National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

BUILDING CYBER OPERATIONS IN THE CANADIAN ARMED FORCES: A BLUEPRINT TO LAY A SOLID FOUNDATION

Major Devon Smibert

JCSP 42

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 42

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 42 – PCEMI 42
MAY 2019

MASTER OF DEFENCE STUDIES – MAÎTRISE EN ÉTUDES DE LA DÉFENSE

BUILDING CYBER OPERATIONS IN THE CANADIAN ARMED FORCES: A BLUEPRINT TO LAY A SOLID FOUNDATION

By Major Devon Smibert

Word Count: 13,981

Nombre de mots : 13,981

TABLE OF CONTENTS

ABSTRACT

The increasing threats to national security interests within the cyber domain led the Canadian Armed Forces (CAF) to announce the creation of a cyber operator occupation in 2017. Standing up a new capability within a military organization is a complex endeavour that is fraught with organizational, political, and human factors that have prevented other capabilities such as Influence Activities (IA) from becoming institutionalized. CAF allies such as the United Kingdom (UK) and United States (US) have nearly a decade of experience and lessons learned from building their own cyber capabilities that could be leveraged to accelerate Canadian capability development. CAF planners will need to put in place the proper foundational elements including healthy budgets, dedicated establishments, modern tools, and a meaningful mission to ensure the continued health and evolution of a new cyber capability.

INTRODUCTION

> *If you have built castles in the air, your work need not be lost; that is where they should be. Now put the foundations under them.*
>
> — Henry David Thoreau, *Walden*

The field of cybersecurity has been rapidly gaining visibility and mind share of people around the world for over a decade with a series of alleged state sponsored cyber-attacks resulting in significant damages to the target and in many cases significant collateral damages. In 2010 it was uncovered that a piece of malicious software, allegedly created by the Americans and Israelis to disrupt the Iranian nuclear program, destroyed approximately one fifth of Iran's nuclear centrifuges and later propagated to computer systems around the world[1]. A clear sign that cybersecurity was going mainstream was in 2014 when vulnerabilities, which previously would be assigned a numeric code such as CVE-2014-0160, were getting regular and sustained coverage by major media outlets given catchy names and the "Heartbleed" vulnerability possibly being the first to receive a flashy logo[2]. Likely partially due to the media coverage received from the provocative vulnerability names, threat actors (also known as advanced persistent threat or APT groups) started to get names like Fancy Bear, Deep Panda, and Charming Kitten[3]. Then for those that do not watch the news, a series of investigations by the Federal Bureau of

Figure 1 - Heartbleed Bug Logo (heartbleed.com)

[1] BBC News, "Stuxnet Worm Hits Iran Nuclear Plant Staff Computers," *BBC News,* 26 September, 2010, www.bbc.com/news/world-middle-east-11414483.
[2] John Biggs, "Heartbleed, The First Security Bug With A Cool Logo," *TechCrunch*, 9 April, 2014, techcrunch.com/2014/04/09/heartbleed-the-first-consumer-grade-exploit/.
[3] Florian Roth, "The Newcomer's Guide to Cyber Threat Actor Naming," *Medium*, 25 March, 2018, medium.com/@cyb3rops/the-newcomers-guide-to-cyber-threat-actor-naming-7428e18ee263.

Investigation (FBI) and other US government agencies accused Russian state actors of interfering with the 2016 Presidential Elections[4]. For any nations or individuals that were previously in denial of the strategic importance of cybersecurity to national security, the debate was over and cybersecurity vaulted to the top of the agenda for several governments and many corporations.

Early in 2017, the Canadian Armed Forces (CAF) announced the creation of a new military occupation by the name of "Cyber Operator" signifying a major step towards building capabilities to operate in the cyber domain. Unfortunately for planners and commanders of this fledgling force, building a fully operational cyber command with all of the tools, equipment, and trained personnel will require some foundational elements to be put in place. These building blocks include streamlined procurement, solutions for talent management, and teaching leaders how to combat adversaries in the cyber domain whose culture and ethics allow the employment of methods and tactics very different from our own. Private industry will compete with recruiters for the same talent but generally offer better compensation and working conditions than the CAF can offer in the near term. Other nations are willing to cross ethical lines that Canadian laws, culture, and values will not allow its forces to cross. Then once people are in place and an operating framework is established, future commanders of this cyber force will need to navigate procurement systems and processes that were recently called "the worst military procurement system in the Western World" [5] to obtain the tools to equip cyber operators

---

[4] CNN, "2016 Presidential Campaign Hacking Fast Facts," *CNN*, 24 November, 2018, www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html.

[5] Richard Shimooka, "Canada Has the Worst Military Procurement System in the Western World," *The Hill Times*, 18 January, 2019, www.hilltimes.com/2019/01/21/canada-worst-military-procurement-system-western-world/184060.

for success. Once these obstacles have been overcome, the CAF will need to learn how to operate within the Law of Armed Conflict, Canadian Law, and International law in an operating environment where seconds and even fractions of seconds can be the difference between winning or losing a battle in cyberspace.

The CAF must take the time to understand the human factors that slowed cyber capability development of our allies and the organizational realities within the CAF that prevented Influence Activities (IA) from becoming institutionalized. A proper foundation laid with healthy budgets, dedicated establishments, modern tools, and a meaningful mission, will pave the way for the ingenuity and perseverance Canadian soldiers are known for to create a cyber operations capability that can punch above its weight class.

RESEARCH LIMITATIONS

It is important to note a few limitations in the research and presentation of materials in this paper that may impact the completeness of information available or information that could be presented. The first major limitation pertains to the sensitivity of the current security posture and capabilities of the CAF. Some information regarding the cyber capabilities of the CAF are classified and therefore not permitted for disclosure in the public domain. In order to minimize the potential for inadvertent disclosure of classified information and impact to the effectiveness of this paper, discussions regarding current capabilities were minimized and restricted to analyzing information that is readily available through public sources. Deeper investigation of specific capabilities, technologies, etc. is likely better suited to national and multinational working groups along with other collaborative classified efforts with allied nations. The overall impact of this limitation is assessed to be low.

The largest limitation for this paper is the requirement to conduct a point in time assessment of the current situation and the cyber operating environment. The rapidly changing cyber threat landscape, capabilities of the CAF, its allies and adversaries required research and assessment of factors leading to a situation where some factors will have changed between the time that research has completed and the paper is published. Research for this paper was therefore time boxed to allow for revisions and a final draft to be generated in order to limit the impact of the changing situation to the validity of analysis and recommendations. The paper also focuses on issues that have a longer time horizon for resolution such as procurement, talent management, and organizational structures which do not change as rapidly as the threat landscape or technologies in use.

The overall impact to the effectiveness of this paper is assessed to be low initially and will increase as time passes beyond the end of 2018 when research was completed.

CANADA'S CONTEMPORARY CYBER OPERATING ENVIRONMENT

Before diving into the details of the challenges that the CAF will face in building its cyber capabilities, one must understand a little about the cyber-threat landscape, current force structure, as well as the Government of Canada cyber strategy and foreign policy.

Canada's Cyber Threat Landscape – Far From a "Fireproof House"

Many Canadians feel that we indeed live in the "fireproof house, far from inflammable materials" envisaged by Raoul Dandruand in his statement to the League of Nations in 1924[6]. Perhaps a reasonable assumption following decades of relative peace, limited direct impacts from terrorism and Canada's geographic location where the Arctic and two oceans isolate it from direct assault by all but our closest ally, the United States.[7] This dated view of threats has left many Canadians reluctant support the building of a large military force or to spend more than about 1% of GDP on defence when conventional military threats would need to cross the Arctic, an ocean, or defeat the US before presenting a serious threat to Canada's security[8]. A view that not only misses the rising tide of cyber-threats but also ignores conventional threats that have been present for decades such as intercontinental ballistic missiles (ICBM). The worldwide crises across healthcare, government, and private sector resulting from a new variant of ransomware called WanaCrypt0r (also known as "WannaCry" in popular media)

---

6 Sarah Katherine Gibson, "Dreams of a 'Fireproof House'," *The Kingston Whig-Standard*, 16 September, 2013, www.thewhig.com/2013/09/16/dreams-of-a-fireproof-house/wcm/795ec0d9-7cc4-80ff-8ac4-5767d5c86049.

7 Victor Platt, "Still the Fire-proof House? An Analysis of Canada's Cyber Security Strategy," *International Journal* 67, no. 1 (Winter 2011-12): 155, http://www.jstor.org/stable/23265971.

8 David McDonough and Tony Battista, "Fortress Canada: How Much of a Military Do We Really Need?" *IPolitics*, April 27, 2016, http://ipolitics.ca/2016/04/27/fortress-canada-how-much-of-a-military-do-we-really-need/.

demonstrated that cyber-attacks know no boundaries. Over 150 countries and more than 230,000 computers were affected by this malware variant that spread like a pandemic around the world in a matter of weeks[9]. The threat of serious impact on Canadian interests is clear as nation states (Russia, China, North Korea, Iran, etc.), terrorists and organized crime now regularly use cyberspace for not only the execution of offensive operations but also to spread propaganda, recruit new members to their cause and gather intelligence −all with minimal risk exposure[10].

CAF Current State

At the time of writing this paper, there are still many key decisions to be made and new announcements regarding Canada's cyber security plans every few months. The CAF has been analysing the need for cyber capabilities for years. As far back as 2009 CAF planners identified the growing need for cyber operations capabilities and even identified cyber operations as a potentially new and distinct Tactical/Enabling Concept[11].

