National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

Choosing Complicated: The Canadian Approach to National Security in Cyberspace

Lieutenant-Colonel James R.D. Siebring

JCSP 47

Master of Defence Studies

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI 47

Maîtrise en études de la défense

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 47 – PCEMI 47

2020 – 2021

MASTER OF DEFENCE STUDIES – MAÎTRISE EN ÉTUDES DE LA DÉFENSE

CHOOSING COMPLICATED: THE CANADIAN APPROACH TO NATIONAL SECURITY IN CYBERSPACE

By Lieutenant-Colonel J.R.D. Siebring

TABLE OF CONTENTS

ABSTRACT ii
ACRONYMS iii
INTRODUCTION 1
CHAPTER 1: NATIONAL SECURITY AND THE CANADIAN PERSPECTIVE 5
- **Elements of National Power** 5
- **Natural Determinants** 6
- **Social Determinants** 9
- **Chapter Summary** 18

CHAPTER 2: A MIDDLE POWER IN CYBERSPACE 20
- **Malicious Cyber Actors** 21
- **The Canadian National Interest** 22
- **Canadian Population and Economy** 24
- **Tools of Influence** 25
- **Chapter Summary** 32

CHAPTER 3: CANADIAN APPROACH TO CYBERSPACE 34
- **National Cyber Security Strategy 2010** 35
- **Shared Services Canada** 38
- **Strong, Secure, Engaged: Canada's Defence Policy** 39
- **National Cyber Security Strategy 2018** 40
- **Canadian Center for Cyber Security** 42
- **Communications Security Establishment Act 2019** 43
- **Review of the Canadian Cyber Program** 45
- **Chapter Summary** 53

CHAPTER 4: CAF CYBER PROGRAM AND THE BROADER ECOSYSTEM 55
- **Evolution of the CAF Cyber Program** 55
- **Organizational Structure** 58
- **Prioritization and Capacity** 62
- **Diverging Perspectives** 64

CONCLUSION 68
BIBLIOGRAPHY 71

ABSTRACT

Canada faces new threats in cyberspace. The advent of the digital age has permitted a host of malicious cyber actors to bypass its traditional geographic security assurances and reach into the country. Its high levels of connectivity, strong economy, advanced research, and alliances make it an attractive target. With the ability to act from beyond the reach of national authority, these actors have found a low-risk, high reward environment within Canada.

In response, Canada has carried forward its traditional 20th Century playbook. It has focused domestically, demonstrating little deviation from its traditional approaches to national security. It has illustrated a continued a preference for horizontal governance, retaining central control while delegating routine daily functioning of the system across multiple departments. Internal to the military, a cyber organization has been overlaid on top of existing positions and organizations, creating systemic prioritization and resource tensions. Individually these systems are complicated, even more so in combination, yet they result from deliberate decisions influenced by an unwavering national assumption of security.

ACRONYMS

ADM(IM)	Associate Deputy Minister of Information Management
CAF	Canadian Armed Forces
CCCS	Canadian Centre for Cyber Security
CBSA	Canadian Border Services Agency
CDS	Chief of Defence Staff
CFINTCOM	Canadian Forces Intelligence Command
CSE	Communications Security Establishment
DGIMO	Director General Information Management Operations
DND	Department of National Defence
GDP	Gross Domestic Product
IT	Information Technology
ICT	Information and Communications Technology
MCA	Malicious Cyber Actors
NATO	North Atlantic Treaty Organization
RCMP	Royal Canadian Mounted Police
SSC	Shared Services Canada
SSE	Strong, Secure, Engaged
UN	United Nations
UNGGE	United Nations Group of Governmental Experts
US	United States
USD	United States Dollar(s)

INTRODUCTION

The rapid advances in network technologies that marked the end of the 20th Century continue to have a profound international impact. Within Canada, high rates of connectivity and the reach of the global communications infrastructure have provided opportunity and new threats from criminals and nation-state actors. With a perspective that cyberspace is a critical element of the nation's prosperity, the country has taken a series of steps to capitalize on the opportunities presented while mitigating risk.

Between 2010 and 2020, the country released two cyber security strategies, a defence policy, updated laws and created new organizations, illustrating the Government's approach to cyberspace. Canada has demonstrated a primarily domestic focus in its approach, emphasizing efforts to improve security and counter cybercrime. In its program, Canada has acknowledged that its emphasis is challenged as the majority of cyber threats originate from outside the country.[1] The reach of the environment enables criminals and hostile states to hide behind political barriers while exploiting victims in Canada.

Worse, the threats facing the country are not limited simply to fraud and extortion. Nation-states target Canada for corporate espionage, both undermining Canadian companies' competitiveness and harming the national economy. They also leverage new social media platforms to shape public opinion, and probe the nation's critical infrastructure such as water and power systems.

Canada's response has been domestically focused, despite threats emerging from beyond its territory. It has established a central coordination organization, the Canadian Centre for Cyber

[1] Canada and Public Safety Canada, *National Cyber Security Action Plan 2019-2024: Budget 2018 Investments*, 2019, 17.

Security with aims to improve the national cybersecurity posture. On its national security portfolio, it has been less coherent. It has established a federal governance model dependent on interagency collaboration. It assigned broad roles and responsibilities to a host of federal departments, including Shared Services Canada, the Communications Security Establishment, National Defence, and Global Affairs. To oversee the program the Department of Public Safety was assigned coordinating role that lacks directive authority. The efficient functioning of the system relies on the alignment of numerous departments, each with different cultures and priorities, guided on a day-to-day basis by only the power of persuasion.[2]

Canada's national efforts have stimulated cyber programs within each of its departments, including National Defence. Within the broader government eco-system, the Canadian military has implemented a series of initiatives to adapt to the new environment. A core element of the Canadian military's program is the Cyber Force. An organizational structure created to prepare for, plan, and conduct military cyber activities. The military created the structure by adding to the Department's existing Information Technology (IT) organization, the Associate Deputy Minister of Information Management.

Within this organization, subordinate to the Deputy Minister of National Defence, it overlaid new responsibilities on existing positions and organizations, adding a new reporting relationship to the Chief of Defence Staff. The organization is responsible to the two most senior leaders within the department. In this multi-polar approach, successive levels of leadership within the Cyber Force are required to balance the requirements of multiple supervisors and divergent priorities producing systemic prioritization and resource tensions.

---

[2] Canada. "Horizontal Evaluation of Canada's Cyber Security Strategy." Ottawa, On: Public Safety, 2017, 8.

Canada's approach to national security and defence are the product of assumed safety. Through the 20th century its beneficial geography and collective security arrangements developed a national perspective that war and conflict are distant concerns. Without looming threat, the Nation had discretion on when and how it participated in global security. In this environment, it developed a multilateral foreign affairs doctrine, “horizontal” national security governance, and a contribution approach to defence aimed to maintain relationships, such as those with the US and UN. While cyberspace is now challenging the Nation's foundational assumptions, these traditional approaches continue to form the basis for Canada's response. The complicated governance of Canada's approach to national security in cyberspace is the product of the Nation's continued adherence to 20th century approaches in the digital age.

This paper will highlight these influences and the resulting Canadian Government cyber eco-system over four chapters. Chapter 1 will discuss the traditional Canadian outlook. It will explore the nation’s foundational elements to illustrate how they have shaped the national perspective. It will illustrate a country that is inwardly focused, has few defence concerns and leverages a multilateral approach to foreign affairs. Chapter 2 will examine the new threats presented in cyberspace and how they impact the foundational elements discussed earlier. It will illustrate how traditional assumptions of security are not as certain. New threats within cyberspace are now able to bypass geographic barriers and the country’s multilateral approach to foreign affairs hampered by the lack of international cyberspace norms. Building on these two chapters, the paper will then outline the Canadian response to this environment. It will review key policies and strategies with an emphasis on national security and defence. The product of Canada’s approach is a domestically focused program, one that continues its approaches to national security and foreign affairs. Finally, it will outline friction points within the governance

model impacting its effective functioning. Finally, chapter 4 will outline the military's cyber structure and draw together the analysis from earlier chapters to illustrate the cumulative resource and prioritization tensions within Canada's approach to national security in cyberspace. It will outline an environment produced through the application of 20th Century perspectives.

CHAPTER 1: NATIONAL SECURITY AND THE CANADIAN PERSPECTIVE

This chapter will illustrate Canada's national perspectives and their impact on the country's approach to foreign affairs, national security and defence. These foundational elements provide the frame through which the Canadian government views cyberspace and informs its actions. In exploring this perspective, the chapter will start by evaluating the Nation's building blocks, illustrating the foundational influences. Finally, this chapter will explore Canada's approach to foreign affairs, multilateral and centered on a rule-based international order. It will expand this discussion into the related impacts on national security and defence in Canada. It will illustrate the tension between Canada's assumed security, traditional approaches to foreign affairs and the complicated relationship it creates with the Canadian military. This chapter illustrates the traditional considerations and perspectives that continues to inform the Nation's approach to cyberspace.

Elements of National Power

Canada today is a product of its environment. Its perspectives and actions are shaped by the numerous individual elements that form the Nation's building blocks. David Jablonsky defines such building blocks as the elements of national power. His model provides a useful means to explore Canada's national perspective and key influences. The model has two primary categories: natural and social determinants.[3] The natural stem from the resources a nation possesses, those available to build the structures of the social determinants. Natural determinants

[3] David Jablonsky and J. Boone Bartholomees, "NATIONAL POWER," U.S. ARMY WAR COLLEGE GUIDE TO NATIONAL SECURITY POLICY AND STRATEGY (Strategic Studies Institute, US Army War College, 2014), JSTOR, http://www.jstor.org/stable/resrep12023.12, 104; The model also introduces informational and psychological determinants which are explored through discussion of cyberspace in later chapters.

include geography, natural resources and population; social are comprised of economy, politics and the military.

Natural Determinants

Geography

Sir Wilfred Laurier once quipped that Canada's challenge is one of too much geography.[4] Everything about its scale is grand, with a total area of 9,984,670 square kilometers; it is the world's second-largest country and possesses the longest coastline. As large as it is, it is also isolated, surrounded by three oceans and bordering the United States (US).[5]

Canada's position has made it a strategic partner for the US. In the 1930s, with the threat of war approaching, President Roosevelt stated that "the people of the United States will not sit idly by if the dominion of Canadian soil is threatened by any other empire."[6] In response, Prime Minister King promised to make Canada as resistant to attack as reasonably possible and prevent an enemy from approaching the US through Canada by air, land or sea.[7] The advent of post-World War II competition between the US and the Soviet Union, with Canada positioned between them, further cemented this relationship. US defence policy sought to ensure that any Soviet aggression could be detected and interdicted as early as possible, the goal of which was reliant on the use of Canadian geography.[8]

---

[4] Kim Richard Nossal, "The Imperatives of Canada's Strategic Geography," in *Canadian Defence Policy in Theory and Practice*, ed. Thomas Juneau, Philippe Lagassé, and Srdjan Vucetic (Cham: Springer International Publishing, 2020), 11–28, 11.

[5] "Canada - The World Factbook," accessed January 25, 2021, https://www.cia.gov/the-world-factbook/countries/canada/.

[6] Justin Massie and Srdjan Vucetic, "Canadian Strategic Cultures: From Confederation to Trump," in *Canadian Defence Policy in Theory and Practice*, ed. Thomas Juneau, Philippe Lagassé, and Srdjan Vucetic (Cham: Springer International Publishing, 2020), 13-14.

[7] *Ibid,* 14.

[8] *Ibid,* 15.

In the 20th Century, Canada's geography isolated it from threats, and intertwined its defence with the interests a global super-power. Where other nations faced external threats, Canada's geography insulated it. The resulting sense of security has had a defining impact on Canada. It has contributed to a perspective that wars and conflict are foreign matters, primarily the concern of others.

Natural Resources

In addition to the security assurances, Canada's geography has placed it close to the major economy of the US, and provided it rich reserves of natural resources. The country has over 2 million lakes and access to 20 percent of the world's freshwater. Canada also has vast energy resources, expansive forests and rich metal deposits. It is third in the world for proven oil reserves, exceeded only by Venezuela and Saudi Arabia.[9] It also has extensive arable land that provides opportunities for agriculture. Canada is among the very few countries whose natural resource production exceeds their national consumption.[10]

Canada's rich resources have provided economic strength. While they have long been a central element of the Canadian economy, exploiting them is often at odds with national and global efforts to counter climate change. A natural resource-based economy and trade with the US has benefited Canada through the 20th Century, but increasingly, the country has an interest in diversifying.[11]

Population

---

[9] Canada - The World Factbook.

[10] *Ibid*.

[11] Alan Gelb, "Economic Diversification in Resource Rich Countries," 2010, 3; Sidney Weintraub, "Current State of U.S.-Canada Economic Relations," *American Review of Canadian Studies* 24, no. 4 (December 1, 1994), 484.

With large geography and a population of only 38 million, Canada ranks 39th globally and has one of the lowest population densities.[12] This ratio creates governance challenges and limits the human resources available to contribute to the nation's economic or military strength. Despite its small size, Canada's population has a unique character; a 2019 poll provided insights into Canadian's perspectives. The report outlined that the top election issues were climate change, the economy, and healthcare.[13]

On Canada's international role, the poll noted the most common opinions amongst Canadians demonstrated a preference for providing leadership on climate change and promoting peace and national interests. The latter view indicates a preference for a focus on domestic issues.[14] When broken down by province, these opinions varied across the country. For example, Western oil-rich provinces placed lower priority on climate change, and demonstrated lower support for international engagements.[15] Absent in the concerns raised by Canadians were the issues of defence and national security.

The Canadian view on defence and security is a defining population characteristic. Defence has not been a compelling election issue in Canada.[16] Canadians have neither rallied to calls for increased defence expenditures nor are there outcries when defence budget cuts are implemented. National Defence is the single largest discretionary budget item, but Canadians remain largely indifferent.[17]

---

[12] *Ibid*.
[13] Potloc, "Potloc - 2019 Election Poll," accessed February 2, 2021, https://business.potloc.com/hubfs/federal_election.pdf?hsCtaTracking=7c71b014-b272-49a7-bd61-30154595dee7%7Cfe3ba5b1-35b9-403b-aad8-95097ab9cc84, 4.
[14] *Ibid*, 46.
[15] *Ibid*, 12, 18, 19,20,23.
[16] Nossal, 17.
[17] *Ibid*, 17-18; Johnathan Cox, "Canadian Forces Transformations and Canada's Way of War in the Twenty-First Century" (Fort Leavenworth, KS, U.S. Army Command and General Staff College, 2019), 1, 23.

While they may have little concern for national security, the same cannot be said for education. The Organization for Economic Co-operation and Development rated the country as having the highest post-secondary education rate in the world. Its teenagers are also standouts amongst their peers, scoring sixth globally based on their reading, math and science abilities.[18] An educated population is a national strength and an important consideration in the global digital economy.

Despite these strengths, the size of the Canadian population limits its international influence. It moderates the human resources available to expand its economy, govern its landscape and build its military. The population, a key driver of national priorities within the Canadian democracy, has a decidedly domestic focus with limited security or defence concern.

Social Determinants

Economy

In 2019, Canada's Gross Domestic Product (GDP) was 1.7 Trillion dollars, placing it tenth in the world. Its economy is centered primarily on service, manufacturing and natural resources, with trade heavily weighted toward the US. In 2019, exports totalled 432.7 billion dollars with imports of 390.8 billion. In a distant second, the Nation's next most significant trading partner is the European Union. 2019 exports totaled 46.2 billion dollars and imports 63.5 billion.[19]

[18] Organization for Economic Co-operation and Development, "PISA 2018 Results," Publications-PISA, 2018, https://www.oecd.org/pisa/PISA-results_ENGLISH.png.

