strategic Context: More than C4ISR, More than CNO." In *Conference on Cyber Conflict Proceedings 2010*. Eds. C. Czosseck and K. Podins. Tallinn, Estonia: COE Publications, 2010.

———. *CF Cyber Operations in the Future Cyber Environment Concept.* Ottawa: Defence R&D Canada, December 2009. http://cradpdf.drdc-rddc.gc.ca/PDFS/unc92/p532776.pdf.

Betz, David J. and Tim Stevens. *Cyberspace and the State: Toward a Strategy for Cyber-Power.* London: The International Institute for Strategic Studies, 2011.

Blum, Andrew. *Tubes: A Journey to the Center of the Internet.* Toronto: HarperCollins, 2012.

Braga, Matthew. “Where Canada's Three Political Parties Stand on Cybersecurity and Surveillance.” *Vice Motherboard*, October 9, 2015. https://motherboard.vice.com/en_us/article/where-canadas-three-political-parties-stand-on-cybersecurity-and-surveillance.

Brewster, Murray. “Canada Ranks 23 out of 28 NATO Countries on Defence Spending.” *CBC News*, July 4, 2016. http://www.cbc.ca/news/politics/canada-defence-spending-1.3664272.

———. “Former CSIS Head Says Canada Should Have its Own Cyber-Warriors.” *CBC News*, June 22, 2016. http://www.cbc.ca/news/politics/military-cyber-wars-fadden-1.3648214.

———. “Canada's Electronic Spy Service to Take More Prominent Role in ISIS Fight.” *CBC News*, February 18, 2016. http://www.cbc.ca/m/touch/politics/story/1.3454617.

Brownell, Claire. “Hackers are Bombarding the Bank of Canada with Cyber Attacks and the Crack in the Bank's Armour is its Employees.” *Financial Post*, January 26, 2017. http://business.financialpost.com/technology/hackers-bombard-the-bank-of-canada-with-cyberattacks.

Boutilier, Alex. “Canada’s Spies Examining ‘Vulnerabilities’ in Election System.” *Toronto Star*, May 12, 2017. https://www.thestar.com/news/canada/2017/05/12/canadas-spies-examining-vulnerabilities-in-election-system.html.

———. “Canada Developing Arsenal of Cyber-Weapons.” *Toronto Star*, March 16, 2017. https://www.thestar.com/news/canada/2017/03/16/canada-developing-arsenal-of-cyber-weapons.html.

Buchanan, Ben. *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations.* New York: Oxford University Press, 2017.

Carr, Jeffrey. *Inside Cyber Warfare*. Sebastopol: O'Reilly Media, 2012.

CBC News. “Tax time 2015: How to File Your Tax Return Online.” March 2, 2015. http://www.cbc.ca/news/business/taxes/tax-time-2015-how-to-file-your-tax-return-online-1.2960477.

———. “Heartbleed Bug May Shut Revenue Canada Website until Weekend.” April 9, 2014. http://www.cbc.ca/news/business/heartbleed-bug-may-shut-revenue-canada-website-until-weekend-1.2603742.

Center for Strategic and International Studies. *Net Losses: Estimating the Global Cost of Cybercrime*. McAfee, June 2014. http://www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf.

Connolly, Amanda. “Experts say Munk Debate Needs to Include Cybersecurity.” *iPolitics*, September 23, 2015. http://ipolitics.ca/2015/09/23/experts-say-munk-debate-needs-to-include-cybersecurity/.

Cornish, Paul, David Livingstone, Dave Clemente, and Claire Yorke. *On Cyberwarfare.* London: Chatham House, November 2010. https://www.chathamhouse.org/publications/papers/view/109508.

Council of Europe. Chart of Signatures and Ratifications of Treaty 189: Additional Protocol to the Convention on Cybercrime Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems. Last modified March 3, 2017. http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p_auth=LGcvu24X.

———. Chart of Signatures and Ratifications of Treaty 185: Convention on Cybercrime. Last modified March 3, 2017. http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=tcrnNcYJ.

———. *Additional Protocol to the Convention on Cybercrime Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems.* Strasbourg: European Treaty Series, 2003. https://rm.coe.int/168008160f.