9 Woon Teck, "Cyber Threat Has No Borders," *RSM Global*, May 26, 2017, https://www.rsm.global/insights/rsm-global-blog/cyber-threat-has-no-borders.
[10] Victor Platt, "Still the Fire-proof House? An Analysis of Canada's Cyber Security Strategy," *International Journal* 67, no. 1 (Winter 2011-12): 157, http://www.jstor.org/stable/23265971.
[11] Melanie Bernier and Joanne Treurniet, "CF Cyber Operations in the Future Cyber Environment Concept," December 2009, 10, http://cradpdf.drdc-rddc.gc.ca/PDFS/unc92/p532776.pdf.

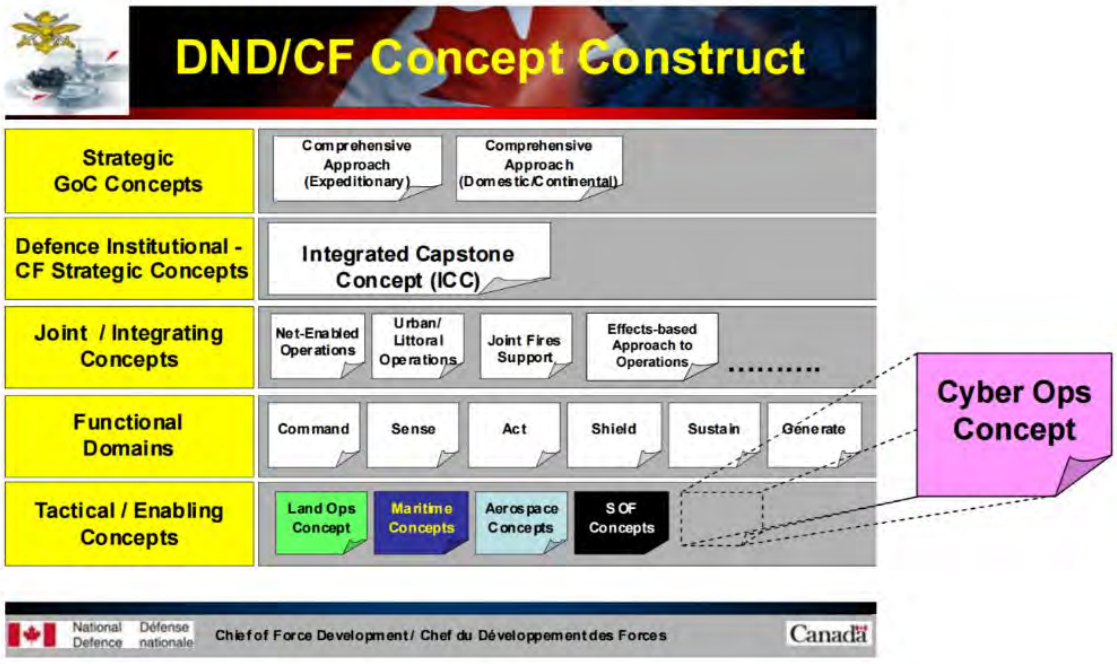

Figure 2 - DND/CF concept construct for cyber ops

As late as Fall 2016 the CAF still had not publicly committed to building a cyber operations capability. This gap in strategy and capability drove experts like the former director of the Canadian Security Intelligence Service (CSIS) to publicly urge the Canadian Government to force generate its own "cyber-warriors"[12] –not just to defend against cyber-attacks but to also have the capability and mandate to go on the offensive when required. Several months later, the Department of National Defence (DND) published the "DND and CAF 2017-18 Departmental Plan" where one of the key risks identified in is the lack of a comprehensive framework for the conduct of cyber operations[13]. CAF commanders and planners are then in a position where cyber security has been cited as a priority within the departmental plan and specifically mentioned in the

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

[13] Department of National Defence, "Department of National Defence and the Canadian Armed Forces 2017-18 Departmental Plan," March 9, 2017, 17, http://www.forces.gc.ca/assets/FORCES_Internet/docs/en/dp-2017-18-_-final_eng.pdf.

Minister of National Defence's mandate letter, but there is still a gap in national cyber security strategy.

The Challenges of Introducing a New Domain to Warfare

The art of war is continually evolving, however, occasionally the introduction of a new technology radically changes with the introduction of an entirely new battlespace or domain. Adaptation of tactics, techniques, and procedures (TTP) in response to the use of technology in innovative ways to gain an advantage over one's adversary is a challenge with which military commanders have had to grapple as long as opposing sides sought to settle their differences in combat. The introduction of new platforms to interact with the battlespace on a different plane tend to have material impacts on the planning and execution of operations. These early attempts to apply new technology in novel ways tend to go through several iterations of change and evolution as commanders invent new ways of employing new capabilities to achieve their desired effects in a battlespace. The example that likely resonates strongest with contemporary commanders is the introduction of airplanes to the battlespace in World War I. Airplanes were actually first employed by the Italians against the Turks in 1911 but later saw widespread adoption and innovation in World War I. Early adopters started first with reconnaissance and then later moved on to carry out ground attacks using machine guns and then to dropping bombs[14]. By the end of World War I, air had been broadly accepted as the third domain (or dimension) of warfare and these three domains remained constant until the recognition of Space as the fourth dimension in 1991 (arguably due to the strategic contributions to the

[14] David MacIsaac, "Air Warfare," *Encyclopedia Britannica*, 18 July, 2016, www.britannica.com/topic/air-warfare.

Persian Gulf War)[15]. The recognition and acceptance of Air and Space as new domains took time to fully mature and be incorporated into doctrine. However, the definition of these domains and conceptual understanding did not appear to have the same challenges faced by areas that have gained greater prominence in recent years such as Cyber, Information, and the various aspects of Influence Activities[16]. Heftye posits that the challenges associated with defining and obtaining wide acceptance of one or more of these concepts stems from the fact that these new planes of operation have no physical existence that can be dominated or defended in ways that conventional commanders are accustomed[17].

Likely in recognition of these challenges, the United States Department of Defense attempted to redefine the traditional domains from Air, Land, Sea, and Space to Physical, Virtual, and Human with the original domains being grouped together under the Physical domain[18]. While this representation did not survive as the accepted definition of domains, it likely triggered a series of working groups and consultations to generate a solution that was more evolutionary than revolutionary.

Physical	Virtual	Human
Air	Cyber	Social
Sea	Information	Moral
Land		Cognitive
Space		

Figure 3 - US temporary redefinition of domains

[15] Nordin Yusof, "Part 2: High Technology Warfare," essay, in *Space Warfare: High-Tech War of the Future Generation* (Penerbit Universiti Teknologi Malaysia, 1999), pp. 11-12.
[16] Erik Heftye, "Multi-Domain Confusion: All Domains Are Not Created Equal," *The Strategy Bridge*, May 2017, https://thestrategybridge.org/the-bridge/2017/5/26/multi-domain-confusion-all-domains-are-not-created-equal.
[17] Erik Heftye, "Multi-Domain Confusion: All Domains Are Not Created Equal," *The Strategy Bridge*, May 2017, https://thestrategybridge.org/the-bridge/2017/5/26/multi-domain-confusion-all-domains-are-not-created-equal.
[18] Joint Chiefs of Staff and Department of Defence (2005), https://apps.dtic.mil/dtic/tr/fulltext/u2/a476464.pdf, 16.

The Physical, Virtual, and Human domains were replaced in 2009 when version 3.0 of the "Capstone Concept for Joint Operations" was published with cyberspace referenced as the fifth domain in addition to the physical domains of Air, Land, Sea, and Space[19]. While this definition seems to have remained constant within US doctrine since 2009[20], The CAF must operate within a multinational context that includes many other strategic allies. As of the summer 2018, NATO has yet to publish standardized definitions related to the cyber domain[21] nor have there been great strides made towards publishing joint cyber doctrine or policies[22]. The US and United Kingdom (UK) have published some unclassified doctrine to share with their allies which is covered in a later discussion regarding how Canada can learn from our allies. Canada's late development of cyber capabilities may prove to be advantageous due to the opportunity to build structures and doctrine from a clean slate and to leverage recent advances in technology such as artificial intelligence (AI) and machine learning (ML). Unfortunately, neither are there any clearly successful operating models that the CAF can emulate. In later sections we will further analyze some of the innovative approaches to talent management and organizational design that that are showing promise among NATO members.

---

[19] Joint Chiefs of Staff and Department of Defense (2009), https://apps.dtic.mil/dtic/tr/fulltext/u2/a493960.pdf, 27.

[20] Erik Heftye, "Multi-Domain Confusion: All Domains Are Not Created Equal," *The Strategy Bridge*, May 2017, https://thestrategybridge.org/the-bridge/2017/5/26/multi-domain-confusion-all-domains-are-not-created-equal.

[21] NATO Cooperative Cyber Defence Centre of Excellence, "Cyber Definitions," *CCDCOE*, April 28, 2015, https://ccdcoe.org/cyber-definitions.html.

[22] Ministry of Defence (UK), "Joint Doctrine Note 1/18: Cyber and Electromagnetic Activities ," *Gov.UK*, Feb. 2018, assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf, 8..

Acquiring Technologies and Systems Could Be Major Obstacles for Cyber Development

Procurement system challenges are probably the easiest to identify and are well-understood by serving members and civilians alike. Canadian media is littered with stories about delayed and cancelled major defence procurement programs[23], but a few have gone a step further to blame the legal foundation of our procurement processes and the large political influence it introduces to the process.[24] Queen's University political scientist Kim Richard Nossal also highlights that unnecessary "Canadianization" of equipment and "Industrial Regional Benefits" result in defence procurement being more focused on wealth redistribution than obtaining the right equipment to support military objectives[25]. For traditional military procurement and capability development, these issues deliver sub-optimal results and inefficiency. In the cyber domain, lengthy timelines and inefficiencies will likely translate to systems and capabilities being obsolete and ineffective before even being deployed.