[19] Canada, "Canada's State of Trade 2019" (Ottawa: Global Affairs Canada, 2019), https://www.international.gc.ca/gac-amc/publications/economist-economiste/state_of_trade-commerce_international-2019.aspx?lang=eng, 64,66.

Canada's economy depends heavily on natural resources and trade with the US. In this position, the country's economy risks significant volatility. Changing commodity prices, shifts in the US or Canadian dollar, or any fluctuations in the Canadian US trade relationship, such as tariffs, could have a widespread impact. From enhancing stability to an interest in addressing climate change, Canada has numerous motivations to diversify its economy. With this interest and an educated population, it is little surprise that Canada has come to see a growing technology sector as vital to Canadian prosperity.[20]

Technology is an increasing element of the national economy. In 2019, the Information, Communications and Technology (ICT) sector employed over 650,000 across 43,000 companies. The industry has shown steady year-over-year growth, outpacing the rest of the Canadian economy. Between 2013 and 2019, ICT employment increased at an average annual rate of 3.1 percent, compared to 0.9 overall. With an estimated 2019 revenue of 210 billion, the ICT sector is a growing component of the broader Canadian economy.[21]

The Canadian economy continues to benefit from technology, and the Government is seeking to reinforce this trend. In 2019, The Department of Innovation, Science and Economic Development released an innovation and skills plan. Titled 'Building a Nation of Innovators,' the program presents an ambitious roadmap spanning skills development, infrastructure development and research investments. It aims to establish innovation hubs across the country to expand Canada's competitiveness in an increasingly connected, technology-centered global economy. The growing tech industry provides many opportunities, including a path to diversify Canada's

[20] Canada, *Building a Nation of Innovators - Innovation for a Better Canada* (Ottawa: Innovation, Science and Economic Development Canada, 2019), 4.

[21] Canada, "2019 Canadian ICT Sector Profile" (Ottawa: Innovation, Science and Economic Development Canada, 2019), 3,6,7.

resource and US trade-dependent economy.[22] A compelling motivator for the Nation's political class.

Political

A country's functioning depends on its political institutions and leaders—their ability to access and focus its foundational elements to advance national goals. Much like any Western democracy, successful governance is weighed through a routine election cycle. The process engrains the priorities of its population into its leaders' decision-making. Thus, successful Canadian politicians organize and apply the resources of the nation to further the priorities of its citizens. In Canada, this is currently a domestic focus on the economy, healthcare and climate change.

Through the 20th Century, Canada's leaders have produced an affluent nation. Aside from population size, the country rates in the top 10 worldwide in many comparisons. Despite the country's strong standing, it is dwarfed by the world's most powerful nations. The US economy and population are larger than Canada's by a factor of ten. China's GDP is over eight times larger and has 1 billion more citizens. Military comparisons are similarly lopsided. Where does this place Canada? The country is a self-declared middle-power. This ill-defined status continues to be debated in the academic community.[23] Whether or not the characterization is useful or accurate, the mindset has shaped Canada's foreign policy approach that has seen little change since the end of the Second World War.[24]

---

[22] Building a Nation of Innovators, 4.

[23] Adam Chapnick, "The Middle Power," *Canadian Foreign Policy Journal* 7, no. 2 (January 1, 1999): 73–82, https://doi.org/10.1080/11926422.1999.9673212., 76-78.

[24] Pierre Casgrain, "From Middle to Major Power: Correcting Course in Canadian Foreign Policy" (Ottawa, On: Macdonald-Laurier, 2020), 19.

Foundationally, Canada's approach to international affairs acknowledges the limitations of its national power. It recognizes that its interests could be easily overcome if countered by a more powerful state. It accepts that Canada may only unilaterally advance its interests in narrow circumstances. With this recognition, Canada has developed a multi-lateral approach and invested heavily in promoting an international rules-based order. The country participates in and helped shape organizations like the United Nations (UN) and the North Atlantic Treaty Organization (NATO).[25]

These institutions and similar multilateral agreements provide structural advantags to Canada. In addition to collective security arrangements, they offer a structured and predictable international environment. They provide a foundation that enables the country to advance its interests diplomatically. Where disagreements are encountered, dispute resolution frameworks moderate power imbalance. The rules and collective approaches prevent the 'might-is-right' scenario where larger nations automatically override Canada's interests. The importance of these organization to Canada is demonstrated in the mandate letters for the Ministers of National Defence and Foreign Affairs, where supporting and reinforcing these institutions is directed in both Ministers' first explicit tasks.[26]

A stable international rules-based order, a beneficial geography and collective security assurances have placed Canada in the enviable position of being able to focus its attention and resources domestically. The nation can afford to be episodically interested in security. The last significant example was the international response to 9/11. Responding in solidarity with its

---

[25] *Ibid*, 77; Justin Trudeau, "Minister of Foreign Affairs Mandate Letter" (Canada, December 13, 2019), https://pm.gc.ca/en/mandate-letters/2019/12/13/minister-foreign-affairs-mandate-letter; Canada, "Securing an Open Society : Canada's National Security Policy" (Ottawa, Ontario: Privy Council Office, 2004), http://publications.gc.ca/collections/Collection/CP22-77-2004E.pdf, 47; From Middle to Major Power, 4.

[26] Minister of Foreign Affairs Mandate Letter.

primary ally, this event stimulated an update to the country's approach to national security. In response, Canada created the department of Public Safety and the Canadian Border Services Agency (CBSA), centralizing elements of various departments and building atop others. The CBSA, Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Service were then grouped under the new Public Safety Department.[27]

The resulting Canadian structure distributed national security efforts across three primary departments: Global Affairs Canada (then Department of Foreign Affairs and International Trade), the Department of Defence and Public Safety. To coordinate these efforts, a new National Security Advisor was created within the Privy Council Office. The initiative was punctuated by Canada's first and only release of a National Security Strategy in 2004.[28]

The early 2000 organizational changes stopped short of identifying who was responsible for the national security portfolio. Instead, Canada leveraged a horizontal national security structure. This structure retained centralized control within government, with day-to-day functioning dependent on coordination amongst several departments, each with varying priorities and cultures. Public Safety was identified as the 'coordinating hub,' aside the National Security Advisor's role. Judicial inquiries in the following years highlighted governance challenges in this structure. However, recommendations such as empowering the National Security Advisor with decision-making authority were not implemented.[29]

Canada's approach to foreign affairs has a foundation in the stable international order provided by organizations such as the UN and NATO. They have provided additional security

[27] Wesley Wark, *A Case for Better Governance of Canadian National Security | Centre for International Governance Innovation* (Waterloo, On: Centre for International Governance Innovation, 2021), 1-2.
[28] *Ibid,* 1.
[29] *Ibid*.

assurances and enabled the country to moderate power imbalances with larger nations. These structures' collective security arrangements further enhanced the nation's security posture, which has provided Canada has significant discretion on when and how it becomes involved in matters of security and defence. These activities, however, compete for resources with its domestic priorities.[30]

Military

> Canada's location—separated from the rest of the world by three oceans … and the United States, a dominant and hegemonic power, as its southern neighbour—means that Canadians have the extraordinary luxury of being able to devote their wealth to things other than defence, so that whatever defence needs to be done … should be done on the cheap. [31]

In Canada, with a domestically focused population with a foundational assumption of an assured national security, the military is a topic that carries political risk. Military commitments and expenditures can easily be framed as wasteful, deadly, or unnecessary. With a population that is not concerned with defence, Canadian leaders must approach the subject cautiously or face electoral consequences. This environment has profoundly impacted the Canadian military, shaping everything from structure, capital procurement, and military operations.

The political risk inherent for Canada's leaders has driven a bipartisan interest in ensuring military accountability and the avoidance of an over-reliance on military advice. The perspective led to the creation of a Deputy Minister of National Defence, a co-equal peer of the Chief of Defence Staff (CDS), both reporting to the Minister of National Defence. The Deputy Minister is responsible for the Department of National Defence (DND), a civilian branch of National Defence, while the CDS is responsible for the Canadian Armed Forces (CAF). The

[30] Cox, 24-25.
[31] Nossal, 18.

Deputy Minister provides accountability to the government through their control of finance, procurement, and DND/CAF policy. The CDS, for their part, is responsible for organizing, training and employing military forces.[32]

The division of responsibilities between the Deputy Minister and Chief of Defence Staff requires coordination to ensure the efficient functioning of the department. As a simple example, the Chief of Defence Staff's responsibility to oversee training and operations relies on finance that the Deputy Minister controls. The co-leadership and interdependencies between the Department of National Defence and the Canadian Armed Forces can create a blurry separation between the roles of the CDS and Deputy Minister.

Proponents of this model argue that it provides accountability and ensures resources allocated to the military are used in accordance with government priorities.[33] Critics the structure argue it is inefficient, allows inappropriate civilian involvement in operational military matters, decreases effectiveness and creates internal ambiguity.[34] Despite these concerns, the structure endures, indicative of the government's preference to retain accountability on the politically risky subject of defence in Canada.

Despite the inherent political risk that military activities represent, it remains an important tool within Canada's foreign policy efforts. Canada's partnership with the US has a foundation in joint continental defence. The mutual relationship balances US assurances of protection with Canada's commitment to do everything within reason to ensure continental

---

[32] Philippe Lagassé, "Accountability for National Defence" (IRPP, March 2010), 32-34; Canada, "Accountabilities of the Minister, Deputy Minister and Chief of the Defence Staff - Canada.Ca," March 11, 2021, https://www.canada.ca/en/department-national-defence/corporate/reports-publications/transition-materials/defence-101/2020/03/defence-101/accountabilities.html.

[33] *Ibid.*

[34] *Ibid.*

security.[35] Given the disparity between the country's geographic size and population, Canada would be unable to fully secure its borders without US assistance. Its resources are insufficient to assure sovereign control across such a large geographical border. Partnership with the US provides Canada with a security level it could not otherwise afford.[36]

Nils Ørvik conceptualized Canada's approach to the military as one of "defence against help."[37] He asserted that Canada maintains a minimum level of defence to prevent unwanted assistance: situations where the US believes it must infringe on Canadian sovereignty to ensure its own security. An alternate perspective is that Canada's approach is a "defence against lockdown."[38] This perspective asserts that Canada's defence investments must be sufficient to prevent US security concerns about their shared border. Failure to achieve the minimum level of security risks border restrictions or "lockdowns," with significant economic ramifications. These perspectives differ on rationale, but they share the same foundational element: Canada's defence investments must be sufficient to assuage US concern.

Canada's relationship with the US is not the only one that requires military commitments. Its membership in organizations such as the United Nations and NATO presents another challenge of balance. The country benefits from the international rules-based order the institutions maintain, but the cost of these is military investment. For example, NATO recommends member nations spend two percent of national GDP on their militaries to ensure all are contributing to collective security. Within the UN, a similar metric does not exist. Still,

[35] Nossal, 14.
[36] *Ibid*, 13-14.
[37] Massie and Vucetic, 14.
[38] Massie and Vucetic, 37.

military commitments to UN missions and initiatives increase standing and gain the attention of the larger nations, providing political capital within the organization.

Thus, the Canadian Government's challenge is determining the military investment required to maintain defence heavy international commitments while also retaining public support. The Nation's answer is currently 1.29 percent of its GDP, a modest investment compared to the NATO average of 2.42. Similarly sized Australia commits to the NATO recommended level of 2.0 percent in its own defence budget.[39]

Canada's strategic culture and multilateral approach significantly impact how it views national security and defence. The country's relationships with important allies and institutions such as the US, "Five Eyes" security partnership, UN, and NATO rest on military commitment, but these obligations must be justified to a population with entrenched assumptions of security. The uniquely Canadian result sees military engagements commonly motivated by an interest in being seen to be involved, to be doing their part. The Government's military commitments typically aimed to maintain and advance relationships, having little to do with the specific military operation's objectives.[40] General Vance, a former CDS, described this approach concisely: contribution warfare.[41]

The implications of this approach are important to understand. Canada has levied a requirement on its military to support domestic emergencies, conduct continental defence with the US and support expeditionary operations with the UN, NATO, or other coalitions.[42] This

---

[39] Nossal, 17-18.

[40] Jonathan H. Vance, "Tactics without Strategy or Why the Canadian Forces Do Not Campaign," in *The Operational Art: Canadian Perspectives Context and Concepts* (Kingston, Ontario: Canadian Defence Academy Press, 2005), 280.

[41] *Ibid.*

[42] Canada, "Strong Secure Engaged" (Department of National Defence, 2017), 14.

range of possible commitments creates a demand for a significant array of military capabilities with a budget insufficient to acquire them.[43] This disparity could be reconciled if the Canadian government provided routine guidance and priorities to its military, however; unlike countries such as the US, Canada does not produce routinely produce national defence strategies.[44]

This tension places the CDS and the military's leaders in a position where prioritization is both essential and challenging. The organization does not have the resources to be simultaneously prepared to respond to the breath of possible demands levied by the government. They must forecast requirements and apply their limited resources in order to be prepared to meet anticipated need. They must carefully prioritize the right procurements, capability development and training.

Chapter Summary

Canada's national perspective was developed through the 20th Century. During this period, the country's beneficial geography and rich natural resources provided a foundation for a prosperous nation. It was shielded from conflict by distance and both collective security and defence measures. This environment has developed a national perspective with an entrenched assumption of security.

With little concern for security, Canada's political focus has been predominantly on domestic issues and on international policies which support the maintenance of international rules and norms. When required to advance its interests in the international forum, it has applied

[43] *Ibid;* Massie and Vucetic, 31.

[44] Lindsay Rodman, "You've Got It All Backwards: Canadas National Defence Strategy," in *Canadian Defence Policy in Theory and Practice*, Canada and International Affairs (New York, NY: Palgrave Macmillan, 2019), 273-274.

a middle-power doctrine, working through multi-lateral structures and organizations. Its prospects have been furthered by an international rules-based order.

Despite the country's relative safety, Canada requires basic military commitments to advance and protect its interests. It must commit sufficient resources to national and continental security as a "defence against help," or "lockdown." It must support NATO, and the UN to maintain good standing as an international partner through contributions to a stable international order. These commitments are discretionary; Canada may choose when and how much it contributes. With a public more concerned with the economy than security, these activities and investments represent a political risk.

In this environment, a horizontal approach to national security has emerged. It sees responsibilities divided across numerous federal departments and Public Safety assigned a coordination role. This approach has allowed the government to retain centralized control of the national security portfolio, calling on departments when needed to advance a specific issue. This complicated relationship provides little standing direction to the Canadian military. Instead, it asks the military to be prepared for a range of potential scenarios. It levies broad demands accompanied by limited resources.

CHAPTER 2: A MIDDLE POWER IN CYBERSPACE

Canada's perspectives and traditional approaches are facing new challenges in the digital domain of cyberspace. No longer are former assumptions as certain as they once were. This chapter will evaluate Canada's foundational elements and approaches to national security. It will illustrate the complicated threats now manifesting themselves through cyberspace. It will start by exploring new threats to Canada's national interests, followed by those faced by Canadians and Canadian organizations. It will discuss the nascent status of international cyberspace norms and their impact on Canada's ability to respond to these threats. Finally, it will highlight the cyberspace risks facing the Canadian military. The sum of these considerations will demonstrate that Canada is in a period of liability, encountering new risks while its traditional tools of influence have been diminished.