———. *Explanatory Report to the Convention on Cybercrime.* Budapest: European Treaty Series, 2001. https://rm.coe.int/16800cce5b.

Cox, James. *Canada and the Five Eyes Intelligence Community*. Canadian International Council and the Canada Defence & Foreign Affairs Institute, 2012. http://cdfai.org.previewmysite.com/PDF/Canada%20and%20the%20Five%20Eyes%20Intelligence%20Community.pdf.

Davis, Joshua. "Hackers Take Down the Most Wired Country in Europe." *Wired*, August 21, 2007. https://www.wired.com/2007/08/ff-estonia/.

Department of Defense (United States). *Department of Defense Strategy for Operating in Cyberspace*. July 2011. http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

Department of National Defence (Canada). *Strong, Secure, Engaged: Canada's Defence Policy*. Ottawa: Her Majesty the Queen in Right of Canada, 2017. http://dgpaapp.forces.gc.ca/en/canada-defence-policy/index.asp.

———. Operation REASSURANCE. Last modified May 9, 2017. http://www.forces.gc.ca/en/operations-abroad/nato-ee.page.

Dunlap, Charles J. "Perspectives for Cyber Strategists on Law for Cyberwar." *Strategic Studies Quarterly* 5, no. 1 (Spring 2011): 81-99.

Dunn Cavelty, Myriam. "Cyberwar: Concept, Status Quo, and Limitations." *CSS Analysis in Security Policy*, no. 71 (April 2010). http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSS-Analyses-71.pdf.

Easton, Stephen, Hilary Furness, and Paul Brantingham. *The Cost of Crime in Canada.* Vancouver: Fraser Institute, October 2014. https://www.fraserinstitute.org/sites/default/files/cost-of-crime-in-canada.pdf.

Economist. "Marching Off to Cyberwar." December 4, 2008. http://www.economist.com/node/12673385.

Elliott, David. "Deterring Strategic Cyberattack." *IEEE Security & Privacy* (September/October 2011): 36-40.

Fekete, Jason and Ian Macleod. "Hacker Group 'Anonymous' Claims Credit for Federal Cyber Attacks." *Ottawa Citizen*, June 17, 2015. http://ottawacitizen.com/news/politics/federal-computer-servers-cyber-attacked-clement.

Fisher, Matthew. "Canada's Forces Deployed in Latvia to Include 'Cyber Warriors' to Counter Russians." *National Post*, March 9, 2017. http://news.nationalpost.com/news/world/matthew-fisher-canadas-forces-deployed-in-latvia-to-include-cyber-warriors-to-counter-russian-attacks.

Florencio, Dinei and Cormac Herley. "Sex, Lies and Cyber-crime Surveys." *10th Workshop on the Economics of Information Security*, Fairfax, VA, United States, June 1, 2011. Available at: https://www.microsoft.com/en-us/research/publication/sex-lies-and-cyber-crime-surveys/.

Freeze, Colin. "Hackers Target Canadian Government's Energy and Resource Departments." *Globe and Mail*, November 17, 2016. http://www.theglobeandmail.com/news/politics/hackers-target-governments-energy-and-resource-departments/article32890960/.

———. "China Hack Cost Ottawa 'Hundreds of Millions,' Documents Show." *Globe and Mail*, March 30, 2017. https://beta.theglobeandmail.com/news/national/federal-documents-say-2014-china-hack-cost-hundreds-of-millions-of-dollars/article34485219/?ref=http://www.theglobeandmail.com&.

Forcese, Craig and Kent Roach. "The Roses and the Thorns of Canada's New National Security Bill." *Maclean's*, June 20, 2017. http://www.macleans.ca/politics/ottawa/the-roses-and-thorns-of-canadas-new-national-security-bill/.

Forrester Research. "Canadian Online Retail Forecast, 2014 to 2019." October 14, 2014. https://www.forrester.com/report/Canadian+Online+Retail+Forecast+2014+To+2019/-/E-RES115497.

Gertz, Bill. *iWar: War and Peace in the Information Age*. New York: Threshold, 2017.