Highlighting a tangible example of this problem, in May of 2016 DND published a document outlining the project timelines for "The Defensive Cyber Operations Decision Support Project." By following traditional defence procurement processes, the Request for Proposal will not even be released until 2021 and delivery of the project is slated for 2024[26]. From the announcement in 2016 to the delivery in 2024 Moore's law

---

[23] Scott Gilmore, "Military Procurement Is a National Disgrace," *Macleans.ca*, June 24, 2015, http://www.macleans.ca/news/canada/military-procurement-is-a-national-disgrace/.
[24] Charles Davies, "Why Defence Procurement so Often Goes Wrong," *Policy Options*, January 20, 2016, http://policyoptions.irpp.org/magazines/january-2016/why-defence-procurement-so-often-goes-wrong/.
[25] Eric Morse, "Canadian Defence Procurement Still Looks like Massive Case of Charlie Foxtrot," *IPolitics*, January 3, 2017, http://ipolitics.ca/2017/01/03/canadian-defence-procurement-still-looks-like-massive-case-of-charlie-foxtrot/.
[26] Department of National Defence, "Defensive Cyber Operations Decision Support," *Government of Canada*, May 26, 2016, http://www.forces.gc.ca/en/business-defence-acquisition-guide-2016/joint-and-other-systems-401.page.

predicts that computing power will increase by 16 times over that 8 year period which will make the designs and requirements from the start of the project likely irrelevant by the time of delivery. The need to procure equipment and software quickly in order to keep up with the rate of change in the cyber domain was identified in the 2009[27] "Cyber Operations in the Future Cyber Environment Concept" document and has proven even more important in recent years. John Kindervag, the inventor of the "Zero Trust" security model and world-renowned researcher, tells his audiences that he only has six months of cyber security experience. This is a statement that shocks his audience since he has worked in the industry for over 30 years, but he makes this argument because the field changes so rapidly that the tools and techniques that worked even just three years earlier become nearly obsolete during that time frame[28].

In June of 2018, DND published the "Defence Investment Plan" which outlines several promising indicators of intent to change the way that the CAF develops and procures new capabilities.[29] The plan calls outlines changes to low risk, low complexity projects that reduces the number of steps required to approve and execute these projects which should help more small and medium sized businesses to propose solutions to defence problems.

Even with these improvements, cyber operations commanders will likely need to have the ability to expedite and perhaps even bypass traditional procurement processes to

---

[27] Melanie Bernier and Joanne Treurniet, "CF Cyber Operations in the Future Cyber Environment Concept," December 2009, 23, http://cradpdf.drdc-rddc.gc.ca/PDFS/unc92/p532776.pdf.
[28] John Kindervag, "Zero Trust Networks" (lecture, Zero Trust Networks, Calgary Marriott, Calgary, April 19, 2017).
[29] Department of National Defence, "Defence Investment Plan 2018: Ensuring the Canadian Armed Forces Is Well-Equipped and Well-Supported," *Government of Canada*, June 2018, www.canada.ca/en/department-national-defence/corporate/reports-publications/defence-investment-plan-2018.html?utm_campaign=not-applicable&utm_medium=vanity-url&utm_source=canada-ca_Defence-Investment-Plan.

keep pace with the evolving infrastructure and toolsets required to be effective in the cyber domain. Organizations around the world are in a cyber arms race as nation states, and organized crime groups continue to reap massive profits and gains in their political and diplomatic objectives. Cyber-crime alone is expected to have cost the world over $6 trillion by 2021[30] with 2018 revenues estimated at over $1.5 trillion in 2018[31] which means that adversaries in the cyber domain have a lot of resources to invest in the development of new cyber weapons. As noted in Chapter 1, even conventional warfare capabilities with lifecycles measured in decades suffer from over-"Canadianization" of solutions and attempts to build versus buy off the shelf. The global cybersecurity industry spend on cybersecurity is expected to reach $124 billion[32] (USD) whereas the Canadian government has earmarked $500 million over 5 years spread across several departments. Attempting to make do with dated tools or trying to develop in-house tools with the limited resources available should quickly be eliminated as viable solutions. Canadian leaders and commanders will need to have the flexibility to select, procure, and deploy new tools in months rather than years to be effective.

Recommendation #1 – Technology acquisition and implementation enabling cyber capability development and support must be completed in months, not years.

---

[30] Steve Morgan, "Cybercrime Damages Expected to Cost the World $6 Trillion by 2021," *CSO Online*, August 22, 2016, http://www.csoonline.com/article/3110467/security/cybercrime-damages-expected-to-cost-the-world-6-trillion-by-2021.html.

[31] Nick Ismail, "Global Cybercrime Economy Generates over $1.5 Trillion," *Information Age*, 20 June, 2018, www.information-age.com/global-cybercrime-economy-generates-over-1-5tn-according-to-new-study-123471631/.

[32] Stu Sjouwerman, "Global Cyber Security Spending to Top $114bn in 2018, Says Gartner," *KnowBe4*, 16 Aug. 2018, blog.knowbe4.com/global-cyber-security-spending-to-top-114bn-in-2018-says-gartner.

OVERCOMING THE STRATEGIC HEADWINDS TO INSTITUTIONALIZING CYBER CAPABILITIES

In recognition of the changing cybersecurity threat landscape, the Government of Canada recognized that it needed to have a plan for how to protect Canadians from this rapidly emerging threat vector and published "Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada" in 2010[33]. This spurred a series of investments in the Communications Security Establishment Canada (CSEC), law enforcement, and public awareness campaigns but there was a large gap in strategic direction from 2010 to the 2018 publication of "National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age"[34] which will take time for departments and agencies to interpret and implement. In an analysis of Canada's 2010 Cyber Security Strategy, Victor Platt highlights that the focus of the document is very inwardly focused with strong emphasis placed on building detection and response capabilities within Law Enforcement and government agencies such as CSEC[35]. These were logical first steps to gain visibility, guidance, and assistance in the protection of Canadian Government information and infrastructure, but defensive actions are not always sufficient to deter or defeat an adversary. Sometimes a commander needs to take the fight to an adversary which requires the ability to carry out offensive operations which has traditionally been the domain of a nation's armed forces.

---

[33] Public Safety Canada, "National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age," June 12, 2018, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx.
[34] Ibid.
[35] Victor Platt, "Still the Fire-proof House? An Analysis of Canada's Cyber Security Strategy," *International Journal* 67, no. 1 (Winter 2011-12): 164-165, http://www.jstor.org/stable/23265971.

The Need for Clear Strategic Direction on Cyber Security

Announcing new offensive capabilities for any armed forces is a politically charged action that it not to be taken lightly. This argument has become increasingly palatable for citizens around the world to accept as technology is being leveraged more every day for the automation and optimization of everything from home thermostats to pipelines and nuclear power plants. As a result, cyber-attacks are rapidly approaching or even overtaking kinetic attacks in their potential for destruction[36]. A quick review of the CSEC mandate reveals that offensive cyber operations in support of military operations do not fall within the agency's mandate[37] leaving a large gap in Canada's cyber defence capabilities. "Support[ing] the Minister of Public Safety and Emergency Preparedness in a review of existing measures to protect Canadians and our critical infrastructure from cyber-threats" is among the priorities set for Minister Harjit Sajjan but was not included in the DND Mandate letter of 2015[38] and was subsequently included in the "Defence Investment Plan 2018: Ensuring the Canadian Armed Forces Is Well-Equipped and Well-Supported"[39] published in June 2018. In the absence of a clear mandate, the CAF "leaned forward" with the inclusion of plans to establish a cyber capability in its 2017-18

---

[36] Alex Boutilier, "Former Electronic Spy Chief Urges Ottawa to Prepare for 'cyber War'," *Thestar.com*, September 01, 2016, https://www.thestar.com/news/canada/2016/09/01/former-electronic-spy-chief-urges-ottawa-to-prepare-for-cyber-war.html.

[37] Communications Security Establishment, "Communications Security Establishment: What We Do and Why We Do It," *Communications Security Establishment*, March 08, 2017, https://www.cse-cst.gc.ca/en/inside-interieur/what-nos.

[38] Rt. Hon. Justin Trudeau, P.C, M.P., "Minister of National Defence Mandate Letter," *Prime Minister of Canada*, November 13, 2015, http://pm.gc.ca/eng/minister-national-defence-mandate-letter.

[39] Department of National Defence, "Defence Investment Plan 2018: Ensuring the Canadian Armed Forces Is Well-Equipped and Well-Supported," *Government of Canada*, June 2018, www.canada.ca/en/department-national-defence/corporate/reports-publications/defence-investment-plan-2018.html?utm_campaign=not-applicable&utm_medium=vanity-url&utm_source=canada-ca_Defence-Investment-Plan.

departmental plan.[40] The new Cyber Operator occupation was created, but the exact role and how it will be operationalized remains to be defined.