Canada's leaders see opportunity in cyberspace. The country's policy and strategy documents state goals such as building a globally competitive nation based on a culture of innovation and positioning it as a world leader in cybersecurity.[45] Its strategies and policy documents present the environment with optimism, stating that: "[i]nnovation is the key to competitiveness, productivity, economic growth, creating good jobs, and overall making life better for all Canadians."[46] For their part, Canadians are also embracing technology. The country is highly connected with a technology sector that is the most rapidly growing element within the economy. The Government is attempting to support this momentum with an innovation plan to increase Canada's global competitiveness; but Canada is not unopposed in realizing these

[45] Building a Nation of Innovators, 3.
[46] *Ibid*, iii.

ambitions.[47] The more time and resources it commits in cyberspace, the more connected it becomes, the greater the interest created for a host of Malicious Cyber Actors (MCA).

Malicious Cyber Actors

MCA are a broad grouping reflecting a range of individuals and organizations. They are often fluid and challenging to distinguish. An individual could be conducting fraud to fund terrorism; a criminal organization today could be a contracted government proxy tomorrow, and all MCA strong motivations to mask their actions and identities to avoid repercussions. Despite these definitional challenges, categorization helps conceptualize the range of threats, motivations, and the type of necessary response. To this end, MCA can be grouped broadly into four categories: [48] Criminals, Terrorists, Hacktivists and State Actors.[49] Each of these groups has different personalities and motivations ranging from financial to ideological and geopolitical.[50]

The most significant threats to Canada are criminals and state actors.[51] These groups continue to target Canada and Canadians and produce new risks to Canadian national security.[52] Canada's 2020 Cyber Threat Assessment states that financially motivated threat actors represent

---

[47] *Ibid*.

[48] Insider threats and thrill seekers are other categories of malicious cyber actors not independently presented in this paper.

[49] Canadian Centre for Cyber Security, *An Introduction to the Cyber Threat Environment.* (Ottawa, 2018): 2,3,6; Chris Bronk and Gregory S. Anderson, "Encounter Battle: Engaging ISIL in Cyberspace," *The Cyber Defense Review,* (2017)*:* 93, 97, 100.

[50] Canada, "CSIS Public Report 2019" (Ottawa: Canadian Security and Intelligence Service, 2019), 18; Globe and Mail, "Anonymous' Claims Responsability for Cyber Attack that shut down Government Websites," accessed 9 November 2020, https://globalnews.ca/news/2060036/government-of-canada-servers-suffer-cyber-attack/; CTV News, "Anonymous Claims Attack on RCMP Websites in Response to Police Shooting," accessed 9 November 2020, https://www.ctvnews.ca/canada/anonymous-claims-attack-on-rcmp-websites-in-response-to-police-shooting-1.2476710; Scott Hilts, " A Persepective on Cyber Security form the Canadian Nuclear Private Sector," *Governing Cyber Security in Canada, Australia and the United States,* (2018): 20.

[51] National Cyber Threat Assessment 2020, 5, 10, 11, 20.

[52] *Ibid*, 5, 10, 11.

Canadians' most significant threat while state activity from China, Russia, Iran, and North Korea pose the Nation's most significant strategic threat.[53]

> "[Canada's enemies] are not just trying to steal our personal and financial information, but also attempting to sabotage our critical infrastructure – the cyber and physical systems, networks and assets we rely on every day, in all aspects of our lives."[54]

The Canadian National Interest

While cyber threats and crime have been persistent problems, the ability to undermine democratic institutions is a relatively new phenomenon. A prominent example was the US Presidential election in 2016. In the run-up to the vote, Iran and Russia conducted sophisticated campaigns to influence public opinion. Leveraging the same tactics used to focus advertising, they developed tailored messaging targeted at specific audiences. They deliberately sought to inflame tensions and sway voting in favour of the Trump Campaign. Russia supplemented their online information campaigns with targeted compromises of numerous Democratic Party leaders and offices. Subsequently, they released hundreds of thousands of documents, calculating the timing to maximize impact on Secretary Clinton's electoral prospects.[55]

Large scale influence campaigns on social media have become the 'new-normal.'[56] These activities are not limited to elections and can have a decisive impact in the sphere of international and geopolitical competition. Recent Russian attempts to create destabilizing effects by inflaming US race tensions are another example.[57]

---

[53] *Ibid*, 5, 10, 11, 20.
[54] CSIS Public Report 2019, 2.
[55] Robert S. Mueller, "Report on the Investigation Into Russian Interference In the 2016 Presidential Election" (Washington, D.C.: U.S. DOJ Special Counsel, April 2019).
[56] National Cyber Threat Assessment 2020, 13.
[57] Julian E. Barnes and Adam Goldman, "Russia Trying to Stoke U.S. Racial Tensions Before Election, Officials Say - The New York Times," March 10, 2020, https://www.nytimes.com/2020/03/10/us/politics/russian-interference-race.html.

The intermingled North American media environment exposes Canadians to influence campaigns focused on the US, but Canada is not merely a victim of just collateral effects.[58] Both Iranian and Russian actors have targeted Canada. They have sought to inflame Canadian divisions on various issues including climate change, terrorism, pipelines, and immigration policy. Many of these activities aimed to shape national dialogue after events such as the 2017 Quebec Mosque shooting or the 2019 approval of the trans-mountain pipeline.[59] These activities are described as "increasing," their goal to advance foreign economic and national security interests while undermining the same within Canada.[60]

Attempts to shape public opinion are not the only means that states are using to target Canada. State-sponsored actors are conducting espionage against Canadian organizations and probing Canadian critical infrastructure.[61] The Canadian Center for Cyber Security assessed that it was 'very likely,' an assessment of higher than eighty percent certainty, that state actors are developing the capability to disrupt Canadian critical infrastructure, including power.[62] While these abilities can cause significant damage and loss of life, they are unlikely to be employed outside a significant international conflict. The Cyber Center assesses that these actions are more likely to be used as an intimidation tactic.[63]

---

[58] National Cyber Threat Assessment 2020, 2, 5, 13.

[59] *Ibid*, 14, 19; Catharine Tunney, "Foreign Enemies 'increasingly Targeting Canada,' Privy Council Warns New Minister | CBC News," *CBC*, February 2, 2020, https://www.cbc.ca/news/politics/foreign-interference-increasingly-targeting-canada-leblanc-warned-1.5446134. Ross Fetterly, "The World Has Changed. Canada's Defence Strategy Hasn't Changed with It" (Macdonald-Laurier Institute, October 8, 2019.

[60] *Ibid*.

[61] National Cyber Threat Assessment 2020, 2. Angela Gendron, "Cyber Threats and Multiplier Effects: Canada at Risk," *Canadian Foreign Policy Journal* 19, no. 2 (June 1, 2013), 182-183; Martin Rudner, "Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge," *International Journal of Intelligence and CounterIntelligence* 26, no. 3 (September 1, 2013):464.

[62] *Ibid*, 5, 9, 21.

[63] National Cyber Threat Assessment 2020, 5, 9, 21.

Canadian Population and Economy

Canada's 2018 Cyber Security Strategy highlighted that "digital technologies are essential to our [Canada's] way of life".[64] Canada's high connectivity rates attest to this fact; its citizens are amongst the most pervasively connected populations on the planet. In 2018, 94 percent of Canadian households had internet service, and over 31 million had a mobile phone subscription. Over 50 percent of Canadians had internet-connected smart home devices, such as thermostats, lights and cameras. With this level of technological adoption, it should be little surprise that Canadians are also heavy internet users. Its population averages 43.5 hours a month online, the highest globally.[65]

The population is also increasing its use of social media, streaming services and online shopping. With an average per capita GDP of just over $46,000 (USD), Canadian's are comparably wealthy.[66] Their online shopping totals over 57 billion dollars of goods online, and they provide over 4.2 billion in annual revenue to streaming services.[67] Given their wealth and connectivity, it follows that the most common threats to Canadians and businesses are fraud and crime.[68] In 2018, individual Canadians reported losing over 43 million dollars to such activity. [69] The actual total is likely much higher.

Canadian businesses, and by extension, the Canadian economy, also face threats in cyberspace. In 2018, the head of the Canadian Security and Intelligence Service remarked that

---

[64] Canada, *National Cyber Security Strategy*, (Ottawa: 2018): 2.
[65] *Ibid*, II; Gendron, 178.
[66] Statistics are based on 2019 data; "World GDP per Capita Ranking 2020 - StatisticsTimes.Com," accessed February 15, 2021, http://statisticstimes.com/economy/projected-world-gdp-capita-ranking.php.
[67] Statistics Canada, "Canadian Internet Use Survey," accessed February 2, 2021, https://www150.statcan.gc.ca/n1/daily-quotidien/191029/dq191029a-eng.htm, 1.
[68] National Cyber Threat Assessment 2020, 14.
[69] *Ibid*, 16.

state-sponsored commercial espionage represents the most significant threat to the Canadian economy. More than a threat, he noted that countries such as Russia and China have already caused considerable harm, undermining Canada's future economic growth.[70]

> Economic espionage activities in Canada continue to increase in breadth, depth and potential economic impact. Hostile foreign intelligence services or people who are working with the tacit or explicit support of foreign states attempt to gather political, economic, commercial, academic, scientific or military information through clandestine means in Canada.[71]

State-Sponsored Actors and cybercriminals steal intellectual property and proprietary information from Canadian companies.[72] They also seek direct financial gain, employing ransomware and other extortion and fraud schemes. These acts cause significant damage, imposing recovery costs in addition to secondary effects such a reputational damage. The cumulative impact undermines the competitiveness of targeted companies. [73]

Tools of Influence

Cyberspace Norms

Aggravating these threats to Canada is the uncertain international environment. Canada's traditional 'middle power' approach relies on a stable rules-based order where it can work multi-laterally to create collective efforts to achieve its national aims. This environment is built upon norms and laws collectively adhered to by all states. These states, in turn, moderate the activity such as crime within their borders.

---

[70] Catharine Tunney, "CSIS Chief Calls Commercial Espionage 'the Greatest Threat to Our Prosperity' | CBC News," accessed February 15, 2021, https://www.cbc.ca/news/politics/david-vigneault-csis-economy-1.4932407.

[71] CSIS Public Report 2019, 16.

[72] National Cyber Threat Assessment 2020, 5.

[73] *Ibid*, 5,20, 22.

Norms are an accepted set of principles, collective expectations that establish what represents acceptable behaviour within a specific community.[74] International rules and norms can be leveraged to justify or condemn actions, constrain undesired behaviours, and apply punitive measures against violators.[75] They set the expectations for responsible state behaviour and form the structure for a stable international order.

In 2010, recognizing the deteriorating trends in cyberspace, the UN Group of Governmental Experts (UNGGE) was established. Their goal was to counter the growing threats of transnational crime and destabilizing state action in cyberspace. The group aimed to develop a set of norms to establish an international baseline.[76]

Implementation of norms relies on group consensus amongst the given community and takes time to evolve. For example, the norms relating to the conduct of war have been debated and refined for centuries.[77] In cyberspace, the establishment of norms is challenged by differing values, the number of actors involved, and definitional challenges.

In order for cyberspace norms to be effective, they would require broad acceptance between Canada, its allies, and "non-like-minded" nations such as China and Russia.[78] Unfortunately, this effort has stalled at the starting line. The discussion of norms has been stymied by questions as foundational as to how the internet should be governed.

---

[74] T. Erskine and M. Carr, "Beyond Quasi-Norms: The Challenges and Potential of Engaging with Norms in Cyberspace," 2016, 87, 90.
[75] *Ibid,* 89, 93.
[76] Roger Hurwitz, "The Play of States: Norms and Security in Cyberspace," *American Foreign Policy Interests* 36, no. 5 (September 3, 2014): 322, 326.
[77] Erskine and Carr, 95.
[78] Hurwitz, 328.

Countries like Russia and China, which view the internet from a domestic and national security perspective, are pushing for a state-centric model. Their vision is an internet where the state maintains powerful tools of censorship, surveillance and control.[79] Canada and its allies, by comparison, are advocating for the maintenance of the existing open multi-stakeholder partnership that includes academia, industry, civil society groups and governments.[80]

While the argument over governance continues to impact progress on norms, there remain other extensive challenges should even this initial conundrum be resolved. The sheer number of stakeholders involved in cyberspace adds to the amount of perspectives that must be balanced. Whether it is differing perspectives of China vs Canada, or commercial interests of private industry, a large and diverse community increases the challenge of securing consensus within it.[81]

A further challenge is the nuance of definitions. For example, what is the line between espionage and intellectual property theft? In the international forum, espionage is accepted as the legitimate business of states; however, when they enrich their domestic industries by stealing information from other nations, should a line be drawn?[82] The challenge of these types of distinctions further illustrates the complexity of establishing consensus.

---

[79] Ron Deibert, "Canada and the Challenges of Cyberspace Governance and Security," *The School of Public Policy* 5, no. 3 (March 2013), 2.

[80] National Cyber Threat Assessment 2020, 13.

[81] Roger Hurwitz, "The Play of States: Norms and Security in Cyberspace," *American Foreign Policy Interests* 36, no. 5 (September 3, 2014): 323; T. Erskine and M. Carr, "Beyond Quasi-Norms: The Challenges and Potential of Engaging with Norms in Cyberspace," 2016, 96, 97.

[82] Roger Hurwitz, "The Play of States: Norms and Security in Cyberspace," *American Foreign Policy Interests* 36, no. 5 (September 3, 2014): 328.

Beyond consensus, the environment itself is a complicating factor. Even if international consensus on norms could be established, the nature of cyberspace itself would continue to complicate the regulation of online behaviour. The difficulty of definitively attributing online identity permits plausible deniability.[83] In an environment of universally accepted norms, an entity or state could still deny responsibility for any violation of online norms. Some argue that such a dynamic environment does not lend itself to establishing norms at all.[84]

Despite the ongoing challenges, the UNGGE has developed a proposed set of norms.[85] They include:

- "states should not knowingly allow their territory to be used for internationally wrongful acts using ICT;" [86]
- "states should not conduct or knowingly support ICT activity that intentionally damages critical infrastructure;"[87]
- "states should take steps to ensure supply chain security, and should seek to prevent the proliferation of malicious ICT and the use of harmful hidden functions;"[88]
- "states should not conduct or knowingly support activity to harm the information systems of another state's emergency response teams and should not use their own teams for malicious international activity;" [89]

---

[83] T. Erskine and M. Carr, "Beyond Quasi-Norms: The Challenges and Potential of Engaging with Norms in Cyberspace," 2016, 98; Angela Gendron, 179.

[84] Roger Hurwitz, "The Play of States: Norms and Security in Cyberspace," *American Foreign Policy Interests* 36, no. 5 (September 3, 2014): 322.

[85] CCDCOE, "2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law," accessed April 2, 2021, https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/.

[86] *Ibid*.

[87] I*bid*.

[88] *Ibid*.

[89] *Ibid*.

- "states should respect the UN resolutions that are linked to human rights on the internet and to the right to privacy in the digital age." [90]

Unless these norms are endorsed by countries like China, Russia, Iran and North Korea, they will have little impact. Canada's adoption of such norms is a largely symbolic gesture that does not improve its resilience to cyber threats. Given the foundational debate still occurring and the complexity of the environment, cyberspace norms are likely to remain elusive for the foreseeable future. [91]

In the interim, a digital arms race is ongoing.[92] Fueled by a lack of international structure and a growing economy of cyber skills and tools available for purchase, states and criminal organizations are conducting increasingly sophisticated cyber campaigns.[93] This security environment is a departure for Canada. In the past, the nation's relative safety has traditionally permitted it to take time and delay when making difficult and politically sensitive security decisions.[94] From behind the protection of geographic boundaries, and a Western consensus on the rules-based international order and collective security assurances, Canada had considerable discretion on the scale of its investments in national security. In the current environment, distant threats are able to penetrate its formally secure geography.