Government of Canada. *Cyber Threats to Canada's Democratic Process.* Ottawa: Communications and Security Establishment, 2017. https://www.cse-cst.gc.ca/sites/default/files/cse-cyber-threat-assessment-e.pdf.

———. *Canada 2030: Scan of Emerging Issues.* Ottawa: Policy Horizons Canada, 2017. http://www.horizons.gc.ca/eng/content/canada-2030-scan-emerging-issues-infrastructure.

———. *Security and Prosperity in the Digital Age: Consulting on Canada's Approach to Cyber Security*. Ottawa: Public Safety Canada, 2016. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-scrty-prsprty/index-en.aspx.

———. *Digital Canada 150.* Ottawa: Industry Canada, 2014. http://www.ic.gc.ca/eic/site/028.nsf/eng/home.

———. *Action Plan for Critical Infrastructure: 2014-2017*. Ottawa: Public Safety Canada, 2014. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pln-crtcl-nfrstrctr-2014-17/index-en.aspx.

———. *Cyber Incident Management Framework for Canada.* Ottawa: Public Safety Canada, 2013. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-ncdnt-frmwrk/index-en.aspx.

———. *Canada's Cyber Security Strategy.* Ottawa: Public Safety Canada, 2010. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-en.aspx.

Greenberg, Andy. "The NSA Confirms It: Russia Hacked French Election 'Infrastructure'." *Wired*, May 9, 2017. https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/.

Hadnagy, Christopher. *Social Engineering: The Art of Human Hacking*. Indianapolis: Wiley Publishing, 2011.

Hildebrandt, Amber, Dave Seglins, Michael Pereira. "Communication Security Establishment's Cyberwarfare Toolbox Revealed." *CBC News*, March 23, 2015. http://www.cbc.ca/news/canada/communication-security-establishment-s-cyberwarfare-toolbox-revealed-1.3002978.

Holsti, K.J. "The Concept of Power in the Study of International Relations." *Background* 7, no. 4 (1964): 179-194.

Huntley, Wade L. "Strategic Implications of Offense and Defense in Cyberwar." *49th Hawaii International Conference on System Sciences.* Koloa, Hawaii: IEEE, 2016.

International Committee of the Red Cross. "What Limits Does the Law of War Impose on Cyber Attacks?" June 28, 2013. https://www.icrc.org/eng/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm.

Kindred, Hugh M., Phillip M. Saunders, Robert J. Currie, Jutta Brunnée, Ted L. McDorman, Ikechi Mgbeoji, Karin T. Mickelson, René Provost, Linda C. Reif, Chris Waters. *International Law Chiefly as Interpreted and Applied in Canada*. 8th ed. Toronto: Emond Montgomery Publications, 2014.

Kissinger, Henry. *World Order*. New York: Penguin Press, 2014.

Klimburg, Alexander. *The Darkening Web: The War for Cyberspace*. New York: Penguin, 2017.

Kramer, Franklin D., Stuart H. Starr, Larry Wentz, Elihu Zimet, Lesley J. McNair, and Daniel Kuehl. "Frameworks and Insights Characterizing Trends in Cyberspace and Cyberpower." *12th International Command and Control Research and Technology Symposium*. Newport, Rhode Island, June 2007. Available at: https://www.semanticscholar.org/paper/Frameworks-and-Insights-Characterizing-Trends-in-C-Kramer-Starr/5eb231cdb687265a0099cf498165a17a66fd012f.

Lambeth, Benjamin S. "Airpower, Spacepower, and Cyberpower." *Joint Forces Quarterly* 60 (First Quarter 2011): 46-53.

Liberal Party of Canada. *Real Change: A New Plan for a Strong Middle Class.* Liberal Party of Canada, 2015. https://www.liberal.ca/wp-content/uploads/2015/10/New-plan-for-a-strong-middle-class.pdf.

Liberal Senate Forum. "The State of Cyber Security in Canada." October 19, 2016. http://liberalsenateforum.ca/open-caucus/october-19-2016-state-cyber-security-canada/.

Libicki, Martin C. "Cyberwar as a Confidence Game." *Strategic Studies Quarterly* (Spring 2011): 132-146.