In addition to the cyber capability gaps identified by Platt, he also explains how the 2010 Canadian Cyber Security Strategy focused on intelligence, national law enforcement, and incident response, failing to take into consideration the complexities of diplomatic relations, the borderless nature of cyber threats[41]. The limited discussion regarding international diplomatic relations and cooperation does not appear to have translated into concrete actions[42] and Public Safety Canada's summary of progress against the "Action Plan 2010-2015 for Canada's Cyber Security Strategy" shows little concrete action towards ensuring that Canada is prepared to defend against modern cyber threats[43]. The 2018 National Cyber Security Strategy shows recognition that action is required and commits to an action plan that should help to gain momentum in building the capabilities required to defend Canada's interest.[44] It builds on the previous strategy and most importantly allocates more than $500 million in funding over a five-year period to address key gaps in structure, coordination and support for effective cyber defence of Canada's interests. Some of these initiatives have already started to be implemented such as the establishment of the Canadian Centre for Cyber Security in October of 2018[45] and

---

[40] Department of National Defence, "Department of National Defence and the Canadian Armed Forces 2017-18 Departmental Plan," March 2017, 41, http://www.forces.gc.ca/assets/FORCES_Internet/docs/en/dp-2017-18-_-final_eng.pdf.
[41] Victor Platt, "Still the Fire-proof House? An Analysis of Canada's Cyber Security Strategy," *International Journal* 67, no. 1 (Winter 2011-12): 155, http://www.jstor.org/stable/23265971.
[42] Ibid, 165-166.
[43] Public Safety Canada, "Action Plan 2010-2015 for Canada's Cyber Security Strategy," December 2015, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/index-en.aspx.
[44] Public Safety Canada, "National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age," June 2018, www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx.
[45] Communications Security Establishment, "Canadian Centre for Cyber Security," 16 Oct. 2018, cse-cst.gc.ca/en/backgrounder-fiche-information.

expansion of the scope and reach of services delivered by the Canadian Cyber Incident Response Centre (CCIRC). These are important first steps, but the true measure of effectiveness for these investments will be the level of consumption by the public and private sectors and tangible improvements in the overall security posture of our nation over time.

Seeking Help from Canadians: 2016 Public Consultation on Cyber Security

Turning to industry, academia, and other government agencies in 2016 for input, Public Safety Canada led a public consultation on cyber security to inform and guide the development of an updated cyber security strategy and support other planning. Unfortunately for CAF planners seeking support and guidance, the report generated from contributions to the public review process makes no mention of military or defence capabilities but a common theme identified across participants was that Canada should be more proactive and perhaps have more offensive capabilities moving forward[46]. The path that Public Safety Canada is currently taking for creating a new Canadian Cyber Security strategy appears to be inwardly focused rather than considering opportunities to learn and collaborate with allies and not learning from failed and stalled initiatives over the last 15 years. The report seems to rehash many of the same priorities identified in 2010 except for the notable absence of goals to improve military capabilities which were present in the original 2010 strategy. In the table below, the first column in the table below includes excerpts from “Action Plan 2010-2015 for Canada's Cyber Security Strategy” [47], the

[46] Public Safety Canada, “CYBER REVIEW CONSULTATIONS REPORT,” January 17, 2017, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2017-cybr-rvw-cnslttns-rprt/2017-cybr-rvw-cnslttns-rprt-en.pdf.

[47] Public Safety Canada, "Action Plan 2010-2015 for Canada's Cyber Security Strategy," December 03, 2015, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/index-en.aspx.

second column in the table below includes excerpts from the "CYBER REVIEW CONSULTATIONS REPORT" [48]. A row by row analysis of the recommendations from 2010 unfortunately reinforce that the problem space is fairly well understood, but we appear to lack the ability to deliver on the commitments for improvement being made.

Table 1 – Analysis of 2016 Cyber Security Public Consultation against the 201 Cyber Security Strategy Action Plan

2010 Strategic Pillars and corresponding Actions	2016 Public Consultation Key Findings and Excerpts	Analysis
Helping Canadians to be secure online 7 initiatives relating to public education and awareness where 2 are completed and the rest are ongoing	Increase public education and awareness; • "Participants recommended that public education and awareness be developed to improve cyber security in Canada" "awareness of the importance of cyber security and understanding of basic security measures is lacking among the general public"	Little to no progress appears to have been made in this area as the report recommends the creation of education and awareness programs that have been in progress since 2011 and basic public awareness is still assessed to be lacking.
Partnering to secure vital cyber systems outside the federal Government Invest in CCIRC's technical capability, through training, analytical systems and processes, automation and technology. (ongoing)	Improve training for cyber security professionals and law enforcement Improved training for… protect[ing] critical infrastructure. Improved public education and awareness Improved training for Law enforcement in cyber*	There is no direct mapping between these key points, but some overlap exists with past initiatives. The 2010 action plan included initiatives to collaborate with industry to secure critical infrastructure, improved public education in awareness was repeated, and Law Enforcement was singled out while the military was overlooked.
Securing Government systems Consolidate the Government's information technology security architecture, in order to improve the security of Government networks. (Completed)	Develop and promote established standards, best practices, certification and legislation Developing standards, best practices, certification, and legislation	A 2002 report from the Auditor General of Canada recommended that cyber security standards be developed for implementation[49]. Considerable resources have been invested in standards already by

[48] Public Safety Canada, "CYBER REVIEW CONSULTATIONS REPORT," January 17, 2017, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2017-cybr-rvw-cnslttns-rprt/2017-cybr-rvw-cnslttns-rprt-en.pdf.

[49] Auditor General of Canada, "2002 April Report of the Auditor General of Canada," *Government of Canada*, April 16, 2002, http://www.oag-bvg.gc.ca/internet/English/parl_oag_200204_03_e_12376.html.

Develop and implement of new security standards for the procurement of information technology products and services for the Government. (completed) Develop enterprise IT security architecture designs to ensure basic security building blocks are instilled as Government IT infrastructure is renewed. (ongoing)		CSEC[50]. The fact that a key finding from the public consultation report is to develop standards and best practices demonstrates that the standards already being developed by CSEC are not widely perceived to be adding value. UK, Italy, Japan, the Republic of Korea, Australia and the EU—are standardizing on the NIST Framework[51] Shared Services Canada has made little progress in transformation and public account of progress states they have only established a RACI for security responsibilities[52].
-	4. Increase funding and resources for all areas of cyber security.	

The report reiterates the need for public education and awareness to protect critical infrastructure, and (new to the 2016 report) the need to invest in strengthening law enforcement capabilities on cyber investigations and enforcement. The recommendations also appear to be leaning towards the development of Canadian standards and best practices (echoing a 2002 recommendation from the Auditor General of Canada[53]) even though CSEC has been investing in resources developing standards for many years. The recommendation to develop new standards demonstrates a common theme of a desire to "Canadianize" solutions rather than leverage the efforts and lessons

[50] Communications Security Establishment Canada, "ITS Advice and Guidance," November 28, 2016, https://www.cse-cst.gc.ca/en/group-groupe/its-advice-and-guidance.
[51] Scott J. Shackelford, PhD, Scott Russell, and Jeffrey Haut, "BOTTOMS UP: A COMPARISON OF "VOLUNTARY" CYBERSECURITY FRAMEWORKS," February 16, 2016, 34-37, https://www.nist.gov/sites/default/files/documents/2017/02/14/20160216_scott_j._shackelford_scott_russell_jeffrey_haut.pdf.
[52] Howard Solomon, "Shared Services Canada Defends Progress in Merging IT Systems, Vows to Do Better," *IT World Canada*, October 13, 2016, http://www.itworldcanada.com/article/shared-services-canada-defends-progress-in-merging-it-systems-vows-to-do-better/387384.
[53] Auditor General of Canada, "2002 April Report of the Auditor General of Canada," *Government of Canada*, April 16, 2002, http://www.oag-bvg.gc.ca/internet/English/parl_oag_200204_03_e_12376.html.

learned from larger organizations and allies as discussed in the procurement section of this paper. With the limited resources available for building Canada's cybersecurity capabilities, it is the opinion of the author that we should leverage the significant investments made by the (US) National Institute of Standards and Technology (NIST) in developing standards and frameworks that are widely being adopted by organizations in both he public and private sector. Canada is not alone in developing our own standards that appear to be largely based off of the NIST publications. Many of our allies (and other nations) including UK, Italy, Japan, the Republic of Korea, Australia and the EU appear to be creating their own national standards that have considerable overlap or similarities with the NIST publications[54].

Recommendation #2 – Resist the urge to "Canadianize" – leverage established standards and frameworks versus developing our own.

In order to move forward in building a capable, effective, and relevant cyber capability, CAF leaders need a clear mandate to defend the interests of Canadians and the funding to execute on that mandate. Before getting too far down the path of implementation, DND and departments of the Government of Canada should consider looking to allies and perhaps even adversaries to better understand what is and isn't working for them before committing to any given approach (see the section titled "Looking to Canada's Allies for Lessons Learned" for examples). Canada's modest budgets will require leaders to learn from the lessons of others and leverage the tools, standards, and best practices proven in operations. The release of the much-anticipated

[54] Scott J. Shackelford, PhD, Scott Russell, and Jeffrey Haut, "BOTTOMS UP: A COMPARISON OF ″VOLUNTARY″ CYBERSECURITY FRAMEWORKS," February 16, 2016, 34-37, https://www.nist.gov/sites/default/files/documents/2017/02/14/20160216_scott_j._shackelford_scott_russell_jeffrey_haut.pdf.

Defence Policy Review (DPR) and development of a new national Cyber Security Strategy should provides much greater clarity for CAF commanders on parameters for operationalizing new cyber capabilities, however many have doubts that the DPR will drive the level of changes required to adequately protect Canada's national interests[55].

[55] Marie-Danielle Smith, "Sajjan Faces 'two Burdens': Military, Angered by His Boast, Also Expects His Defence Policy Review to 'fall Short'," *National Post*, May 3, 2017, http://news.nationalpost.com/news/canada/canadian-politics/sajjan-faces-two-burdens-military-angered-by-his-boast-also-expects-his-defence-policy-review-to-fall-short.

CAF ORGANIZATIONAL STRUCTURES – A FROG IN BOILING WATER?