Cyberspace bypasses geographic barriers, and multilateral approaches to foreign affairs lack a foundation of stable laws and norms regulating these types of threats. Without this foundation, there is no rallying point for collective action. Furthermore, in cyberspace, Canada

---

[90] *Ibid*.

[91] Roger Hurwitz, "The Play of States: Norms and Security in Cyberspace," *American Foreign Policy Interests* 36, no. 5 (September 3, 2014): 323, 328.

[92] Ron Deibert, "Canada and the Challenges of Cyberspace Governance and Security," *The School of Public Policy* 5, no. 3 (March 2013), 3.

[93] BlackBerry, "2021 Threat Report," 2021, 8.

[94] Email to author, Government of Canada Cyber Community Official, 28 February, 2021, 2.

has limited influence to deter and respond to globally based cyber threats. It must work through international organizations, alliances and other privileged partnerships such as the “Five Eyes”. It must work through bureaucratic processes, often in an adversarial environment. These actions take time and have limited prospects for success. [95] MCA in countries such as Iran, Russia and China are unlikely to face consequences.[96] High levels of connectivity, wealth, leading-edge research, and international networks afforded by alliance relationships, together with the low probability of consequences from targeting its assets and infrastructure, make Canada a high-reward, low-risk target for MCA. The result is predictable: in 2017, Canada had the third most data breaches and ranked fourth for the number of stolen identities.[97]

> "These threats continue to persist and, in some areas, are increasing. Canada's advanced and competitive economy, as well as its close economic and strategic partnership with the United States, makes it an ongoing target of hostile foreign state activities. Canada's status as a founding member of the North Atlantic Treaty Organization (NATO) and its participation in a number of multilateral and bilateral defence and trade agreements has made it an attractive target for espionage and foreign interference."[98]

The Canadian Military

For decades, technological superiority has propelled Western nations to top rungs of global military might. The ability to rapidly sense, analyze and distribute battlefield information to focus the application of dispersed combat elements has provided a marked advantage. Technologies such as stealth, precision-guided missiles and surveillance capabilities have proven decisive in many conflicts. Through these advances, military platforms are quickly becoming

---

[95] National Cyber Threat Assessment 2020, 13; Brent J. Arnold and Stephanie MacLellan, “Cyber Security in Canada:,” Governing Cyber Security in Canada, Australia and the United States (Centre for International Governance Innovation, 2018), JSTOR, http://www.jstor.org/stable/resrep17311.6, 7.

[96] *Ibid*; Strong Secure Engaged, 56.

[97] Symantec, “Internet Security Threat Report,” 2017, 50.

[98] CSIS Public Report 2019, 16.

networks unto themselves. While this integration provides an advantage, it also presents a risk.[99] The 21st Century poses a host of new challenges for the CAF. To be ready to respond to the Government's call, the CAF must prepare for operations in a drastically different environment. One where the communications systems and weapons platforms face threats in cyberspace.[100]

While the details are redacted, a 2021 US Defense Department Audit illustrates critical cyber vulnerabilities were found on the B-2 Stealth bomber and a guided missile.[101] These findings were not uncommon. In audits of US military projects between 2012 and 2017, nearly all were vulnerable to "relatively simple tools and techniques," which allowed testers to assume control or degrade the system's functioning. [102] Perhaps most concerning, the report concludes that the US Defence Department does not know the full scale of these types of vulnerabilities.[103] These challenges are not exclusive to the US, the author has been involved in Canadian weapons system assessments that provide similar conclusions. Canada's defence policy acknowledges these same concerns, stating that "[adversaries] are rapidly developing cyber means to exploit the vulnerabilities inherent in the C4ISR systems . . . as well as other operational technologies, such as weapons systems."[104]

The impact of the digital age on military operations extends beyond threats to weapons systems and networks. Given the Canadian military's reliance on technology, cyberspace provides the ability to rapidly deliver devastating effects at little cost over great distance.

---

[99] Strong Secure Engaged, 56; Canada, "Joint Doctrine Note Cyber Operations" (Department of National Defence, 2017). 3-13, 3-14.

[100] Joint Doctrine Note Cyber Operations, iii.

[101] United States, "Audit of Cybersecurity Requirements for Weapon Systems in the Operations and Support Phase of the Department of Defense Acquisition Life Cycle," Audit (Washington, D.C.: Department of Defense, February 10, 2021), 10-12.

[102] United States, "Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities," Audit (Washington, D.C.: Government Accountability Office, October 2018), 20-21.

[103] *Ibid*.

[104] Strong Secure Engaged, 56.

Examples could include the destruction or corruption of information, manipulation of navigations systems or attacks on industrial control systems. The range, speed, scope and scale of attacks possible in cyberspace have the potential to shift how conflicts and wars are conducted.[105] In response, an increasing number of nations are developing military cyber capabilities. Adding to the effect of these discrete actions, cyber capabilities are being integrated within broader whole-of-government campaigns to advance geopolitical goals.[106] While cyberspace has already begun to shape military operations, the full extent of its influence is not yet known.

Chapter Summary

Whether it is for financial gain, to advance an ideology or further a political objective, cyberspace offers a growing cadre of malicious actors' opportunity. It provides a means to overcome traditional barriers and directly target Canada, its citizens and businesses. The most common threat are cybercriminals; the most significant strategic threat comes from nation-states. Cyberspace provides these actors with the ability to conduct fraud, extortion, and steal corporate secrets; it provides the ability to influence public opinion, intimidate, and undermine democratic institutions. The country's high connectivity rates, advanced economy, and limited ability to respond internationally produce a high-reward and low-risk environment, which emboldens a range of MCA.

The sense of security Canada developed in the 20th Century is increasingly inconsistent with the current environment. The old assurances of geography and collective security are not as certain in the digital age. Without international norms, Canada's traditional multilateral approach

[105] Joint Doctrine Note Cyber Operations, 3-13, 3-14.
[106] *Ibid,* 4-1.

to foreign affairs is diminished, collective action halted by lack of consensus. The resulting environment places Canada in a period of liability.

CHAPTER 3: CANADIAN APPROACH TO CYBERSPACE

With a vested interest in realizing the economic opportunities in cyberspace and protecting the nation from new threats, Canada has implemented new strategies and policies, developed new organizations, and created new law. This chapter will review these elements to establish an understanding of the Canadian government cyberspace program. It will provide insights into the structure and governance of the approach. Through this process, echoes of Canada's 20th Century approaches will emerge. The country's efforts emphasize enhancing cyber security, establishing and supporting international rules-based order, while placing little emphasis on national security.

Canada's initial approach to cyberspace was formalized with the release of the 2010 National Cyber Security Strategy. This document and accompanying action plan were followed by additional strategies, policies and legislation. These publications have shifted the Canadian government cyber landscape over the past ten years, creating a host of initiatives and changes in organizational structure. Chronologically, the key documents and organizational changes include the:

- 2010 National Cyber Security Strategy;
- 2011 Creation of Shared Services Canada;
- 2017 National Defence Policy;
- 2018 National Cyber Security Strategy;
- 2018 Creation of the Canadian Centre for Cyber Security; and
- 2019 Canadian Security Establishment Act.

The review illustrates an effort spanning numerous activities. While Canadian policy continues to evolve, the current approach relies heavily on collaboration and consensus. This approach, combined with unclear boundaries of responsibility, creates the potential for conflict, competition and inefficiency.

National Cyber Security Strategy 2010

In 2010, Canada released its first Cyber Strategy, stating that "Canada … will strengthen our cyber systems and critical infrastructure sectors, support economic growth and protect Canadians as they connect to each other and the world."[107] The document highlighted the importance of cyberspace to the nation and outlined the growing risks to financial security and the national interest.[108] The strategy directed increased capabilities to "detect, deter and defend against cyber incidents."[109] To advance these priorities, it established three foundational pillars:

- Securing Government Systems;
- Partnering to secure vital cyber systems outside the federal government; and
- Helping Canadians be more secure online.[110]

Common themes in the document included increasing domestic cyber awareness and combatting cyber-crime.[111] The strategy launched notable organizational changes such as establishing Shared Services Canada and implementing initial cyber structures within the

[107] Canada, *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada.* (Ottawa, 2010), 12-15; for the purposes of this paper, references to Canada's cyber strategies will imply both the core document and associated action plan.

[108] Canadian Cyber Strategy 2010, 2-5.

[109] Canada and Public Safety Canada, *Action Plan 2010-2015 for Canada's Cyber Security Strategy.* (Ottawa: Government of Canada, 2013), 9.

[110] Canadian Cyber Strategy 2010, 7.

[111] Canadian Cyber Strategy 2010, 1, 7, 11-12.

Canadian military: the Director General Cyber and a Cyber Task Force.[112] The strategy also outlined roles and responsibilities for key federal institutions:

- Public Safety:
    - Act as the central coordinating body, promote comprehensive approaches;
    - Oversee the development and implementation of the Canadian Cyber Strategy;
    - Coordinate the assessment of complex threats;
    - Through the Cyber Incident Response Centre, continue to act as the focal point for monitoring, providing advice and directing the national response to cyber security incidents; and
    - Lead public awareness and outreach efforts to inform Canadians about cyber threats.[113]
- Communications Security Establishment:
    - Detect cyber threats;
    - Provide foreign intelligence and cyber security services; and
    - Respond to threats and attacks against government networks and information systems.[114]
- Treasury Board:
    - Improve incident management the development of policy and standards; and
    - Act as the overall responsible department of information technology security.[115]
- Royal Canadian Mounted Police:

[112] Action Plan 2010-2015 for Canada's Cyber Security Strategy, 6.
[113] Canadian Cyber Strategy 2010, 9.
[114] *Ibid*, 10.
[115] *Ibid.*

    - Continue mandate of criminal investigations to include those involving government systems and critical infrastructure; and
    - Expand focus on cyber-crime, including establishing additional organizational structures and partnerships with other nations and international organizations. [116]
- Global Affairs Canada:
    - Provide advice on the international dimension of cyber security; and
    - Work to develop an international cyber strategy. [117]
- Canadian Armed Forces:
    - Strengthen ability to defend CAF networks;
    - Work with other government departments to identify threats and response options and exchange best practices with military allies;
    - Provide intelligence assessments and analysis on cyber threats to DND/CAF and military cyber threats to the Government of Canada; and
    - Work to develop policy and legal structures and frameworks for military aspects of cyber complimenting Global Affairs Canada efforts.[118]

Despite the rapidly evolving cyber-environment, characterized by expanding cybercrime and the absence of international structure and norms, as noted previously; the 2010 Strategy demonstrated a continuation of traditional Canadian strategic approaches. It focused on enhancing cyber security by extending the international rules-based order into cyberspace.[119] It

[116] *Ibid*.
[117] *Ibid.*
[118] *Ibid.*
[119] Canadian Cyber Strategy 2010, 8, 9; Action Plan 2010-2015 for Canada's Cyber Security Strategy, 2, 10;

also established a horizontal governance model, similar to that for National Security discussed earlier.

The 2010 strategy is notable as the only consolidated list of cyber-security roles and responsibilities among federal departments.[120] To understand the governance of the federal system, you must start with the 2010 strategy and build on this baseline as the program is amended in later documents. The strategy provided direction and priorities, outlined roles and responsibilities and established basic governance. It emphasized security threats to Canadians and Canadian businesses and the growing risks to critical infrastructure. To advance these efforts, it also outlined expanded coordination with the private sector, academia and other levels of government.[121]

Shared Services Canada

Following the announcement in 2010 Strategy, Shared Services Canada was created by a series of orders-in-council the following year. The initiative centralized government IT services to achieve efficiencies and realize cost savings.[122]

The Shared Services Canada Act mandated the centralization of email, data center and network support from 43 government departments into the newly formed organization. Exclusions included classified systems along with any information technology infrastructure operated by the Department of National Defence, Royal Canadian Mounted Police or the Canadian Border Services Agency that:

---

[120] *Ibid.*

[121] Canadian Cyber Strategy 2010, 7,8.

[122] Canada, "Shared Services Canada History and Legislative Responsibilities - Canada.Ca," accessed March 16, 2021, https://www.canada.ca/en/shared-services/corporate/transparency/briefing-documents/ministerial-briefing-book/shared-services-canada-history-legislative-responsibilities.html; Email to author, Colonel David Yarker, 21 February, 2021, 1.

- are used for the operation of military platforms including ships, aircraft or vehicles;
- are transportable; or
- are used to counter threats to national defence, national security and public safety.[123]

The creation Shared Services Canada transferred the majority of federal departments' network support and accompanying workforces to it. In 2013 this mandate was expanded to include responsibility for the procurement and provision of end-user devices and software.[124]

Strong, Secure, Engaged: Canada's Defence Policy

The next notable advancement in the Canadian government cyber program came in 2017 with the release of Strong, Secure, Engaged (SSE), an updated defence policy. The document was built on three pillars: "Strong at home", "Secure in North America", and "Engaged in the World".[125] These pillars represent Canada's long-standing military priorities.

SSE included a notable emphasis on cyberspace. It outlined how cyberspace provides both opportunities and risk, asserting that advanced technologies are central to successful military operations. It also highlighted that vulnerabilities introduced by technology are now being successfully exploited, the nation's adversaries are increasingly capable of using cyberspace to target military platforms such as ships and aircraft.[126]

Recognizing the risks and opportunities, the defence policy introduced numerous cyber-related initiatives, including supply chain security and procurement activities and an increase in intelligence capabilities. The policy also outlined plans to increase the number of military

[123] Canada, "Orders In Council 2012-0958," 2012–0958 § (2012), 1.
[124] *Ibid*.
[125] Strong Secure Engaged, 14.
[126] *Ibid*, 70.

personnel dedicated to cyber functions. Along with capability investments, the policy outlines several specific cyber tasks for the CAF:

- Protect CAF networks and weapons systems from cyber effects;[127]
- Develop and employ offensive cyber capabilities against adversaries in support of government-authorized military actions;[128]
- "Ensure threats in the cyber domain do not threaten Canadian Defence and Security Objectives and strategic interests including the economy"; and [129]
- Be prepared to support response to cyber-attacks on domestic critical infrastructure.[130]

Evaluating these tasks against those assigned in the 2010 Cyber Strategy demonstrates the evolution of CAFs original responsibilities. It adds the tasks of defending weapons systems and responding to threats to the national interest.

National Cyber Security Strategy 2018

Following the 2017 defence policy, Canada released its second cyber strategy in 2018. Development had begun two years earlier with a re-evaluation of the 2010 document.[131] Prior public consultation culminated with a 2017 report highlighting a range of governance challenges. Amongst these recommendations was a requirement to clarify roles amongst multiple departments claiming to be the single point of contact for the private sector.[132] The central emphasis of the 2018 Strategy is one of establishing improved coordination. A signature element of the policy, the Canadian Centre for Cyber Security, aimed to provide a central focal point for

[127] *Ibid*.
[128] *Ibid*.
[129] *Ibid*, 60.
[130] *Ibid*, 81.
[131] *Ibid,* 8; Horizontal Evaluation of Canada's Cyber Security Strategy.
[132] Horizontal Evaluation of Canada's Cyber Security Strategy, 7.

other levels of government, academia, businesses and the Canadian public.[133] The primary themes drawn from public consultation are:

- the government of Canada must expand efforts to counter cybercrime;
- there is a wide-ranging need for improved cyber knowledge and skills across Canada and within the government, and;
- there is a demand for strong federal leadership in the cyber security arena.[134]

The strategy highlights the Government and Canadian's requirement to work together to protect against crime and defend critical systems. It also illustrates the dramatically increasing threats that the country .[135]

The 2018 Strategy expands on the 2010 pillars reframing them in a structure that illustrates Canada's cyber program as a product of collaboration. Instead of an "us" and "them" approach in the 2010 focus of: securing government systems, partnership outside government and helping Canadians be more secure.[136] The 2018 approach outlines a more comprehensive approach, establishing three goals:

- "Secure and Resilient Canadian Systems";[137]
- "An Innovative and Adaptive Cyber Ecosystem"; and[138]
- "Effective Leaderships and Collaboration".[139]

---

[133] Canadian Budget 2018, 203-204; Canada, Canadian Cyber Strategy 2018, III.
[134] Canadian Cyber Strategy 2018, 10-11.
[135] *Ibid*, 9.
[136] *Ibid*, 6.
[137] *Ibid, 9.*
[138] *Ibid.*
[139] *Ibid.*

On national security, the strategy did not include any notable changes beyond acknowledging the growing threats to the Nation's interests.[140] It highlights the ongoing efforts of Global Affairs Canada to establish an international cyber strategy as one of the ways Canada will deter and respond to transnational threats.[141] In the absence of a change in the 2018 strategy, the horizontal federal governance structure established in 2010 remains.