Lindblom, Charles E. "Still Muddling, Not Yet Through." *Public Administration Review* 39, no. 6 (November/December 1979): 517-526.

———. "The Science of 'Muddling Through.'" *Public Administration Review* 19, no. 2 (Spring 1959): 79-88.

Ling, Justin. "Cyber War." *Vice News Canada*, January 18, 2017. https://news.vice.com/story/canada-is-deciding-whether-it-wants-to-get-into-the-business-of-cyberwar.

Lipton, Eric, David E. Sanger, and Scott Shane. "The Perfect Weapon: How Russian Cyberpower Invaded the U.S." *New York Times*, December 13, 2016. https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0.

Makovsky, David. "The Silent Strike: How Israel Bombed a Syrian Nuclear Installation and Kept it a Secret." *The New Yorker*, September 17, 2012. http://www.newyorker.com/magazine/2012/09/17/the-silent-strike.

Manyika, James and Charles Roxburgh. *The Great Transformer: The Impact of the Internet on Economic Growth and Prosperity.* McKinsey Global Institute, October 2011. http://www.mckinsey.com/industries/high-tech/our-insights/the-great-transformer.

Markoff, John. "Before the Gunfire, Cyberattacks." *New York Times*, August 12, 2008. http://www.nytimes.com/2008/08/13/technology/13cyber.html.

McKune, Sarah. "Will the SCO States' Efforts to Address 'Territorial Disputes' in Cyberspace Determine the Future of International Human Rights Law?" *Citizen Lab*, September 28, 2015. https://citizenlab.org/2015/09/international-code-of-conduct/.

Melzer, Nils. *Cyberwarfare and International Law*. UNIDIR Resources, 2011. http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.

Miller, Charlie. *The Legitimate Vulnerability Market: Inside the Secretive World of 0-day Exploit Sales*. Independent Security Evaluators, 2007. http://www.econinfosec.org/archive/weis2007/papers/29.pdf.

Moens, Alexander, Seychelle Cushing, and Alan W. Dowd. *Cybersecurity Challenges for Canada and the United States.* Vancouver: Fraser Institute, March 2015. https://www.fraserinstitute.org/sites/default/files/cybersecurity-challenges-for-canada-and-the-united-states.pdf.

Moffatt, Stewart. "Canadian Social Media Statistics." Sherpa Marketing, July 1, 2014. https://www.sherpamarketing.ca/blogs/canadian-social-media-statistics-.

Mussington, David. "Bill C-59 – The Canadian National Security Act 2017: What You Need to Know." Centre for International Governance Innovation, July 2, 2017. https://www.cigionline.org/articles/bill-c-59-canadian-national-security-act-2017-what-you-need-know.

NATO Cooperative Cyber Defence Centre of Excellence. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Michael N. Schmitt ed., 2nd ed. London: Cambridge University Press, 2017.

Nielsen, *Cyber Review Consultations Report.* Ottawa: Public Safety Canada, 2017. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2017-cybr-rvw-cnslttns-rprt/2017-cybr-rvw-cnslttns-rprt-en.pdf.

Nye, Joseph S. "A Normative Approach to Preventing Cyberwarfare." *Project Syndicate*, March 13, 2017. https://www.project-syndicate.org/commentary/global-norms-to-prevent-cyberwarfare-by-joseph-s--nye-2017-03.

———. "Deterrence and Dissuasion in Cyberspace." *International Security* 41, no. 3 (Winter 2016/17): 44-71.

———. *The Future of Power*. New York: Public Affairs, 2011.

———. "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly* (Winter 2011): 18-38.

Office of the Auditor General of Canada. *2012 Fall Report of the Auditor General of Canada.* Ottawa: Government of Canada, 2012. http://www.oag-bvg.gc.ca/internet/English/parl_oag_201210_e_37321.html.

Open Parliament. Bill C-59: An Act Respecting National Security Matters. June 20, 2017. https://openparliament.ca/bills/42-1/C-59/.