Military organizations have evolved to be organized and operate in very structured hierarchies that enable commanders to mobilize resources quickly, often with limited information about the situation, in order to achieve their commander's intent. This strength can also turn out to be a weakness when military organizations are faced with the introduction of new technologies to the battlespace that may require changes to established doctrine and even changes to organizational structures. Cohen and Gooch describe the repeated failure to adapt across generations of military commanders as "Collective Incompetence and the 'Military Mind'" citing repeated failures by military commanders to change their strategy or tactics to leverage technological advancements on the battlefield as far back as 1302[56]. The introduction of the cyber domain to the battlespace presents contemporary commanders with several complex structural and organizational challenges to overcome that will require change and adaptation at an unprecedented rate. Can CAF commanders and planners learn from the lessons observed over the last decade around the globe in building cyber capabilities and from the CAF failure to institutionalize Influence Activities? In the following sections we will explore these questions in greater detail in order to identify key recommendations for CAF planners to consider.

Cyber Capability Development Direction in Canada's Defence Policy

Canada's Defence Policy – *Strong, Secure, Engaged* – identifies the need to invest in several capabilities to align with changing threats and aging infrastructure; however, most of the discussion focused on capital investments to acquire equipment and

[56] Eliot A. Cohen and John Gooch, Military Misfortunes: the Anatomy of Failure in War (Free Press, 2012), 5-16.

technology[57]. While some of the capital funding has been allocated to support the development of cyber capabilities, the majority of funding will go towards large capital acquisitions such as ships, planes, armoured vehicles etc. and upgrades to existing assets. It is important to note that the CAF will increase the Regular Force personnel by 3,500 (to a total of 71,500) which will "allow us to expand in important areas such [as] space and cyber, intelligence and targeting."[58] There is an interesting inconsistency between pages 19 and 33 of the policy document where the 3,500 Regular Force increase is directly linked to expansion in space, cyber, intelligence and targeting whereas the aggregate increase including the 1,500 personnel increase to the Reserve only mentions support to military operations in areas such as intelligence and procurement[59]. Then later in the document the Reserves are named again as taking on the role of Cyber Operators on page 68[60]. These types of directional statements along with more prescriptive guidance regarding the future force employment of units have created a lot of debate and conversation within the CAF. Of particular interest to the Primary Reserve (PRes) are the new roles assigned to the reserves to provide "full-time capability … through part-time service" which are starting to be referred to as "mission tasks" within parts of the PRes:

> Assign Reserve Force units and formations new roles that provide full-time capability to the Canadian Armed Forces through part-time service, including:
>
> - Light Urban Search and Rescue;

[57] Department of National Defence, "Canada's Defence Policy – Strong, Secure, Engaged," Department of National Defence, 2017, http://dgpaapp.forces.gc.ca/en/canada-defence-policy/docs/canada-defence-policy-report.pdf, 33-41.
[58] Department of National Defence, "Canada's Defence Policy – Strong, Secure, Engaged," Department of National Defence, 2017, http://dgpaapp.forces.gc.ca/en/canada-defence-policy/docs/canada-defence-policy-report.pdf, 33.
[59] Ibid, 19.
[60] Ibid, 68.

- Chemical, Biological, Radiological and Nuclear Defence;
- Combat capabilities such as direct fire, mortar and pioneer platoons;
- Cyber Operators;
- Intelligence Operators;
- Naval Security Teams; and
- Linguists.[61]

For the purposes of this paper, we will focus only on the Cyber Operators portion of this direction from the 2017 Defence Policy; however, it is important to be aware of the other changes and realignment of resources to new roles that are happening concurrently with the cyber role creation and capability development. The salient point that we will explore later in this paper is that the PRes has been clearly assigned a task to the deliver full-time capability of Cyber Operators through part-time service. The key questions that CAF planners will need to answer are:

- How do we structure and organize this new cyber force?
- What lessons can we learn from our allies?
- How can we avoid the "failure to launch" that is still preventing effective institutionalization of Influence Activities in the CAF?
- How can we deliver full-time capabilities through part-time service?

[61] Department of National Defence, "Canada's Defence Policy – Strong, Secure, Engaged," Department of National Defence, 2017, http://dgpaapp.forces.gc.ca/en/canada-defence-policy/docs/canada-defence-policy-report.pdf, 69.

The Role of CAF Structures and Budgets in Shaping the Future Cyber Force

As noted above, military organizations tend to be very hierarchical and bound by carefully defined orders of battle (ORBATs) with specific equipment and manning entitlements that drive most standard resource allocations to units. These ORBATs are organized in a hierarchical manner within defined "establishments" where each position within an establishment will have parameters for the maximum and minimum rank, special qualifications and other criteria in order to deliver capabilities to the CAF within pre-defined resource allocations. The composition of these establishments is extremely important for individual units because every member of the CAF must occupy a position in an establishment for which that member meets the rank and qualification requirements (with some exceptions). This is becoming increasingly relevant to Army Reserve units that have now filled or are have nearly filled all open positions in their establishment thanks to recent changes to the recruiting and enrolment processes introduced in April 2017[62]. In a paper titled "The Canadian Armed Forces: The Role of the Reserves," Coronne McDonald describes how the Reserve Establishment was being restructured in the late 90s to reduce the personnel levels from 24,000 to 18,500 in order to meet budget and capability requirements set by the Government of Canada at that time[63]. Just as the Land Force Reserve Restructure called for an assessment of Reserve unit viability, operational requirements, and ability to force generate[64], *Strong Secure Engaged* has triggered a similar reassessment of CAF unit roles, capabilities, and relevance.

---

[62] David Pugliese, "Canadian Army Cuts Enrollment Time for Reserves – New Process to Take Just Weeks," Ottawa Citizen, April 4, 2017, https://ottawacitizen.com/news/national/defence-watch/canadian-army-cuts-enrollment-time-for-reserves-new-process-to-take-just-weeks.
[63] Corinne MacDonald, "THE CANADIAN ARMED FORCES: THE ROLE OF THE RESERVES," Government of Canada publications, November 29, 1999, http://publications.gc.ca/collections/Collection-R/LoPBdP/BP/prb9911-e.htm#b. Militiatxt.
[64] Ibid.

This is important to understand because military commanders are given a series of assigned tasks, constraints, restraints, and then assigned budgets, equipment, and personnel in order to fulfill those tasks. In 2018, a comprehensive review of all establishments, tasks, unit viability and relevance was undertaken named the Force Mix Structure Design (FMSD)[65]. Results of this analysis will be used to reallocate positions, equipment, budget, and tasks across the CAF in order to better align resources with the stated desired future state. CAF planners will need to deal with the inevitable conflict and tension that will materialize across several levels of command that Harvard Business Review (HBR) identifies as a significant contributing factor to the failure of over 70% of transformation efforts[66]. This resistance to reallocation of resources is not unique to military organizations, but likely more pronounced than in the private sector, particularly in fields with high rates of innovation. After getting over the initial shock to the system of transformational changes on the horizon, CAF planners may want to consider a more regular and deliberate reallocation of resources on an annual basis similar to the manner that top performing organizations carry out in the private sector to achieve better results[67]. DND, much like many public and private sector organizations, do not follow a "Zero Based Budgeting" (ZBB) approach and typically build budgets based on a review of historical expenditures, forecast growth, with some amount set aside for new

---

[65] Department of National Defence, "Execution - Defence Plan 2018-2023," Canada.ca (Innovation, Science and Economic Development Canada, May 17, 2018), https://www.canada.ca/en/department-national-defence/corporate/reports-publications/defence-plan-2018-2023/execution.html.

[66] Ron Carucci, "Organizations Can't Change If Leaders Can't Change with Them," Harvard Business Review, October 24, 2016, https://hbr.org/2016/10/organizations-cant-change-if-leaders-cant-change-with-them.

[67] Stephen Hall, Dan Lovallo, and Reinier Musters, "How to Put Your Money Where Your Strategy Is," McKinsey & Company, March 2012, https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-to-put-your-money-where-your-strategy-is.

investments[68]. This often leads to a gradual bloat of operating budgets over time that ends up displacing opportunities for investment and innovation due to teams and initiatives competing for a finite pool of resources. A ZBB approach reinforces a results-oriented culture where success is rewarded with additional resources to innovate and thrive whereas under-performing initiatives (and individuals) are eliminated over time. At the close of 2018, the CAF did not have a continuous feedback loop in place to measure and report on the effectiveness of units and individuals that enables continuous reallocation of resources to reward success, invest in strategic capabilities, and eliminate waste and spend on capabilities that are no longer relevant. The CAF is increasingly using a suite of systems developed by the Military Command Software Centre (MCSC) in order to reduce the administrative burden of tracking tasks, qualifications, and other key performance indicators (KPI) across the forces[69]. As with the adoption of any new tool or technology, formations and individual units have seen varying levels of adoption and success with two of the key components that provide some of the most valuable information to senior commanders. CF Tasks, Planning and Operations (CFTPO) and Monitor Military Administrative Support System (MASS) together have the ability to paint a picture of how effective a unit is through reporting against a series of periodic combat readiness qualifications and the level and types of activities or tasks its members complete. The intent to leverage metrics from these systems as part of the FMSD to make informed decisions regarding the reallocation of positions and budget was communicated to

---

[68] Shaun Callaghan, Kyle Hawke, and Carey Mignerey, "Five Myths (and Realities) about Zero-Based Budgeting," McKinsey & Company, October 2014, https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/five-myths-and-realities-about-zero-based-budgeting.
[69] Chris McGill, "Benefits of New CAF Software," Trident Newspaper, March 13, 2018, https://tridentnewspaper.com/benefits-new-caf-software/.

commanders across the CAF in 2018, however this is a one-time effort as part of a transformational program. One of the challenges associated with large transformational activities is that the first iteration will almost certainly not be perfect and further refinement and iteration of analysis and change will be required over time. Furthermore, once units realize that the metrics generated from CFTPO and Monitor MASS will be used for annual reallocation of positions and budgets the unit adoption of these solutions will approach 100% and then even better decisions can be made each subsequent year.