Canadian Center for Cyber Security

The creation of the Canadian Centre for Cyber Security was announced in early 2018.[142] In a similar approach to that of Shared Services Canada, the Cyber Centre was created by centralizing employees and functions from various departments into a single entity. The reorganization included the consolidation of Public Safety's Cyber Incident Response Center, elements of Shared Services Canada's Security Operations Center and the Communications Security Establishment's Information Technology Security Section.[143] The 2018 budget emphasized both the 'focal point' it would provide to Canadians and the collaboration it would enable between different levels of Canadian governments.[144]

The Canadian Center for Cyber Security is mandated to:

- Serve as a focal point for cyber security within the federal government, providing unified advice to Canadians, Canadian businesses and partners;[145]

[140] Canadian Cyber Strategy 2018, 13, 14, 18.
[141] *Ibid*.
[142] Canada, "Budget 2018: Equality and Growth" (2018), 203.
[143] Canada, "Backgrounder: Canadian Centre for Cyber Security | Communications Security Establishment," accessed March 16, 2021, https://cse-cst.gc.ca/en/backgrounder-fiche-information.
[144] Canadian Budget 2018, 203-204.
[145] Canadian Cyber Strategy 2018, 28.

- Provide strategic cyber threat assessment and contextualize cyber threats to enhance the Government of Canada and Canadian's understanding of cyber events;[146]
- Partner with owners and operators of critical infrastructure to enhance security against advanced cyber threats;[147]
- Provide cyber security expertise in support of government departments in the delivery of their core functions, including collaborating with the RCMP's effort to counter cybercrime;[148]
- Inform, communicate and educate Canadian's and Canadian businesses on cyber security issues;[149]
- Defend Government of Canada systems, and respond to significant cyber security threats and incidents to reduce and mitigate harm to the federal government; and[150]
- Share cyber security advice and guidance as well as technical capabilities.[151]

Compared to the roles outlined in the 2010 Cyber strategy, these tasks represent the transfer of all of Public Safety's previous responsibilities, less those coordinating functions and overseeing the development and implementation of the cyber strategy.

Communications Security Establishment Act 2019

Following the establishment of the Canadian Centre for Cyber Security and the Defense Department's 2017 Policy, the Communications Security Establishment (CSE) Act was created,

---

[146] Canadian Budget 2018, 6.
[147] *Ibid*.
[148] National Cyber Security Action Plan 2019-2024, 17.
[149] Canada, "About Us: Canadian Centre for Cyber Security," accessed March 17, 2021, https://cyber.gc.ca/en/about-cyber-centre.
[150] Canadian Centre for Cyber Security Backgrounder.
[151] *Ibid*.

establishing new responsibilities and authorities for the organization. The document outlined CSE's primary responsibilities for monitoring foreign signals intelligence and acting as the technical authority on cybersecurity and information assurance.[152] These responsibilities have five elements:

- Foreign Intelligence – Acquiring information through the global information infrastructure to provide foreign intelligence;[153]
- Cyber Security – Providing advice, guidance and services to help protect electronic information and infrastructures belonging to federal organizations and other entities specifically identified by the Government of Canada;[154]
- Defensive Cyber Operations – Conducting activities within the global information infrastructure to help protect information and infrastructures belonging to federal organizations and other entities specifically identified as important by the Government of Canada;[155]
- Active Cyber Operations – Conduct activities through the global information infrastructure to generate effects against a foreign individual, organization or state relating to security, defence or foreign affairs; and[156]
- Technical and Operational Assistance – Provide technical or operational support to federal law enforcement, defence and security agencies.[157]

[152] Canada, "Communications Security Establishment Act," Pub. L. No. S.C. 2019, C. 13, S.76 (2019), 7, 8.
[153] *Ibid*, 7.
[154] *Ibid.*
[155] *Ibid.*
[156] *Ibid*, 8.
[157] *Ibid.*

The CSE Act is noteworthy as it included specific changes to the Communications Security Establishment's cyber responsibilities, expanding their role into offensive (active) cyber operations. While they are prohibited from targeting Canadians or causing 'bodily harm,' this broader mandate provides a new tool the government of Canada may wield.[158] The Communications Security Establishment Act also expanded defensive and security roles for the organization and clarified the ability of the DND/CAF to request support from the organization. This amendment permits, but does not direct coordination between the DND/CAF and CSE.[159]

Review of the Canadian Cyber Program

Canada faces growing threats in cyberspace. The environment provides new means for a host of malicious cyber actors to target Canadians and produce threats to national security. A lack of international norms in cyberspace has created an environment where Canada has few tools to deter or directly counter these threats. With its broader global influence, even the US faces challenges in this arena.

> The department of Justice has used every tool available to disrupt the illegal computer intrusions and cyberattacks by these Chinese citizens, regrettably, the Chinese communist party has chosen a different path of making China safe for cybercriminals so long as they attack computers outside China and steal intellectual property helpful to China.[160]

As discussed in chapter 2, the primary cyber threats to Canada are financially motivated actors.[161] This group, comprised mainly of transnational criminals, target Canadians and Canadian companies with fraud, extortion and corporate espionage schemes. While less

---

[158] *Ibid*, 14.
[159] *Ibid*, 7, 8.
[160] United States, "Seven International Cyber Defendants, Including 'Apt41' Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally," September 20, 2020.
[161] National Cyber Threat Assessment 2020, 5, 10, 11, 20.

prevalent, the most dangerous strategic cyberspace threats are those from China, Russia, Iran and North Korea. These are examples of nation-states that conduct malicious cyber-activities, such as corporate espionage or influence campaigns and continue to develop capabilities in order to manipulate Canada's critical infrastructure.[162]

In response to these threats, Canada's has emphasized increasing its cyber security to make the country more resilient against malicious cyber actors. It has demonstrated an emphasis on the predominant risks to the country, those threatening critical infrastructure and financial security. Recognizing the range of entities involved in this endeavor, the government has clarified roles for coordination between the federal government and external Canadian stakeholders by establishing the Canadian Centre for Cyber Security. Internationally, in the absence of norms, it has sought to establish them. It has contributed to various initiatives and international bodies in attempts to extend the international rules-based order into cyberspace.[163]

In this approach, Canada has been criticized for being too domestically focused. Given that the majority of responses to cyber events require rapid, coordinated international action, an inward emphasis is insufficient.[164] This domestic prioritization is further illustrated in the fact that Canada has developed two national cybersecurity strategies, since 2010, yet it has not release an associated foreign policy or updated its approaches to national security.

As an example, Canada has maintained a preference for horizontal governance on cyberspace within the federal government. This approach carries forward a structure it had previously applied on its national security portfolio. Public Safety remains the 'hub' responsible

[162] National Cyber Threat Assessment 2020, 2, 5, 10-11, 20-21.
[163] Action Plan 2010-2015 for Canada's Cyber Security Strategy, 10.
[164] Angela Gendron, 180.

for coordinating the efforts of a host of multi-purpose departments each assigned responsibilities, some overlapping, and many subject to interpretation.

A 2017 Review of the Canadian government's cyberspace governance illustrated the challenges of the current approach.[165] It states that "[Public Safety's] authority is limited to its persuasion power."[166] It outlines a multi-stakeholder environment reliant on coordination led by multi-departmental working groups and governing bodies that lacked clear roles, responsibilities and expectations.[167] It assessed that the resulting atmosphere is prone to stove-piping, and internal bureaucratic rifts, hardly an organization capable of coordinating rapid international responses.[168]

In addition to the inherent challenge of aligning efforts in a horizontal model, the Canadian structure presents three additional challenges:

- uncertainty on where the responsibility of the coordinating 'hub' actually rests;
- the separation of responsibilities for the operation and security of federal networks; and
- Absence of clarity on the approach to countering threats to the national interest.[169]

A Horizontal Model with Two Heads

The 2010 Cyber Strategy outlined broad responsibilities for various government departments. In the following years, Public Safety's assigned role as the central hub for cyber

[165] Horizontal Evaluation of Canada's Cyber Security Strategy, 5, 6, 7.
[166] *Ibid*, 8.
[167] *Ibid*, 5, 6,7.
[168] *Ibid*.
[169] Email to author, Colonel Christopher Horner, 8 Mar, 2021, 2-4.

coordination became increasingly unclear. The creation of the Cyber Center transferred personnel and responsibilities from Public Safety, reducing its residual role to:

- Act as the central coordinating body, promote comprehensive approaches;
- Oversee the development and implementation of the Canadian Cyber Strategy; and
- Coordinate the assessment of complex threats. [170]

However, the tasks below, originally assigned to Public Safety, were transferred to the Cyber Centre along with the associated staffs.

- Through the Cyber Incident Response Centre continue to act as the focal point for monitoring, providing advice and directing the national response to cyber security incidents; and
- Lead public awareness and outreach efforts to inform Canadians of cyber threats.[171]

The reassignment of these roles opens the question of Public Safety's residual responsibilities.

The Cyber Centre is described as Canada's cyber 'focal point.' With a host of detection, coordination, incident response and advisory tasks, there is an uncertain boundary between Public Safety's roles to coordinate complex events. Equally, with the Cyber Centre's significant coordination roles, the distinction of Public Safety responsibilities to act as the central coordinating body and promote comprehensive approaches is unclear.

[170] Canadian Cyber Strategy 2010, 9.
[171] Canadian Cyber Strategy 2010, 9.

The sole unambiguous residual responsibility of Public Safety is to lead the development and implementation of Canada's Cyber Strategy; however, with the transfer of most expert staff, even this task comes into question. In name, Public Safety retains its role as the hub; however, in day-to-day operations, the Cyber Centre appears to be the central node within the Canadian Government's cyber eco-system. Lack of clarity creates an environment with two major nodes responsible for aligning an array of other departments' actions, complicating the functioning of the consensus-based system.

Responsibility for Federal IT Systems

Within Canada's horizontal governance model, additional complication is introduced through the lack of clear responsibilities for the operation and security of federal IT Systems.[172] The establishment of Shared Services Canada distributed responsibilities for network operations between them and their client departments. Given the dependence on networks for their core business, client departments encountered frustrations when attempting to prioritize network services critical to their organization. A 2015 audit found that Shared Services Canada did not establish clear expectations for the service levels their partners would receive. The audit also assessed that they did not provide partners sufficient information on the security of the services they provided.[173]

Many Shared Services Canada's failures are a matter of public record. Complaints from the RCMP and DND have made news headlines. Both organizations highlighted impacts to their operations based on the level of service provided by the organization.[174] Perhaps most tellingly,

---

[172] Some Federal networks remain exempt to SSC integration, refer to the exemption criteria in the earlier SSC section.

[173] Canada, "Report 4—Information Technology Shared Services," 2015, 4.16, 4.48, 4.49.

[174] Alison Crawford, "Government Tech Support Putting RCMP, Public Safety at Risk, Documents Reveal | CBC News," 2016, https://www.cbc.ca/news/politics/rcmp-it-shared-services-canada-1.3492640; Alison Crawford,

nearly ten years after the organization's establishment, one of the priority issues within DND's IT leadership is to "[e]volve a service delivery framework that is mutually-beneficial to the Department of National Defence and Shared Services Canada."[175]

These challenges illustrate the awkward result of the program's implementation. The initiative centralized federal network infrastructure support into one organization while leaving the endpoints, such as office computers, the responsibility of the supported departments.[176] From a security perspective, it attempts to separate the security of information from that of network infrastructure. The challenge in this structure is that the arbitrary separation creates barriers for the network operators that do not exist for malicious cyber actors. In a common compromise, an actor exploits software through a malicious email and later pivots into network infrastructure. They continually expand access until a goal is achieved. When the responsibility for the security of information and infrastructure is separated, combined action is required to contain a threat resident on both sides of the arbitrary line. This counter-intuitive structure makes the operation

---

"Canada's Top Cop Said It Would Be 'reckless' to Keep Using Federal Government's IT Service | CBC News," 2017, https://www.cbc.ca/news/politics/ssc-rcmp-it-public-safety-1.4373232; Alison Crawford, "National Defence Reports IT Headaches over Shared Services Support | CBC News," CBC News, accessed April 13, 2021, https://www.cbc.ca/news/politics/national-defence-headaches-over-shared-services-1.3494469; Lee Berthiaume, "Poor IT Support Hurting Canadian Military Operations, Internal Review Finds | CTV News," accessed April 13, 2021, https://www.ctvnews.ca/politics/poor-it-support-hurting-canadian-military-operations-internal-review-finds-1.5253148.

[175] Canada, "Assistant Deputy Minister (Information Management) - Canada.Ca," accessed April 8, 2021, https://www.canada.ca/en/department-national-defence/corporate/reports-publications/transition-materials/defence-101/2020/03/defence-101/adm-im.html.

[176] Shared Services Canada History and Legislative Responsibilities; Email to author, Colonel David Yarker, 21 February, 2021, 2; "Shared Services Canada Shows the Sprawling Chaos of Big Government | Ottawa Citizen," 2016, https://ottawacitizen.com/opinion/editorials/editorial-shared-services-canada-shows-the-sprawling-chaos-of-big-government/; Beeby Dean, "U.S. Consultants Slam Shared Services Canada for Failing Projects | CBC News," 2017, https://www.cbc.ca/news/politics/shared-services-canada-it-gartner-consultants-email-brison-harper-management-1.4143071.

of the environment, in addition to the detection and response to network security threats a multi-departmental affair.[177]

Segmenting federal networks in the manner described creates artificial boundaries that don't map to the physics of a network. At the technical level, this leaves limits of authority unclear.[178] The implementation of Shared Services Canada has created a complicated multi-stakeholder environment, pitting their cost savings mandate against the operational priorities of the supported departments. It separates federal IT systems in a cumbersome matter and leaves no individual or organization responsible for the entire system.[179]

Threats to the National Interest

Canada's approach to cyberspace has prioritized the most common risks, those threatening the financial security of Canadians and Canadian businesses. Despite demonstrated examples and threat assessments that have illustrated threats to the national interest, Canada's programs and policies have yet address how it will respond to these challenges. The nation's approach carries forward its 20th Century perspectives and approaches. It has brought forward a preference for centralized control of a horizontal consensus driven structure; it is attempting to continue its traditional approaches to external affairs by establishing international cyber norms; and it has shown little deviation on approaches to national security and defence.

The traditional Canadian assumption of national security, whether right or wrong, remains unchanged in the digital era. While cyberspace provides the ability to bypass Canada's traditional geo-strategic arrangements, these threats have been insufficient to prompt a change in

[177] Email to author, Colonel David Yarker, 21 February, 2021, 1-2.
[178] *Ibid*, 1-2.
[179] *Ibid*, 2.

this entrenched narrative. With little public interests in the topic, the country's leaders not defined a clear responsibilities for national security in cyberspace.