Pomerleau, Mark. "Army Takes Strategic Cyber Capabilities to the Tactical Edge." *C4ISRNET*, February 9, 2017. http://www.c4isrnet.com/articles/army-takes-strategic-cyber-capabilities-to-the-tactical-edge.

Ponemon Institute. "Cost of Data Breach Study: Global Analysis, 2016." https://www-03.ibm.com/security/data-breach/.

Public Policy Forum. *Securing Canada's Cyberspace.* February 2017. http://www.ppforum.ca/publications/securing-canada%E2%80%99s-cyberspace.

Public Safety Canada. "Canadian Cyber Incident Response Centre (CCIRC)." Last modified April 4, 2016. https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-en.aspx.

PricewaterhouseCoopers. "Global Economic Crime Survey 2016: Canadian Insights." In *PwC 2016 Global Economic Crime Survey*, 2016, https://www.pwc.com/ca/en/services/deals/publications/economic-crime-survey.html.

Public Works and Government Services Canada. "Tactical Edge Cyber Command and Control." Call for letters of interest, *Buyandsell.gc.ca*, last modified May 12, 2017. https://buyandsell.gc.ca/procurement-data/tender-notice/PW-15-00668957.

———. "Defensive Cyber Operations Project." Call for letters of interest, *Buyandsell.gc.ca*, last modified January 26, 2017. https://buyandsell.gc.ca/procurement-data/tender-notice/PW-QE-049-26100.

Raj, Althia. "Canadian Parliament Shuts Down Emails over Fears of Hacking." *Huffington Post*, June 25, 2017. http://www.huffingtonpost.ca/2017/06/25/canadian-government-emails-shut-down-over-fears-of-hacking_a_23000911/.

Reuters. "Massive Cyber Attack Could Trigger NATO Response: Stoltenberg." June 15, 2016, http://www.reuters.com/article/us-cyber-nato-idUSKCN0Z12NE.

Rohozinski, Rafal and Ronald Deibert. *Tracking GhostNet: Investigating a Cyber Espionage Network.* SecDev Group and Citizen Lab, Munk Centre for International Studies, University of Toronto, March 29, 2009. https://citizenlab.ca/2009/03/tracking-ghostnet-investigating-a-cyber-espionage-network/.

Royal Canadian Mounted Police. "Cybercrime: An Overview of Incidents and Issues in Canada." Last modified December 16, 2014. http://www.rcmp.gc.ca/en/cybercrime-an-overview-incidents-and-issues-canada.

Saideman, Steve. "Canada and NATO, NATO and Canada." *OpenCanada.org*, May 20, 2012. https://www.opencanada.org/features/canada-and-nato-nato-and-canada/.

Sanger, David E. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. 2nd ed. New York: Broadway Books, 2013.

Sanger, David E., and William J. Broad. "Hand of U.S. Leaves North Korea's Missile Program Shaken." *New York Times*, April 18, 2017. https://www.nytimes.com/2017/04/18/world/asia/north-korea-missile-program-sabotage.html.

———. "Trump Inherits a Secret Cyberwar Against North Korean Missiles." *New York Times*, March 4, 2017. https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html?_r=0.

Schmitt, Michael N. "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts." In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy.* Washington D.C.: National Research Council, 2010.

———. "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework." *Columbia Journal of Transnational Law* 37 (1998-99): 885-937. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1603800.

Senate of Canada. *Reinvesting in the Canadian Armed Forces: A Plan for the Future*, Report of the Standing Senate Committee on National Security and Defence, eds. Daniel Lang and Mobina S.B. Jaffer. Ottawa: Senate of Canada, May 2017. https://sencanada.ca/en/committees/secd.

———. *Military Underfunded: The Walk Must Match the Talk*. Report of the Standing Senate Committee on National Security and Defence, eds. Daniel Lang and Mobina S.B. Jaffer. Ottawa: Senate of Canada April 2017. https://sencanada.ca/content/sen/committee/421/SECD/Reports/DEFENCE_DPR_FINAL_e.pdf.

———. *Debates of the Senate* 150, no. 69, November 2, 2016. https://sencanada.ca/Content/SEN/Chamber/421/Debates/pdf/069db_2016-11-02-e.pdf.