Recommendation #3 – Create an annual feedback loop into budget and establishment planning to enable adaptation of capabilities to match the changing contemporary operating environment

At the close of 2018 no dedicated cyber units have been created and the Royal Canadian Corps of Signals appears to have been assigned the lead for training new Cyber Operators. The trade is open to members of the Air Force, Army, and Navy with several courses being run out of the Canadian Forces School of Communications and Electronics (CFSCE) in Kingston, Ontario[70]. This means that CAF planners have yet to announce several key decisions regarding the target structure of Canada's cyber capability. These decisions will undoubtedly have significant impacts on the near-term trajectory and velocity of capability development, but planners are also likely looking at the longer-term implications for recruitment, retention, and sustainability of cyber capabilities over a longer horizon. In the following sections, we will review approaches taken by some NATO allies and contrast those against other nations such as Russia, China, and North

[70] Department of National Defence, "Cyber Operator - Job Description," Canada.ca, June 18, 2018, https://www.canada.ca/en/department-national-defence/services/caf-jobs/career-options/fields-work/other-specialty-occupations/cyber-operator.html.

Korea. Within this context, we can propose a few possible courses of action and assess the advantages and disadvantages of each.

Looking to Canada's Allies for Lessons Learned

Canada is relatively late to the process of building military capabilities in the cyber domain when compared to many NATO members and particularly when compared against non-NATO nations such as China, Russia, or North Korea that have over a decade of experience[71]. The CAF is fortunate that one of Canada's closest allies, The United Kingdom, recently published a joint doctrine note in February of 2018 titled "Joint Doctrine Note 1/1: Cyber and Electromagnetic Activities"[72] clarifying the need for, role of, and integration of cyber capabilities with traditional military capabilities. Of particular interest for CAF planners should be that the Ministry of Defence (MoD) has highlighted many of the challenges and pitfalls associated with integrating and coordinating cyber capabilities with traditional Electromagnetic effects in the battlespace. The MoD has named this new coordinated capability as Cyber and Electromagnetic Activities (CEMA) which CAF planners should review and understand before proceeding too far along its planning. Current challenges of keeping cyber, electromagnetic effects, and failure to coordinate with non CEMA activities such as Influence Activities (IA) and kinetic effects is that each of these disciplines relies on communication mediums and their effects on the battlespace in order to achieve their respective desired outcomes. To

[71] NATO, "The History of Cyber Attacks - a Timeline," NATO, 2013, https://www.nato.int/docu/review/2013/cyber/timeline/en/index.htm.
[72] Ministry of Defence (UK), "Joint Doctrine Note 1/18: Cyber and Electromagnetic Activities," Gov.UK, February 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf.

illustrate the importance of this coordination, the doctrine note describes this fictional scenario that would likely resonate with members of each of the affected components:

> At the tactical level, a planned operation requires phone use to be blocked in the operations area. This is achieved by an electronic warfare operation jamming the broadcast tower. Due to insufficient synchronisation and coordination, it was not appreciated that jamming the tower also stopped an ongoing strategic cyber operation being conducted by partners across government.[73]

In the Joint Doctrine Note, the MoD outlines an iterative approach to capability development and integration with the established domains of cyber and electromagnetic activities in order to set proper expectations for stakeholders up front and to avoid inaction resulting from lengthy analysis. As this model assumes that cyber has already been established as a capability that needs to be integrated and coordinated with electromagnetic effects and Influence Activities, the CAF may have an opportunity to design its cyber capabilities in such a way that moves rapidly through the first stage of development due to funding and support that have already been identified for cyber capability development in Canada. The four steps from the doctrine note can be summarized as follows:

1. **Level 1: initial step**. Cyber and electromagnetic activities are independent, with funding and personnel fully allocated and existing doctrine may leave commanders and soldiers entrenched in existing ways of operating.

[73] Ministry of Defence (UK), "Joint Doctrine Note 1/18: Cyber and Electromagnetic Activities," Gov.UK, February 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf.

2. **Level 2: evolving step**. This phase shows dramatic increase in synchronization and coordination that does not involve changing force structures or funding sources.
3. **Level 3: integrated step**. Refers to Joint Concept Note (JCN) 1/17 for more details and illustrates a blurring of boundaries between the CEMA oversight and coordination with the actual cyber and electromagnetic activities (EMA)[74]. JCN 1/17 states that CEMA will require centralized command and control with decentralized execution "where execution authority is delegated to the point of best understanding for decision-making."[75]
4. **Level 4: ubiquitous step**. Essentially shows a further blurring of responsibilities between CEMA, cyber, and EMA to the point where the "coordination lines" shown for the previous steps have been removed and the reader is likely meant to interpret this as these organizations ceasing to exist independent from each other[76].

While both the JDN 1/18 and JCN 1/17 avoid explicitly recommending that funding, organizational structures, rules of engagement etc. be realigned under a single command, this appears to be the implicit recommendation of both documents.

---

[74] Ministry of Defence (UK), "Joint Doctrine Note 1/18: Cyber and Electromagnetic Activities," Gov.UK, February 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf, 25.
[75] Ministry of Defence (MoD) Development, Concepts and Doctrine Centre, "Joint Concept Note 1/17 Future Force Concept," Joint Concept Note 1/17 Future Force Concept, 2017, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643061/concepts_uk_future_force_concept_jcn_1_17.pdf, 21.
[76] Ministry of Defence (UK), "Joint Doctrine Note 1/18: Cyber and Electromagnetic Activities," Gov.UK, February 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf, 25.

Organizational structures and funding models tend to create heated debates, and even political conflict, when dealing with the amalgamation, re-role, or disbandment of established units. This is because in order to reallocate resources to achieve new mission tasks and strategic imperatives, the status quo for some units must be disrupted and those resources need to be taken away from existing units and organizations that are theoretically already resource constrained. CAF planners will need to think carefully about how to strike a balance between leveraging people, capabilities, and organizations that are already established against the possibility of creating new cyber or CEMA units that can start fresh without the organizational and doctrinal baggage associated with leveraging existing structures.

LCdr R.A.D Chouinard-Prévost completed a detailed analysis of the organizational options for the CAF cyber capability development and arrived at similar conclusions – that the CAF should create a centralized cyber command in order to successfully transition from level 2 to level 3 in the model outlined above[77]. Below are the pictorial illustrations of the two options proposed by LCdr Chouinard-Prévost:

[77] R.A.D. Chouinard-Prévost, "CYBER CAPABILITY DEVELOPMENT: CONSIDERATIONS FOR OPTIMIZING ORGANIZATIONAL FORM IN THE DND/CAF," Canadian Forces College, 2017, https://www.cfc.forces.gc.ca/259/290/402/305/chouinard-prevost.pdf.