The absence of dialogue permits the CAF or CSE to interpret a wide range of possible organizational responsibilities. They could both assume central and conflicting roles. They could both assume smaller roles leaving capability gaps, or they could work collaboratively. Canada's cyber program governance leaves this range of possibilities subject to the discretion of the CAF and CSE.

CSE and their subordinate Cyber Centre have roles that span intelligence and a range of cybersecurity, defence and offensive activities. They are the lead for public and private coordination, and they have been provided with the authority to conduct offensive (active) cyber operations.[180] The new CSE Act permits the organization to "degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security." [181] From CSE's vantage point, they could easily interpret a central role in response to the national security threats.

From the military perspective, the CAF is charged with eight core missions, the first of which is to: "detect, deter and defend against threats to or attacks on Canada."[182] According to the 2017 Defence Policy, this core mandate includes cyberspace. The CAF is tasked to: ensure threats in the cyber domain do not "threaten Canadian Defence and Security Objectives and strategic interests, including the economy."[183] The CAF is also tasked to develop and employ

[180] Canadian Cyber Strategy 2018, 7-8, 28.
[181] Communications Security Establishment Act, 7-8.
[182] Strong Secure Engaged, 17.
[183] Strong Secure Engaged, 60.

offensive cyber capabilities against adversaries in support of government-authorized military actions and to be prepared to support response to domestic cyber-attacks.[184]

Viewing the CSE and CAF authorities and responsibilities collectively, both have tasks to detect threats, to develop offensive cyber capabilities and to defend the nation in cyberspace. While these mandates permit independent actions, they do not preclude collaborative approaches. Similar combined intelligence and military collaboration have been employed by Canada's allies.[185] While collaboration is a possible and logical outcome, differing perspectives, cultures and priorities between DND/CAF and CSE may create barriers to mutually beneficial coordination.[186]

Chapter Summary

Between 2010 and 2020, Canada has released two cyber strategies and a national defence policy. It has produced new laws and established organizations such as Shared Services Canada and the Canadian Centre for Cyber Security. The country's cyberspace program has focused domestically, emphasizing enhancing its resilience to cyber threats. The approach has been criticized as insufficient given the response to the predominance of threats requires rapid coordinated international action.

Canada has demonstrated little deviation from its 20th Century middle power and contribution warfare doctrines. It continues a preference for horizontal federal governance models; one, on the cyber portfolio, that is coordinated by two departments and a series of multi-

[184] Strong Secure Engaged, 111.

[185] Communications Security Establishment Act, 13; United States, "Department of Defense Strategy for Operating in Cyberspace," July 2011, 5-6; United Kingdom, "National Cyber Security Strategy 2016-2021," 2016, 51.

[186] Email to author, Colonel David Yarker, 21 February, 2021,3-4; Email to author, Government of Canada Cyber Community Official, 28 February, 2021, 2-4; Email to author, Colonel Christopher Horner, 8 Mar, 2021, 2-4.

departmental working groups. These bodies, described in a 2017 audit as lacking clear roles responsibilities and expectations. This approach is illustrative of a continuance of Canada's traditional perspective, one where national security is assumed and the country had little need for rapid response to external threats. Despite cyberspace challenging this assertion, Canada has yet to demonstrate a change in its approach.

CHAPTER 4: CAF CYBER PROGRAM AND THE BROADER ECOSYSTEM

Inside the broader federal government ecosystem, the Canadian military continues to develop an operational cyber capability. This chapter will explore the military's approach, outlining developmental milestones and reviewing organizational structure. This discussion will illustrate a complicated organization characterized by priority and resource tensions.

With an understanding of the DND/CAF cyber program, the chapter will revisit the paper's foundational thesis: the complicated governance of Canada's approach to national security in cyberspace is the product of the Nation's continued adherence to 20th century approaches. It will highlight that deliberate decisions rooted in the country's traditional approaches to national security and defence have produced a complicated governance model.

Evolution of the CAF Cyber Program

Initiation of the CAF's formal cyber efforts began in 2009 with the Integrated Capstone Concept. The doctrine document introduced cyberspace as a domain of warfare, signaling the CAF's requirement to develop new capabilities in this environment.[187] The following year, the first Canadian National Cyber Strategy was released, which included initial organizational structures within DND/CAF to begin the development of a broader cyber program.[188] As noted previously, the 2010 Cyber Strategy assigned new tasks to DND/CAF, which were expanded upon by internal direction and guidance. Notable examples included directives on defensive

[187] Canada, *Integrated Capstone Concept* (Ottawa, Ontario: Chief of Force Development, National Defense Headquarters, 2010),29; Canada, "Cyber Operations 101 and Planning Considerations" (Ottawa: Department of National Defence, February 2021), 18.

[188] Action Plan 2010-2015 for Canada's Cyber Security Strategy, 6; Cyber Operations 101 and Planning Considerations, 18; Canadian Cyber Strategy 2010, 10.

cyber operations (2015), mission assurance (2017) [189], and offensive cyber operations (2019).[190] While the specific direction is classified, the consolidated tasks for the CAF are drawn from the 2010 Cyber Strategy and expanded within the 2017 Defence Policy are:

- Protect CAF networks and weapons systems from cyber effects;[191]
- Develop and employ offensive cyber capabilities against adversaries in support of government-authorized military actions;[192]
- Work with other government departments to identify threats and response options and exchange best practices with military allies;[193]
- Provide intelligence assessments and analysis on cyber threats to DND/CAF and military cyber threats to the Government of Canada;
- "Ensure threats in the cyber domain do not threaten Canadian Defence and Security Objectives and strategic interests including the economy"; and [194]
- Be prepared to support response to cyber-attacks on critical domestic infrastructure.[195]

In undertaking these tasks, the CAF adopted a similar approach to that of allies, seeking to develop a range of cyber capabilities and integrate them into military operations. This transition required a fundamental shift, one that moves from a view of IT systems as services to a perspective of IT as part of a broader environment enabling friendly and enemy militaries to

[189] Mission assurance is a broad categorization that refers to efforts protecting CAF's ability to conduct its assigned missions. It places an emphasis on the protection of CAF's platforms and weapons systems from cyber threats.
[190] Cyber Operations 101 and Planning Considerations, 18.
[191] Strong Secure Engaged, 111.
[192] *Ibid*.
[193] *Ibid*.
[194] *Ibid*, 60.
[195] *Ibid*, 81.

generate decisive effects.[196] Instead of a focus on industry best practices and administrative efficiency, cyber operations center on the adversary and the military mission.[197]

While the CAF is assigned cyber tasks, how they will be realized is a complicated topic. A military's core purpose is to prepare for the worst-case scenario—the high-impact, low-probability prospect of war. While there are centuries of experience to draw from in conventional warfare, we have yet to witness conflict between opponents with advanced cyber capabilities. Cyber operations within war remains a field of speculation. A growing range of discreet examples provide insights, such as the ability to attack domestic infrastructure and military weapons systems, influence public opinion, and steal volumes of information. Yet, we have no real-world data about how cyber capabilities can or should be wielded comprehensively in a military campaign, and thus nothing on which to generate military doctrine for its use.[198]

The CAF's 2017 Joint Doctrine Note illustrated initial thought on the subject. The document acknowledges the challenges of defining an approach to cyberspace. It states that many concepts remain "subject to heated debate and outright disagreement among experts."[199] It asserts that it is "far too soon to commit the CAF to a rigid doctrine for cyber operations; there remain too many areas for active intellectual development."[200] While acknowledging the challenge, it also highlighted that it was already late to begin acting on basic principles.[201]

---

[196] Joint Doctrine Note Cyber Operations, 4-1; Email to author, Colonel David Yarker, 8 April, 2021, 2.
[197] Joint Doctrine Note Cyber Operations, 1-3, 3-14, 3-15, 4-2, 4-3.
[198] Email to author, Colonel David Yarker, 8 April, 2021, 2.
[199] "Joint Doctrine Note Cyber Operations, iii.
[200] *Ibid.*
[201] *Ibid.*

Organizational Structure

Given the unknowns within the environment, early work to develop CAF requirements were estimates drawn from information available at the time. In developing initial personnel requirements, the CAF deliberately established a modest estimate. They assumed that existing resources would be re-prioritized to support cyber operations.[202]

As cyber positions were approved, they were invested across DND/CAF. Developing a new capability required cyber personnel in intelligence organizations, operational headquarters, project staffs, and advisors in senior organizational roles. The remaining approximately two-thirds of the positions were used to build new cyber organizations and augment four levels of headquarters.[203]

As the CAF program continued to mature through personnel investments and concept development, its structure took shape in 2018 with the implementation of the Cyber Force Command.[204] The new organization created a central cadre responsible for everything from training to developing and employing cyber capabilities. In military parlance, it is responsible for: force generation, force employment, force development and force management. [205] The approach provides efficiencies by centralizing all elements under one commander. It provides unity of focus and expedites the process of identifying, adapting and responding to operational requirements, all actions critical in an environment as uncertain and dynamic as cyberspace.

[202] Email to author, Colonel David Yarker, 15 April, 2021, 1.
[203] Email to author, Colonel David Yarker, 15 April, 2021, 1; The four levels of headquarters were: CFNOC, CFIOG, DGIMO and CJOC.
[204]Cyber Operations 101 and Planning Considerations, 18; Joint Doctrine Note Cyber Operations, 6-1, 6-2.
[205] Cyber Operations 101 and Planning Considerations, 19.

Despite a centralized approach offering these advantages, realizing them is complicated by how the structure was implemented.

The Cyber force structure was established within the Associate Deputy Minister of Information Management (ADM(IM)), DND's IT Service organization.[206] The CAF approach mapped cyber roles and responsibilities onto existing individuals and organizations, selectively adding new positions throughout the structure.[207] Without the requirement for a new organization or support infrastructure, the plan was expedient and practical. Figure 4.1 illustrates the resulting organizational structure for cyber operations. This illustration is not meant to provide detailed understanding; it simply demonstrates the cost of expedience: complication.

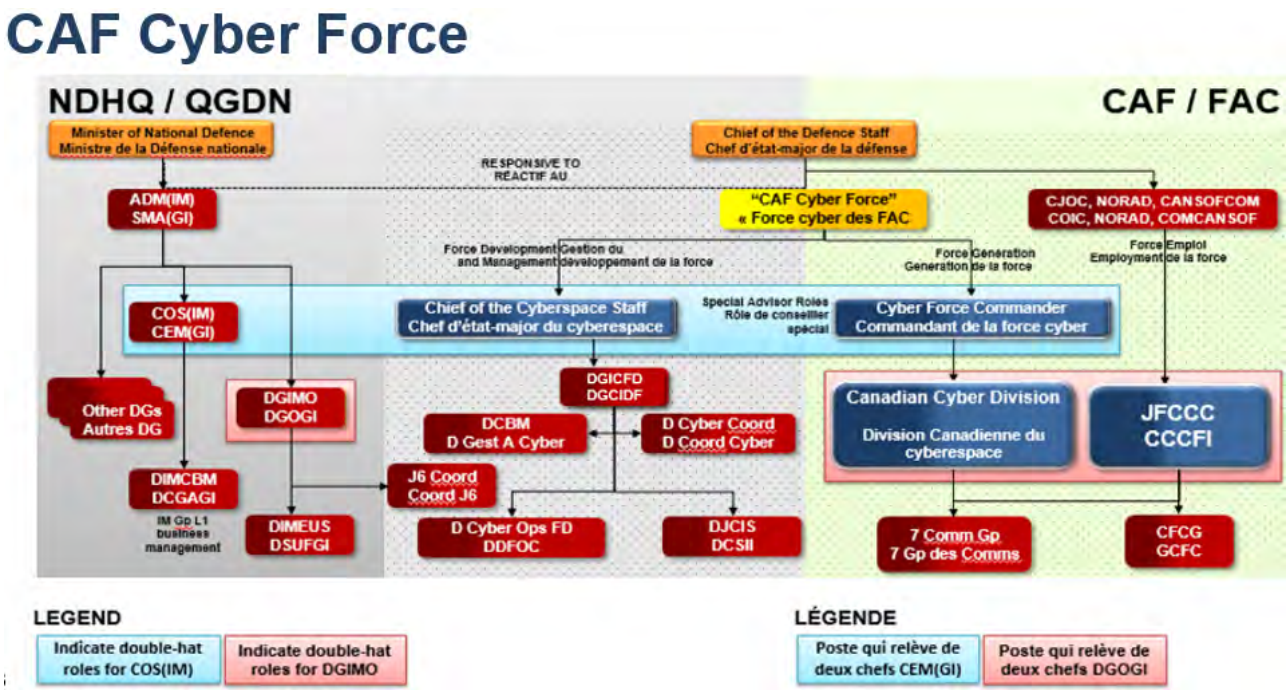

Figure 4.1 -- CAF Cyber Force Structure
Source: Canada, "Cyber Operations 101 and Planning Considerations", 18.

[206] *Ibid*, 18.
[207] Email to author, Colonel David Yarker, 15 April, 2021, 1.

The challenge of illustrating this structure is a function of its design. The structure attempts to establish a capability responsible for military operations under the CDS, the senior military officer, within an organization that answers to the Deputy Minister. The figure attempts to illustrate how the structure will navigate this separation of responsibilities between the DND/CAF's co-equal senior-most leaders.

The CDS is responsible for the training and employment of military capabilities. Despite the centralization of the cyber force structure within an organization answering to the Deputy Minister, these duties remain.[208] In this approach, the CDS' responsibilities are maintained by establishing a new Cyber Force Commander role and assigning it to the existing ADM(IM) Chief of Staff. The incumbent Major General is responsive to ADM(IM) as the Chief of Staff and the CDS as the Cyber Force Commander.[209]

While responsible for the entire program, the Commander delegates the training, organization and employment of cyber capabilities to the Commander of the Cyberspace Division and the Joint Force Cyber Component Commander; both are new roles assigned to the leader of ADM(IM) 's Operational IT service delivery organization.[210] This arrangement introduces another element into the structure: operational force employers. Organizations such as the Canadian Joint Operations Command, Canadian Special Forces Command, and North American Aerospace Defence Command. Each of these organizations, peers to ADM(IM), are responsible to command CAF operations. Thus, this Brigadier General reports to the Cyber

[208] Lagassé, 32-34.
[209] Joint Doctrine Note Cyber Operations 6-1, 6-2; Cyber Operations 101 and Planning Considerations, 18.
[210] *Ibid*; Operational IT Service delivery organization refers to the Director General of Information Management Operations (DGIMO).

Force Commander on their cyber training and organization roles, to a force employer to support military operations and ADM(IM) on their IT service delivery role.[211]

Subordinate to these leaders are the formations and working-level tactical elements required to conduct day-to-day operations. Notable amongst these is the Canadian Forces Information Operations Group and its subordinate cyber units. The Information Operations Group is an intelligence focused headquarters that answers to ADM(IM) 's Operational IT Service organization and the Canadian Forces Intelligence Command, another organizational peer to ADM(IM). The cyber force structure rebranded the Information Operations Group as the Canadian Forces Cyber Group and added new cyber responsibilities.[212]

Beneath this headquarters are the Canadian Forces Network Operations Center and the Combined Cyber Unit. The Canadian Forces Network Operations Centre, an organization with pre-existing network security requirements levied by ADM(IM), became the primary CAF defensive cyber operations organization. The Combined Cyber Unit represented a new offensive cyber entity.[213]

To explain a very complicated structure concisely, the DND/CAF has built an operational cyber structure on top of its IT Service delivery organization. It has done so by assigning significant new roles and responsibilities on top of existing positions and organizations. The approach makes leaders and organizations responsible to multiple supervisors throughout the structure, each with widely divergent priorities.