———. *Proceedings of the Standing Senate Committee on National Security and Defence*. Issue 2, March 7, 2016. https://sencanada.ca/en/Content/Sen/Committee/421/SECD/02ev-52409-e.

Shuster, Simon. "Can NATO Survive a Donald Trump Presidency?" *Time*, November 14, 2016. http://time.com/4569578/donald-trump-nato-alliance-europe-afghanistan/.

Simmons, Donna. *Laws of Canada as They Pertain to Computer Crime*. SANS Institute, May 2002. https://www.sans.org/reading-room/whitepapers/legal/laws-canada-pertain-computer-crime-673.

Singer, P.W. "How the United States Can Win the Cyberwar of the Future." *Foreign Policy*, December 18, 2015. http://foreignpolicy.com/2015/12/18/how-the-united-states-can-win-the-cyberwar-of-the-future-deterrence-theory-security/.

Singer, P.W. and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know.* New York: Oxford University Press, 2014.

P.W. Singer and Noah Shachtman. "The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity Is Misplaced and Counterproductive." Brookings Institution, August 15, 2011, https://www.brookings.edu/articles/the-wrong-war-the-insistence-on-applying-cold-war-metaphors-to-cybersecurity-is-misplaced-and-counterproductive/.

Sloan, Elinor C. *The Revolution in Military Affairs: Implications for Canada and NATO*. Montreal & Kingston: McGill-Queen's University Press, 2002.

Statistics Canada. "Canadian Internet Use Survey, 2012." Last modified November 26, 2013. http://www.statcan.gc.ca/daily-quotidien/131126/dq131126d-eng.htm.

Stone, John. "Cyber War Will Take Place!" *Journal of Strategic Studies* 36, no. 1 (2013): 101-108.

Talbot, David. "Cyber-Espionage Nightmare." *MIT Technology Review*, June 10, 2015. https://www.technologyreview.com/s/538201/cyber-espionage-nightmare/.

Thelen, Jason. "Applying International Law to Cyber Warfare." *RSA Conference 2014*. San Francisco, CA, February 24-28, 2014. https://www.rsaconference.com/writable/presentations/file_upload/law-f03a-applying-international-law-to-cyber-warfare.pdf.

Tikk, Eneken. "Ten Rules for Cyber Security." *Survival* 53, no.3 (June-July 2011): 119-132.

United Nations. Charter of the United Nations. Chapter VII, Article 51. http://www.un.org/en/sections/un-charter/chapter-vii/.

Valentino-DeVries, Jennifer and Danny Yadron. "Cataloging the World's Cyberforces." *Wall Street Journal*, October 11, 2015. https://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710.

Vatis, Michael. "The Next Battlefield: The Reality of Virtual Threats." *Harvard International Review* 28, no. 3 (Fall 2016): 56-71.

Wark, Wesley. "The Summer of Cyber Attacks." *Ottawa Sun*, July 3, 2015. http://www.ottawasun.com/2015/07/03/the-summer-of-cyber-attacks.

Weinberger, Sharon. "How Israel Spoofed Syria's Air Defence System." *Wired*, October 4, 2007. https://www.wired.com/2007/10/how-israel-spoo/.

Weston, Greg. "Foreign Hackers Attack Canadian Government." *CBC News*, February 16, 2011. http://www.cbc.ca/news/politics/foreign-hackers-attack-canadian-government-1.982618.

Wolff, Josephine. “When Companies Get Hacked, Should They Be Allowed to Hack Back?” *The Atlantic*, July 14, 2017. https://www.theatlantic.com/business/archive/2017/07/hacking-back-active-defense/533679/.

World Economic Forum. *The Global Risks Report 2016*, 11th ed. World Economic Forum, 2016. http://www3.weforum.org/docs/Media/TheGlobalRisksReport2016.pdf.

Zetter, Kim. “An Unprecedented Look at Stuxnet, the World's First Digital Weapon.” *Wired*, November 3, 2014. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

———. “Hacker Lexicon: What is a Zero Day?” *Wired*, November 11, 2014. https://www.wired.com/2014/11/what-is-a-zero-day/.

———. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon.* New York: Crown, 2014.