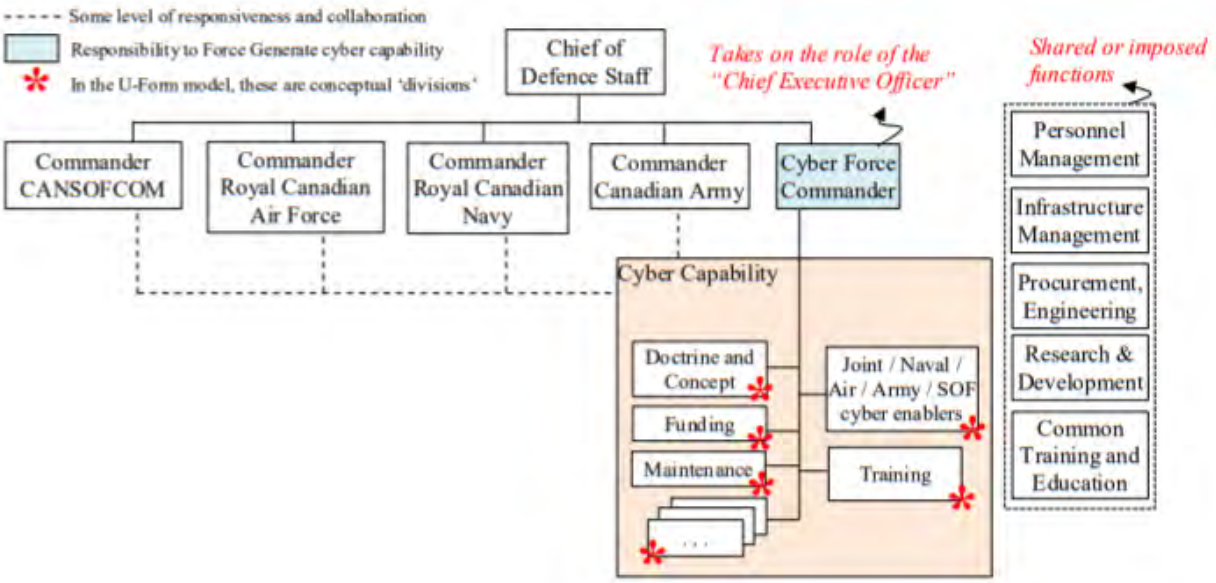

Figure 4 - "U" Form (Centralized) Cyber Structure

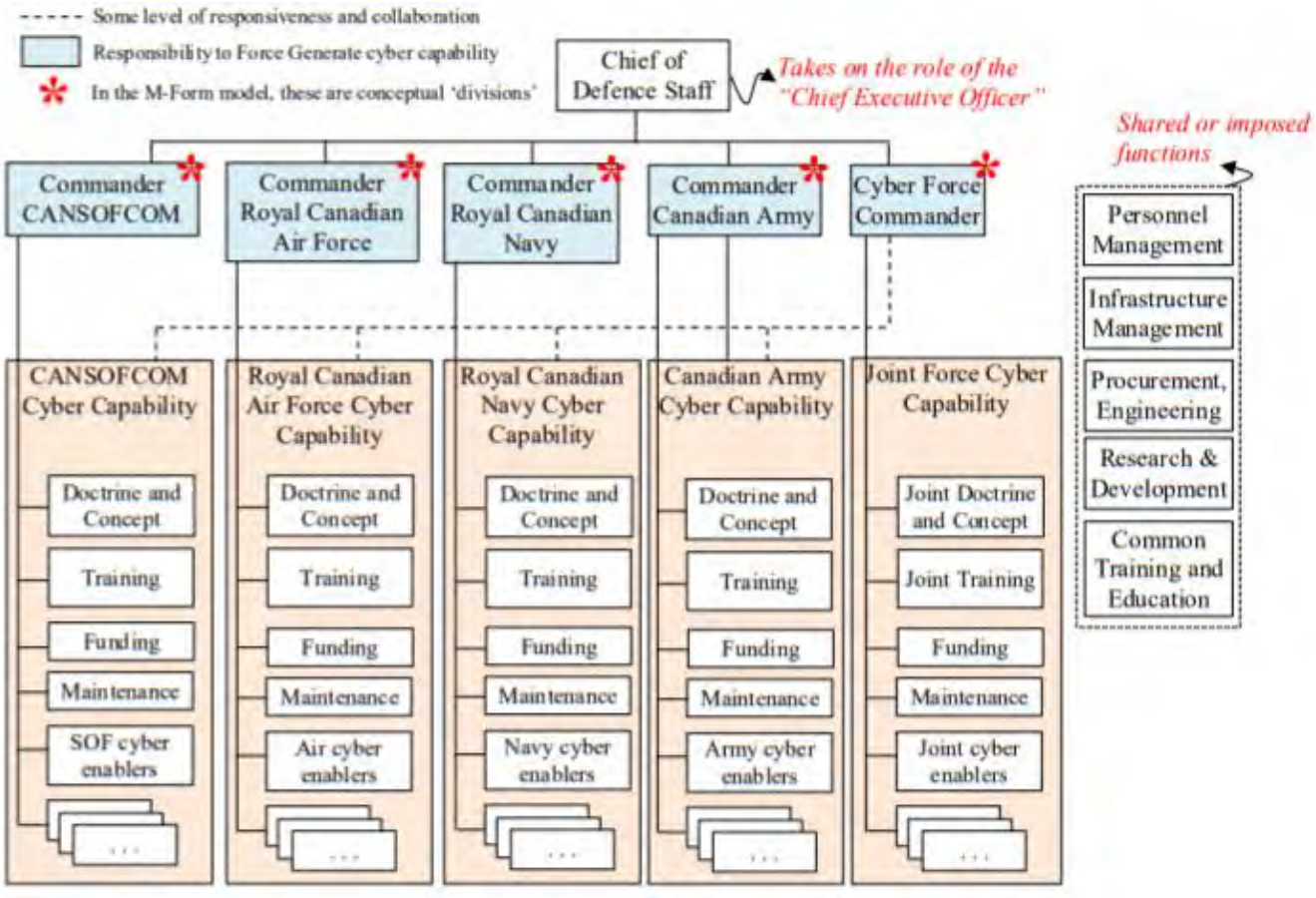

Figure 5 - "M" Form (Decentralized) Cyber Structure

The UK MoD stood up Joint Forces Command in 2011 with the goal of driving interoperability across the Air Force, Navy, and Army commands ("M" form – decentralized) and recently announced changes to that structure that appears to be moving towards a more centralized command structure[78]. If we examine the path that our two largest allies, the US and UK, have taken to build cyber capabilities we can see that both followed the path outlined in JDN 1/18 and have arguably arrived at level 3 in the model with a centralized cyber command. Recognizing that Canada is nearly a decade behind our allies in this capability development, perhaps the CAF can learn from our allies and follow the recommendation of LCdr Chouinard-Prévost to skip the "evolving step" and create centralized cyber command structures from the outset.

Recommendation #4 – Create a separate cyber command with centralized command and control with decentralized execution.

Influence Activities – Different Capability Development, Similar Problems

The CAF has developed and employed what is now known as Influence Activities (IA) as far back as the World War II but only started to recognize IA as a strategic enabler again with Canada's involvement in Afghanistan[79]. Despite over a decade of investment in capability development and several directives issued from as high as the Commander of the Canadian Army, it is the assessment of the author that the CAF has failed to build an effective and sustainable IA capability. IA continues to be recognized as strategic enabling capability that is not understood by most commanders and therefore

[78] Andrew Chuter and Aaron Mehta, "How the UK's Joint Forces Command Is about to Change - and Why It Won't Be Easy," Defense News (Defense News, April 26, 2019), https://www.defensenews.com/global/europe/2019/04/25/how-the-uks-joint-forces-command-is-about-to-change-and-why-it-wont-be-easy/.

[79] Ryan Clow, "PSYCHOLOGICAL OPERATIONS: THE NEED TO UNDERSTAND THE PSYCHOLOGICAL PLANE OF WARFARE," Canadian Military Journal (Government of Canada, National Defence, Canadian Defence Academy, August 27, 2008), http://www.journal.forces.gc.ca/Vo9/no1/05-clow-eng.asp.

rarely properly considered as part of the Operational Planning Process or resourced properly. Measuring the success of operationalizing IA in the CAF could be a thesis topic unto itself, but the simple fact that the only Google search results for "Canadian Forces influence activities" are a handful of individual pages from 5th Canadian Division should be a clear indicator that attempts to operationalize IA have failed. Instead, we will look at a few indicators that may be useful in highlighting obstacles to establishing a new capability in the CAF and seek to understand the disconnect between strategic guidance and execution on the front lines.

As with any planning process, strategic direction issued at the highest level and then successive layers of interpretation and elaboration of planning takes place in order to develop the tactical execution of tasks to realize the desired outcomes laid out in the strategy. Within the context of the CAF, defence policy is issued by the Government of Canada which is translated into a Defence Plan, and then objectives, missions and tasks are cascaded down through chains of command. Commanders at each level execute some variation of what is known in the CAF as the Operational Planning Process (OPP)[80] that will typically involve a review of the following factors for development of their plans:

- relative end states,
- assigned and implied tasks,
- constraints,
- restraints; and
- the intention of the higher commander.

---

[80] Department of National Defence, ″The Canadian Forces Operational Planning Process (OPP) ,″ The Canadian Forces Operational Planning Process (OPP) , 2008, http://publications.gc.ca/collections/collection_2010/forces/D2-252-500-2008-eng.pdf.

It is the assessment of the author that the operationalization of IA in the CAF has failed due to the inability to properly prioritize. This is the same strategic misstep that many organizations in the private sector experience which is dissected in a Harvard Business Review article titled "Too Many Projects: Why Companies Won't Let Bad Projects Die"[81]. Hollister and Watkins start with a famous quote from Michael Porter that "the essence of strategy is choosing what not to do" and then point out that it should follow that "the essence of execution is truly not doing it"[82]. The importance of building and sustaining Influence Activities as a strategic enabler has been stated and reinforced with the following series of plans and directives without realizing the desired outcomes:

- Army Influence Activities Master Implementation Plan dated 23 July 2010
- LFDTS 1901-1 (IATF) – Army Influence Activities Master Implementation Plan Review dated 31 May 2011
- SQFT 4800-1 (G5) – Task Force 3-12 Generation of Influence Activities Specialists dated 24 November 2011
- CLS 3350-1 (G35 UN/NATO) Influence Activities – Interim Force Generation Strategy dated 5 March 2012
- 1901-3 (DLFD) CA Master Implementation Directive – Territorial Battle Group dated March 2012
- Canadian Army Influence Activities Interim Implementation Directive dated 7 June 2013

[81] Rose HollisterMichael D. Watkins, "Why Companies Won't Let Bad Projects Die," Harvard Business Review, August 21, 2018, https://hbr.org/2018/09/too-many-projects.
[82] Ibid.

Each of these planning documents sought to address gaps assessed to be contributing factors to the failure to build and maintain IA capabilities across the CAF culminating with the issuance of the "Canadian Army Influence Activities Interim Implementation Directive" by the Commander of the Canadian Army[83]. It is worth noting that as of December 2018 the "Master Implementation Directive" projected to be released no later than 2016 has not been released and IA elements across the country continue to operate in the "interim" operating model.

So, what lessons can be learned from the IA capability development process in order to inform planning for cyber capability development? We can start with a review of the key constraints, restraints, and challenges identified in an early draft of the Master Implementation Directive (MID) that gathered feedback from members of the IA community across the CAF. Before starting this review, it is important to understand that the IA task was assigned to the PRes largely due to the experience and skills that members of the PRes bring to the role from civilian careers similar to the rationale for assigning cyber to the PRes alluded to in SSE[84]. Many of the obstacles to operationalizing IA capabilities in the CAF arose due to limited resources being allocated to support capability development and others relate more to the more human factors of Reservist motivation and need for certainty. While these are two distinct factors, one heavily influences the other. At the time of writing the MID draft (2013), restraints were imposed on the number of full-time PRes contracts that could be offered resulting from

[83] P.J. Devlin, "Canadian Army Influence Activities Interim Implementation Directive" (Ottawa: National Defence Headquarters, June 7, 2013).
[84] Department of National Defence, "Canada's Defence Policy – Strong, Secure, Engaged," Department of National Defence, 2017, http://dgpaapp.forces.gc.ca/en/canada-defence-policy/docs/canada-defence-policy-report.pdf, 73.

the Strategic Review (SR) and Deficit Reduction Action Plan (DRAP). This meant that any members outside of the core command element known as the IA Coordination Centre (IACC) would need to commit to significant work-up training without the guarantee of full-time employment or deployment on an overseas mission at the end of said work-up training[85]. This effectively limited the pool of potential PRes soldiers who could participate in work-up training to unemployed personnel who could afford to live without a steady income for approximately a year and predictably did not produce the desired outcome of fully qualified IA Companies that were ready to deploy. This lack of clarity and direction continues to hamper the operationalization of IA in 2018 and was even identified in a 2016 report from the Auditor General[86].