---

[211] *Ibid.*

[212] Cyber Operations 101 and Planning Considerations, 18, 32.

[213] Cyber Operations 101 and Planning Considerations; The Combined Cyber Unit is represented as 2 COU at figure 4.2.

Prioritization and Capacity

This brief explanation of the CAF Cyber Force structure does not illustrate the full depth of its complexity. It did not address additional challenges of organizational culture, policies, authorities or workforce education and training. These are all areas worthy of independent study. It is, however, sufficient to highlight the significant organizational issues facing the CAF cyber program, namely priorities and capacity.

Building an organization answerable to multiple supervisors while sharing resources creates tension. Even before the addition of a cyber operations program, ADM(IM) had the already challenging mandate of providing IT services to the large and complex organization of DND/CAF.[214] Inside this organization, the CAF is attempting to build an operational capability required to think differently about networks and technology while also requiring them to retain IT service and security responsibilities.

These challenges had begun before the establishment of the organizational structure in 2018. From 2011 onward, annual growth in cyber resources had been invested in ADM(IM). These new personnel and resources were intended to only partially offset the cyber requirement, with the expectation that existing resources would later be reallocated to meet the actual demand. Unfortunately, the investment of these new resources occurred concurrently with unanticipated cuts within ADM(IM). The transfer of personnel to enable the establishment of Shared Services Canada and a government-wide deficit reduction program both had significant impacts on the organization. Not only were existing resources now unlikely to be reallocated to support cyber

[214] Email to author, Colonel Christopher Horner, 8 March, 2021, 5-6; Canada, "Assistant Deputy Minister (Information Management) - Canada.Ca," accessed April 8, 2021, https://www.canada.ca/en/department-national-defence/corporate/reports-publications/transition-materials/defence-101/2020/03/defence-101/adm-im.html.

efforts, but the cyber resources added to the organization also risked being reallocated to offset the ongoing ADM(IM) resource contraction.[215]

ADM(IM) 's standing responsibilities and the CDS's goal of developing an operational cyber capability, have been levied on the same workforce. While cyber positions have been added, they were invested into an organization concurrent to ongoing program cuts. These tensions and overlapping structure produce an environment where the investment of time, focus, and resources into CAF's cyber program comes at a cost to the priorities of the Deputy Minister and ADM(IM).[216] From the outset, the CAF's cyber program was immediately in competition for resources. Each leader from the Cyber Force Commander through the subordinate headquarters and those at working-level tactical units faced a challenge in managing and responding to divergent responsibilities and expectations. Without consensus between the Deputy Minister, the CDS, ADM(IM), Canadian Forces Intelligence Command (CFINTCOM), force employers and several layers of internal leadership and organizations, CAF Cyber efforts could quickly become fractured and misaligned. As an example, the priorities of CFINTCOM levied on the Information Operations group could shift resources away from ADM(IM) priorities. Equally, ADM(IM) service provisioning requirements could overcome cyber operations in support of a force employer. The system is one that requires careful management and prioritization.

---

[215] Institute of Fiscal Studies and Democracy, "The Deficit Reduction Action Plan: Politics Versus Planning and Transparency in Government Finance," 2017, 1; Canada, "Strategic Review (SR) and Deficit Reduction Action Plan (DRAP) - DPR - 2013-14 - Canada.Ca," 2014, https://www.canada.ca/en/department-national-defence/corporate/reports-publications/departmental-performance/2013-14/section-iv-strategic-review-deficit-reduction-action-plan.html; Email to author, Colonel David Yarker, 15 April, 2021, 1.

[216] Email to author, Colonel Christopher Horner, 8 March, 2021, 5-6.

The competing priorities and double hatted approach make the CAF structure a complicated system to manage. It invests its cyber resources in ADM(IM), creating a structure that is prone to prioritize IT service provisioning over cyber operations.[217] This environment places significant demand on a small resource, leaving little room for the experimentation, testing, failure, adaptation and evolution required to consider and develop a cyber capability to face the unknown unknowns.

Diverging Perspectives

From the CAF Cyber program to that of the federal government, both employ complicated organizational structures and governance. When combined, these systems produce even greater complication. Without context, it is difficult to understand the logic of such a structure. This view, however, does not allow for consideration of the numerous external influences that have informed the approach. This creates an interesting dynamic. When these systems are viewed from the top, from the perspectives of the Government and senior departmental leaders that created them, the approach is rational. When viewed from the inside, at more junior levels by those who must make the system function on a day-to-day basis, it appears counter-intuitive.

The Inside View

The junior personnel working within this structure encounter a complicated governance eco-system with unclear roles, limited resources that is prone to diverging priorities. Inside DND/CAF, the Cyber Force must balance demands from the Deputy Minister and CDS. As one

[217] Email to author, Colonel Christopher Horner, 8 March, 2021, 5-6; The author observed this first-hand as the operations officer at CFNOC between 2018-2020.

moves lower into the organizational structures the requirements of ADM(IM), CFINTCOM and operational force employers are introduced. These organizations levy tasks onto a shared resource. The new cyber responsibilities include preparing for an unknown future environment, in addition to more immediate tasks of defending DND/CAF networks and weapons systems, developing offensive cyber capabilities and working with other government departments and allies to identify and respond to threats to the nation. If not carefully managed and prioritized by senior leaders at multiple levels, this shared workforce risks facing competing demands through multiple supervisory paths.

External to DND/CAF, the Government of Canada's cyber ecosystem is another complicating component. The federal program outlines broad departmental responsibilities and leaves its functioning coordinated by two organizations: Public Safety and the Canadian Centre for Cyber Security. It relies on a partnership between the military, the Canadian Center for Cyber Security and Shared Services Canada to secure and defend military networks. It relies on cooperation to deconflict and coordinate offensive cyber operations between the military and the Communications Security Establishment. It also depends upon the coordination of multiple departments to develop a consolidated understanding of cyber threats.

In each of these relationships, members of the CAF Cyber Force encounter peers from other departments with differing priorities. Within these groups, they must navigate these differences while facing unclear boundaries of organizational responsibility that are subject to interpretation. Where conflict arises, the system's structure of coordination vice authority leaves resolution with very senior leaders such as the Minister of National Defence or the Privy Council Office; executives that are all but unreachable to junior staff. A series of rational decisions has

produced an ecosystem requiring careful and continuous management by institutional leaders to function efficiently.

The View from the Top

Canada is accustomed to far-away threats. Its geography and collective security assurances have engrained a perspective that security and conflict are distant concerns. The country has traditionally enjoyed the ability to choose when it became involved in security and defence matters. From this perspective, a horizontal governance model for national security, one that now extends into its approach to cyberspace, is logical. The structure retains central control of a politically risky portfolio within the Government. When it chooses to respond to a given issue, the system allows the Government to draw on the departments and resources required. The day-to-day inefficiencies are of little concern so long as it is responsive when called. The approach, rooted in an assumption of security, is rational from this perspective.

Within the military, the government continues to employ a contribution approach to employment. This leaves the organization to interpret its priorities based on an array of possible government requirements. Before the requirement to consider cyberspace, the leadership of the Canadian military already faced significant demands on the organizations' limited resources. As it contemplated how it would address its cyberspace requirements, it is not difficult to understand how the efficiencies and resource savings of the current approach would be compelling. The numerous unknowns surrounding military cyber requirements further incentivizes a conservative resource investment. Thus, building the CAF cyber organization within an existing organization is a reasonable approach.

Deliberate and rational decisions from Canada's leaders through to those within the upper echelons of the military have created complicated governance. When viewed without context, it appears inefficient and counter-intuitive. When viewed from Canada's national perspective, the influences of assumed security, horizontal governance and contribution warfare, provide insights into the design.

CONCLUSION

Canada has prospered through the 20th Century. Beneficial geography and rich natural resources provided the foundation for a strong nation. It enjoyed close proximity to the major economy of the US, while being shielded from threats by distance and collective security arrangements. With its security assured, Canada has had the luxury of choosing when and how it participated in the international forum. When it chose to become engaged, it applied a middle-power doctrine, working through multilateral structures and organizations to moderate power imbalances and advance its interests. These structures, which rest on an international-rules-based order, have become a hallmark of the Canadian approach to foreign affairs.

Despite the country's relative safety during this period, Canada required military commitments to advance and protect its interests. It had to commit sufficient resources to appease the US as a defence against help or lockdown. It was required to support NATO, and the UN and other coalitions to maintain international order, a condition essential to its approach to foreign affairs. With a population largely absent national security concern, the government has cautiously balanced these requirements.

The product of this environment is a centralized national security structure. The government retains control on national security matters, but provides few standing priorities to its departments, having produced only a single national security strategy in the country's history. On a day to day basis, this structure is managed through a horizontal, consensus based approach. The structure allows elected leaders to deliberately consider individual issues and draw on the required resources and departments when and where needed. In an environment of distant threats, this approach has suited Canada well.

Canada's traditional approaches are being challenged in the digital age. The protections formerly offered by geography are inverted in cyberspace. Malicious actors now target the country from beyond the reach of Canadian authority. On foreign affairs, its multilateral approach of leveraging collective influence is diminished in the absence of international cyberspace norms. The result has seen Canada become a high-reward, low-risk environment for malicious cyber actors. The country's wealth, research and alliances attractive to malicious cyberspace actors. In response, the country has developed numerous strategies, established new organizations and undertaken a host of initiatives.

The predominant cyber threat to Canada is that from financially motivated criminals who conduct fraud and extortion schemes within the country. While not as prevalent, nation-states are assessed as the greatest strategic threat. They have undermined the Canadian economy, conducted influence campaigns, and probed its critical infrastructure. These threats to the national interest, have yet to be sufficient to alter the nation's entrenched sense of security, and the country has carried forward its traditional approaches into the digital age.

The country's emphasis has been on increasing national cybersecurity to enhance resilience. It created the Cyber Center to act as a domestic focal point and organize a collaborative efforts across the numerous Canadian stakeholders. On foreign affairs, it continues to support efforts to establish norms, the foundation of its multilateral approach. Internal to the government, on the national security portfolio, its governance is less clear. It carries forward the horizontal governance structure. The routine actions of this structure are coordinated by both the Cyber Center and Public Safety. Within the structure additional uncertainty exists. The lines of separation between Shared Services Canada and supported departments on network security

remain unclear as do those between CSE and DND on their roles to defend the national interest in cyberspace.

Within the Canadian military, developing an operational cyber capability represents an additional requirement within an environment where tasks exceed resources. The military already faced the challenge of anticipating and preparing to respond to the government's requirements. In this environment, the CAF selected a conservative and expedient approach to implement a cyber capability. It overlaid new cyber roles and responsibilities on top of an existing organization. In doing so, it created a multi-polar structure responsive to both of the Department's co-equal senior leaders, the CDS and Deputy Minister.

The horizontal governance of the federal cyber program and the multi-polar approach of the Canadian military have inherent prioritization and resource tensions. To function efficiently, the systems require consensus amongst organizations with different priorities and cultures. These complicated structures are the product of Canada's 20th Century doctrines, with assumption of safety, it is accustomed the luxury of time to consider issues of national security. The structures are sufficient for the government to episodically draw on them when it chooses to address a security concern. The new threats in cyberspace, now requiring rapid and coordinated action internal to the country and within the international fora, have yet to be sufficient to motivate a change in Canada's traditional doctrines.

BIBLIOGRAPHY

Arnold, Brent J., and Stephanie MacLellan. “Cyber Security in Canada:” Governing Cyber Security in Canada, Australia and the United States. Centre for International Governance Innovation, 2018. JSTOR. http://www.jstor.org/stable/resrep17311.6.

Barrinha, André, and Thomas Renard. “Power and Diplomacy in the Post-Liberal Cyberspace.” *International Affairs* 96, no. 3 (May 1, 2020): 749–66. https://doi.org/10.1093/ia/iiz274.

BBC News. “Hack Attack Causes ‘massive Damage’ at Steel Works - BBC News.” Accessed March 2, 2021. https://www.bbc.com/news/technology-30575104.

Beeby, Dean. “U.S. Consultants Slam Shared Services Canada for Failing Projects | CBC News,” 2017. https://www.cbc.ca/news/politics/shared-services-canada-it-gartner-consultants-email-brison-harper-management-1.4143071.

Brown, Gary, and Keira Poellet. “The Customary International Law of Cyberspace.” *Strategic Studies Quarterly* 6, no. 3 (2012): 126–45.

Canada. “2019 Canadian ICT Sector Profile.” Ottawa: Innovation, Science and Economic Development Canada, 2019. https://www.ic.gc.ca/eic/site/ict-tic.nsf/vwapj/ICT_Sector_Profile2019_eng.pdf/$file/ICT_Sector_Profile2019_eng.pdf.

———. “About Us: Canadian Centre for Cyber Security.” Accessed March 17, 2021. https://cyber.gc.ca/en/about-cyber-centre.

———. *Action Plan 2010-2015 for Canada’s Cyber Security Strategy*. Ottawa: Government of Canada, 2013. https://central.bac-lac.gc.ca/.item?id=PS9-1-2013-eng&op=pdf&app=Library.

———. “Accountabilities of the Minister, Deputy Minister and Chief of the Defence Staff - Canada.Ca,” March 11, 2021. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/transition-materials/defence-101/2020/03/defence-101/accountabilities.html.

———. “Assistant Deputy Minister (Information Management) - Canada.Ca.” Accessed April 8, 2021. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/transition-materials/defence-101/2020/03/defence-101/adm-im.html.

———. “Backgrounder: Canadian Centre for Cyber Security | Communications Security Establishment.” Accessed March 16, 2021. https://cse-cst.gc.ca/en/backgrounder-fiche-information.

———. Budget 2018: Equality and Growth (2018). https://www.budget.gc.ca/2018/docs/plan/budget-2018-en.pdf.

———. *Building a Nation of Innovators - Innovation for a Better Canada*. Ottawa: Innovation, Science and Economic Development Canada, 2019. https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00105.html.

———. “Canadian Internet Use Survey.” Accessed February 2, 2021. https://www150.statcan.gc.ca/n1/daily-quotidien/191029/dq191029a-eng.htm.

———. *Canada’s Cyber Security Strategy: For a Stronger and More Prosperous Canada.* Ottawa: Govt. of Canada, 2010.

———. “Canada’s State of Trade 2019.” Ottawa: Global Affairs Canada, 2019. https://www.international.gc.ca/gac-amc/publications/economist-economiste/state_of_trade-commerce_international-2019.aspx?lang=eng.

———. “Canadian Centre for Cyber Security - National Cyber Threat Assessment 2020.” Canada, 2020. https://cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2020.

———. Communications Security Establishment Act, Pub. L. No. S.C. 2019, C. 13, S.76 (2019). https://laws-lois.justice.gc.ca/eng/acts/C-35.3/page-1.html.

———. “CSIS Public Report 2019.” Ottawa: Canadian Security and Intelligence Service, 2019.

———. “Cyber Operations 101 and Planning Considerations.” Ottawa, On: Department of National Defence, February 2021.

———. “Cyber Placemat.” Department of National Defence, 19 Nov 20.

———. “Cybersecurity Vulnerabilities Associated with Some Medical Devices with Bluetooth Low Energy Chips - Recalls and Safety Alerts.” Accessed April 1, 2021. https://healthycanadians.gc.ca/recall-alert-rappel-avis/hc-sc/2020/72555a-eng.php.

———. “Departmental Plan 2020-2021, Building a Safe and Resilient Canada.” Ottawa: Public Safety Canada, 2020.

———. “Frequently Asked Questions (FAQs) Concerning Federally-Regulated Petroleum Pipelines in Canada.” Accessed February 27, 2021. https://www.nrcan.gc.ca/our-natural-resources/energy-sources-distribution/clean-fossil-fuels/pipelines/faqs-federally-regulated-petroleum-pipelines-canada/5893.

———. Government Bill (House of Commons) C-59 (42-1) - Royal Assent - National Security Act, 2017, Pub. L. No. Bill C-59 (2019). https://www.parl.ca/DocumentViewer/en/42-1/bill/C-59/royal-assent.

———. “Horizontal Evaluation of Canada’s Cyber Security Strategy.” Ottawa, On: Public Safety, 2017. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/vltn-cnd-scrt-strtg/index-en.aspx.

———, ed. *Integrated Capstone Concept*. Ottawa, Ontario: Chief of Force Development, National Defense Headquarters, 2010.

———. “Joint Doctrine Note Cyber Operations.” Department of National Defence, 2017.

———. “LAND OPERATIONS.” National Defence, January 1, 2008. http://armyapp.forces.gc.ca/SOH/SOH_content/B-GL-300-001-FP-001%20(2008).pdf.

———. “Minister of Foreign Affairs Mandate Letter.” Canada, December 13, 2019. https://pm.gc.ca/en/mandate-letters/2019/12/13/minister-foreign-affairs-mandate-letter.

———. “Minister of National Defence Mandate Letter,” December 13, 2019. https://pm.gc.ca/en/mandate-letters/2019/12/13/minister-national-defence-mandate-letter.

———. *National Cyber Security Strategy*. Ottawa, Ontario, 2018. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx.

———. *National Cyber Security Action Plan 2019-2024: Budget 2018 Investments*, 2019. http://epe.lac-bac.gc.ca/100/201/301/weekly_acquisitions_list-ef/2019/19-34/publications.gc.ca/collections/collection_2019/sp-ps/PS9-1-2019-eng.pdf.

——— . “National Highway System.” Accessed February 27, 2021. https://tc.canada.ca/en/corporate-services/policies/national-highway-system?pedisable=true.

———. Orders In Council 2012-0958, 2012–0958 § (2012). https://orders-in-council.canada.ca/attachment.php?attach=26384&lang=en.

———. Orders In Council 2013-0367, 2013–0367 § (2013). https://orders-in-council.canada.ca/attachment.php?attach=27596&lang=en.

———. “Population Growth: Migratory Increase Overtakes Natural Increase.” Ottawa: Statistics Canada, 2018. https://www150.statcan.gc.ca/n1/pub/11-630-x/11-630-x2014001-eng.htm.

———. “Report 4—Information Technology Shared Services,” 2015. https://www.oag-bvg.gc.ca/internet/English/parl_oag_201602_04_e_41061.html.

———. “Securing an Open Society : Canada’s National Security Policy.” Ottawa, Ontario: Privy Council Office, 2004. http://publications.gc.ca/collections/Collection/CP22-77-2004E.pdf.

———. “Shared Services Canada History and Legislative Responsibilities - Canada.Ca.” Accessed March 16, 2021. https://www.canada.ca/en/shared-services/corporate/transparency/briefing-documents/ministerial-briefing-book/shared-services-canada-history-legislative-responsibilities.html.

———. “Strategic Review (SR) and Deficit Reduction Action Plan (DRAP) - DPR - 2013-14 - Canada.Ca,” 2014. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/departmental-performance/2013-14/section-iv-strategic-review-deficit-reduction-action-plan.html.

———. “Strong Secure Engaged.” Department of National Defence, 2017. http://dgpaapp.forces.gc.ca/en/canada-defence-policy/docs/canada-defence-policy-report.pdf.

———. “The Specific Case of the Crown Prerogative Power to Deploy the CF on Military Operations of Canada - Canada.Ca,” 2015. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/military-law/crown-prerogative/the-specific-case-of-the-crown-prerogative-power-to-deploy-the-cf-on-military-operations-of-canada.html.

Canadian Cyber Threat Exchange. “Cyber Facts.” Accessed April 2, 2021. https://cctx.ca/cyber-facts/.

Caredda, Sergio. “Models: The Lippitt-Knoster Model for Managing Complex Change | Sergio Caredda,” October 10, 2020. https://sergiocaredda.eu/organisation/tools/models-the-lippitt-knoster-model-for-managing-complex-change/.

Casgrain, Pierre. *From Middle to Major Power*. Book, Whole. Macdonald-Laurier Institute for Public Policy, 2020.

CCDCOE. “2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law.” Accessed April 2, 2021. https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/.

Chapnick, Adam. “The Middle Power.” *Canadian Foreign Policy Journal* 7, no. 2 (January 1, 1999): 73–82. https://doi.org/10.1080/11926422.1999.9673212.

Coughlan, Sean. “How Canada Became an Education Superpower - BBC News.” Accessed January 30, 2021. https://www.bbc.com/news/business-40708421.

Crawford, Alison. “Canada’s Top Cop Said It Would Be ‘reckless’ to Keep Using Federal Government’s IT Service | CBC News,” 2017. https://www.cbc.ca/news/politics/ssc-rcmp-it-public-safety-1.4373232.

———. “Government Tech Support Putting RCMP, Public Safety at Risk, Documents Reveal | CBC News,” 2016. https://www.cbc.ca/news/politics/rcmp-it-shared-services-canada-1.3492640.

———. “National Defence Reports IT Headaches over Shared Services Support | CBC News.” CBC News. Accessed April 13, 2021. https://www.cbc.ca/news/politics/national-defence-headaches-over-shared-services-1.3494469.

Deibert, Ron. “Canada and the Challenges of Cyberspace Governance and Security.” *The School of Public Policy* 5, no. 3 (March 2013): 2–12.

Erskine, T., and M. Carr. “Beyond Quasi-Norms: The Challenges and Potential of Engaging with Norms in Cyberspace,” 2016.

Fetterly, Ross. “The World Has Changed. Canada’s Defence Strategy Hasn’t Changed with It.” Macdonald-Laurier Institute, October 8, 2019. https://www.macdonaldlaurier.ca/canada-confronts-complex-threat-environment-ross-fetterly-inside-policy/.

Gelb, Alan. “Economic Diversification in Resource Rich Countries,” 2010, 1–23. https://doi.org/10.1.1.368.6576.

Gendron, Angela. “Cyber Threats and Multiplier Effects: Canada at Risk.” *Canadian Foreign Policy Journal* 19, no. 2 (June 1, 2013): 178–98. https://doi.org/10.1080/11926422.2013.808578.

Hammock, C J. “Enabling the Development and Deployment of NATO Cyber Operations: An Analysis of Modern Cyber Warfare Operations and Thresholds of Global Conflict.” *Journal of Information Warfare* 16, no. 3 (2017): 79–94.

Horn, Bernd, Emily Spencer, and Colonel Bernd Horn. *No Easy Task : Fighting in Afghanistan*. Toronto, CANADA: Dundurn, 2012.

Hurwitz, Roger. "The Play of States: Norms and Security in Cyberspace." *American Foreign Policy Interests* 36, no. 5 (September 3, 2014): 322–31. https://doi.org/10.1080/10803920.2014.969180.

Institute of Fiscal Studies and Democracy. "The Deficit Reduction Action Plan: Politics Versus Planning and Transparency in Government Finance," 2017. http://ifsd.ca/web/default/files/360/DRAP%20Case.pdf.

Jablonsky, David, and J. Boone Bartholomees. "National Power." U.S. Army War College Guide to National Security Policy and Strategy. Strategic Studies Institute, US Army War College, 2014. JSTOR. http://www.jstor.org/stable/resrep12023.12.

Jakob Bund, and Patryk Pawlak. "Minilateralism and Norms in Cyberspace." *European Union Institute for Security Studies*, no. 25 (2017). https://doi.org/10.2815/372100.

Johnathan Cox. "Canadian Forces Transformations and Canada's Way of War in the Twenty-First Century." U.S. Army Command and General Staff College, 2019. https://www.hsdl.org/?view&did=832769.

Jonathan H. Vance. "Tactics without Strategy or Why the Canadian Forces Do Not Campaign." In *The Operational Art: Canadian Perspectives Context and Concepts*. Kingston, Ontario: Canadian Defence Academy Press, 2005.

Judge, David. "The 'Problem' of Representative Government." In *Democratic Incongruities: Representative Democracy in Britain*, edited by David Judge, 107–34. London: Palgrave Macmillan UK, 2014. https://doi.org/10.1057/9781137317292_5.

Julian E. Barnes, and Adam Goldman. "Russia Trying to Stoke U.S. Racial Tensions Before Election, Officials Say - The New York Times," March 10, 2020. https://www.nytimes.com/2020/03/10/us/politics/russian-interference-race.html.

Kathleen Harris. "Canada Loses Its Bid for Seat on UN Security Council | CBC News," June 2020. https://www.cbc.ca/news/politics/united-nations-security-council-canada-1.5615488.

Juneau, Thomas, Philippe Lagassé, and Srdjan Vucetic. *Canadian Defence Policy in Theory and Practice*. Canada and International Affairs. [Place of publication not identified]: Palgrave Macmillan, 2019.

Kim Zetter. "An Unprecedented Look at Stuxnet, the World's First Digital Weapon | WIRED." Accessed March 2, 2021. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

———. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid | WIRED." Accessed March 2, 2021. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

Lee Berthiaume. “Poor IT Support Hurting Canadian Military Operations, Internal Review Finds | CTV News.” Accessed April 13, 2021. https://www.ctvnews.ca/politics/poor-it-support-hurting-canadian-military-operations-internal-review-finds-1.5253148.

Lagassé, Philippe. “Accountability for National Defence.” IRPP, March 2010.

Lindsay Rodman. “You’ve Got It All Backwards: Canadas National Defence Strategy.” In *Canadian Defence Policy in Theory and Practice*. Canada and International Affairs. New York, NY: Palgrave Macmillan, 2019.

Massie, Justin. “Why Canada Goes to War: Explaining Combat Participation in US-Led Coalitions.” *Canadian Journal of Political Science* 52, no. 3 (2019): 575–94. https://doi.org/10.1017/S0008423919000040.

Massie, Justin, and Srdjan Vucetic. “Canadian Strategic Cultures: From Confederation to Trump.” In *Canadian Defence Policy in Theory and Practice*, edited by Thomas Juneau, Philippe Lagassé, and Srdjan Vucetic, 29–44. Cham: Springer International Publishing, 2020. https://doi.org/10.1007/978-3-030-26403-1_3.

Mueller, Robert S. “Report on the Investigation Into Russian Interference In the 2016 Presidential Election.” Washington, D.C.: U.S. DOJ Special Counsel, April 2019.

Nossal, Kim Richard. “The Imperatives of Canada’s Strategic Geography.” In *Canadian Defence Policy in Theory and Practice*, edited by Thomas Juneau, Philippe Lagassé, and Srdjan Vucetic, 11–28. Cham: Springer International Publishing, 2020. https://doi.org/10.1007/978-3-030-26403-1_2.

Organization for Economic Co-operation and Development. “PISA 2018 Results.” Publications-PISA, 2018. https://www.oecd.org/pisa/PISA-results_ENGLISH.png.

Ottawa Citizen. “Shared Services Canada Shows the Sprawling Chaos of Big Government | Ottawa Citizen,” 2016. https://ottawacitizen.com/opinion/editorials/editorial-shared-services-canada-shows-the-sprawling-chaos-of-big-government/.

Pickford, Andrew, and Jeffrey Collins. “Reconsidering Canada’s Strategic Geography:,” n.d., 30.

Potloc. “Potloc - 2019 Election Poll.” Accessed February 2, 2021. https://business.potloc.com/hubfs/federal_election.pdf?hsCtaTracking=7c71b014-b272-49a7-bd61-30154595dee7%7Cfe3ba5b1-35b9-403b-aad8-95097ab9cc84.

Rudner, Martin. “Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge.” *International Journal of Intelligence and CounterIntelligence* 26, no. 3 (September 1, 2013): 453–81. https://doi.org/10.1080/08850607.2013.780552.

Sandal, Ravdeep. “What Are the Actual Extent – and Limits – of the Power of the Prime Minister? – NAOC.” *NATO Association of Canada*. Accessed February 1, 2021. https://natoassociation.ca/what-are-the-actual-extent-and-limits-of-the-power-of-the-prime-minister/.

Sabillon, Regner, Victor Cavaller, and Jeimy Cano. "National Cyber Security Strategies: Global Trends in Cyberspace." *International Journal of Computer Science and Software Engineering* 5, no. 5 (May 2016): 67–81.

Sheehan, Thomas. "Plato: The Allegory of the Cave." Accessed April 11, 2021. https://web.stanford.edu/class/ihum40/cave.pdf.

Stevens, Tim. "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace." *Contemporary Security Policy* 33, no. 1 (April 1, 2012): 148–70. https://doi.org/10.1080/13523260.2012.659597.

Symantec. "Internet Security Threat Report," 2017. https://docs.broadcom.com/doc/istr-22-2017-en.

Tunney, Catharine. "CSIS Chief Calls Commercial Espionage 'the Greatest Threat to Our Prosperity' | CBC News." Accessed February 15, 2021. https://www.cbc.ca/news/politics/david-vigneault-csis-economy-1.4932407.

———. "Foreign Enemies 'increasingly Targeting Canada,' Privy Council Warns New Minister | CBC News." *CBC*, February 2, 2020. https://www.cbc.ca/news/politics/foreign-interference-increasingly-targeting-canada-leblanc-warned-1.5446134.

———. "State Actors Have Done 'significant Harm' to Canadian Companies, Says Head of Spy Agency | CBC News," September 2, 2021. https://www.cbc.ca/news/politics/csis-speech-david-vigneault-1.5906665.

United Kingdom. "Integrated Operating Concept." Ministry of Defence, September 30, 2020. https://www.gov.uk/government/publications/the-integrated-operating-concept-2025.

———. "National Cyber Security Strategy 2016-2021," 2016, 80.

United States. "Audit of Cybersecurity Requirements for Weapon Systems in the Operations and Support Phase of the Department of Defense Acquisition Life Cycle." Audit. Washington, D.C.: Department of Defense, February 10, 2021. https://media.defense.gov/2021/Feb/12/2002581936/-1/-1/1/DODIG-2021-051.PDF.

———. "Canada - The World Factbook." Accessed January 25, 2021. https://www.cia.gov/the-world-factbook/countries/canada/.

———. "Department of Defense Strategy for Operating in Cyberspace," July 2011, 19.

———. "Seven International Cyber Defendants, Including 'Apt41' Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally," September 20, 2020. https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer.

———. "Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities." Audit. Washington, D.C.: Government Accountability Office, October 2018. https://www.gao.gov/products/gao-19-128.

Wark, Wesley. *A Case for Better Governance of Canadian National Security | Centre for International Governance Innovation*. Waterloo, On: Centre for International Governance

Innovation, 2021. https://www.cigionline.org/articles/case-better-governance-canadian-national-security?utm_source=cigi_newsletter&utm_medium=email&utm_campaign=five-things-know-about-hearing-extremism-and-misinformation.

Weintraub, Sidney. "Current State of U.S.-Canada Economic Relations." *American Review of Canadian Studies* 24, no. 4 (December 1, 1994): 473–88. https://doi.org/10.1080/02722019409481778.

"World GDP per Capita Ranking 2020 - StatisticsTimes.Com." Accessed February 15, 2021. http://statisticstimes.com/economy/projected-world-gdp-capita-ranking.php.