If we circle back to the key takeaways from the *Harvard Business Review* article on prioritization of key initiatives, we can quickly see that the operationalization of IA capabilities was not set up for success because the implementation directives did not identify what commanders could STOP doing in order to reallocate resources to IA capability development. Division commanders were essentially tasked with standing up a new capability without the corresponding "seed funding" to build and nurture the capability. Private industry has recognized the importance of providing "seed funding" to build new capabilities but also the need to operate outside of existing structures in order to allow for rapid experimentation and innovation without the constraints and restraints

[85] Influence Activities Task Force, "MASTER IMPLEMENTATION DIRECTIVE INFLUENCE ACTIVITY FORCE GENERATION AND EMPLOYMENT" (Kingston, ON: Influence Activities Task Force, 2013).
[86] Auditor General of Canada, "2002 April Report of the Auditor General of Canada," Government of Canada, Office of the Auditor General of Canada., April 16, 2002, http://www.oag-bvg.gc.ca/internet/English/parl_oag_200204_03_e_12376.html.

associated with operating inside of an established large and bureaucratic organization[87]. The IID effectively assigned unit commanders a secondary task to be staffed with PRes members to participate in IA training as a secondary task as part of their PRes employment which is already secondary to their civilian careers. In an organization that always has more tasks than resources, operationalization of IA capabilities was not set up to succeed.

Proper Application of Cyber Capabilities in Effects Based Operations

Modern military commanders are trained to apply Tactics Techniques and Procedures (TTPs) in alignment with doctrine that has typically been established and evolved over a period of decades to develop plans as part of the OPP. CAF commanders and planners learn about the application of Air, Land, Naval, and even Space power to the battlespace specializing first in their own domain and then learning how to integrate with the others. Most CAF planners and commanders have little or no understanding of cyber capabilities and how they will affect the battlespace. The lack of documented doctrine and TTPs will also limit the ability of training organizations to incorporate these concepts into the career courses of CAF leaders. This is yet another example of a problem experienced in the institutionalization of IA in the CAF that can be applied to the planning for institutionalization of cyber capabilities. In recent years, the CAF has started to incorporate IA planning and concepts into staff college and other leadership courses, but it will still likely take several years for the organizational knowledge gap to be closed. To avoid similar setbacks in the institutionalization of cyber capabilities, the CAF should

[87] CB Insights Research, "The History Of CVC: From Exxon And DuPont To Xerox And Microsoft, How Corporates Began Chasing 'The Future'," CB Insights Research, 2017, https://www.cbinsights.com/research/report/corporate-venture-capital-history/.

prioritize the development of TTPs and doctrine along with the development of course materials to start training its leaders on cyber capabilities as soon as possible.

In the development of the initial drafts of TTPs and doctrine, one of the challenges that CAF planners will face is that the cyber domain is very technical and requires a large foundation of knowledge to fully understand. Thankfully, this can be said for each of the specialized trades in the CAF and therefore planners can leverage the proven design patterns that have been used in order to help Air, Land, and Naval components to work together in joint operations. Standardization Agreements (STANAG) are published by the North Atlantic Treaty Organization (NATO) in order to provide shared standards across a number of NATO allies to improve interoperability[88]. STANAG 2287 – "Task verbs for use in planning and the dissemination of orders" provides a common set of terminology that commanders across NATO allied nations learn so that all commanders within a multinational operation share a common interpretation of tasks that are passed down in orders. With the development of standardized cyber TTPs and doctrine, CAF planners may one day treat cyber capabilities as just another specialized capability that can be brought to bear to achieve desired effects in support of accomplishing a given mission task. The US "Joint Publication 3-12 Cyberspace Operations" does a good job of reinforcing that commanders should not seek to task a cyber capability merely because it is available, but rather focus on the normal process of targeting to accomplish their commander's objectives[89]. Unfortunately, the planning considerations section of JP 3-12 is classified, so we need to look to other

[88] NATO, "e-Library," NATO, 2018, https://www.nato.int/cps/en/natohq/publications.htm.
[89] USCYBERCOM, "Joint Publication 3-12 Cyberspace Operations," Federation of American Scientists, June 8, 2018, https://fas.org/irp/doddir/dod/jp3_12.pdf.

sources for insights on how to apply cyber capabilities in support of achieving a commander's objectives for the purposes of this paper.

Defence Research and Development Canada (DRDC) researchers Bernier and Perrett conducted a detailed analysis of defensive cyber capabilities to tasks based off of the NATO Communication and Information Agency (NCIA) Communications and Information System (CIS) Security Capability Breakdown[90]. This analysis could be very useful to CAF planners in helping to describe the different capabilities that are available and the likely tasks that could be assigned in support of delivering defensive effects in the battlespace. Defensive effects only provide half of the picture for us, but this is still very useful in identifying the subsequent analysis and mapping required to provide CAF planners with the supporting lists of capabilities and potential tasks for cyber forces. A quick review of the NCIA CIS Security Capability Breakdown by a non-cyber trained CAF planner would reveal only a couple of terms (deceive and assess) in the entire chart that translate to existing tasks covered in existing CAF courses[91].

[90] Melanie Bernier and Kathryn Perrett, "Mission-Function-Task Analysis for Cyber Defence," Defence Technical Information Centre, 0AD, https://apps.dtic.mil/dtic/tr/fulltext/u2/1017005.pdf.
[91] Bernier, Melanie, and Joanne Treurniet. CF Cyber Operations in the Future Cyber Environment Concept . 2009, CF Cyber Operations in the Future Cyber Environment Concept , cradpdf.drdc-rddc.gc.ca/PDFS/unc92/p532776.pdf, Pg 4.

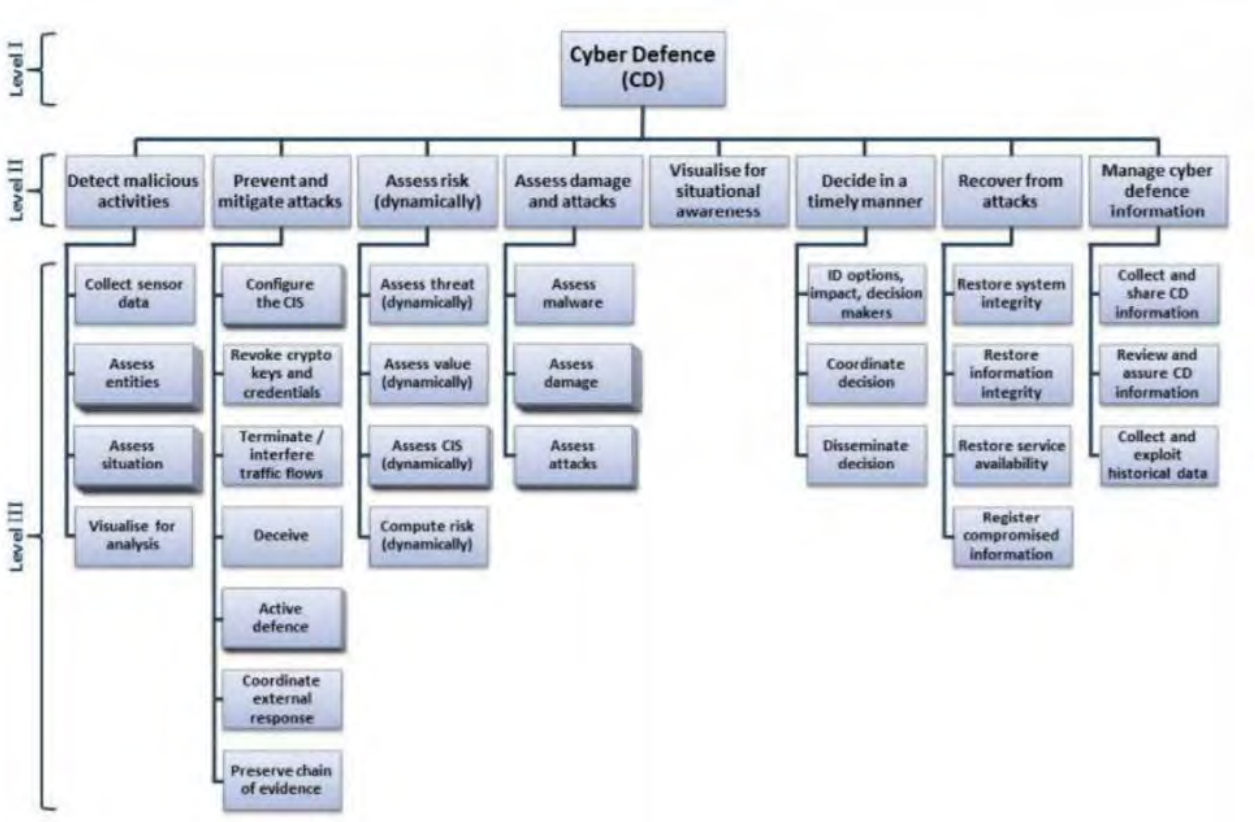

Figure 6 - NCIA CIS Security Capability Breakdown

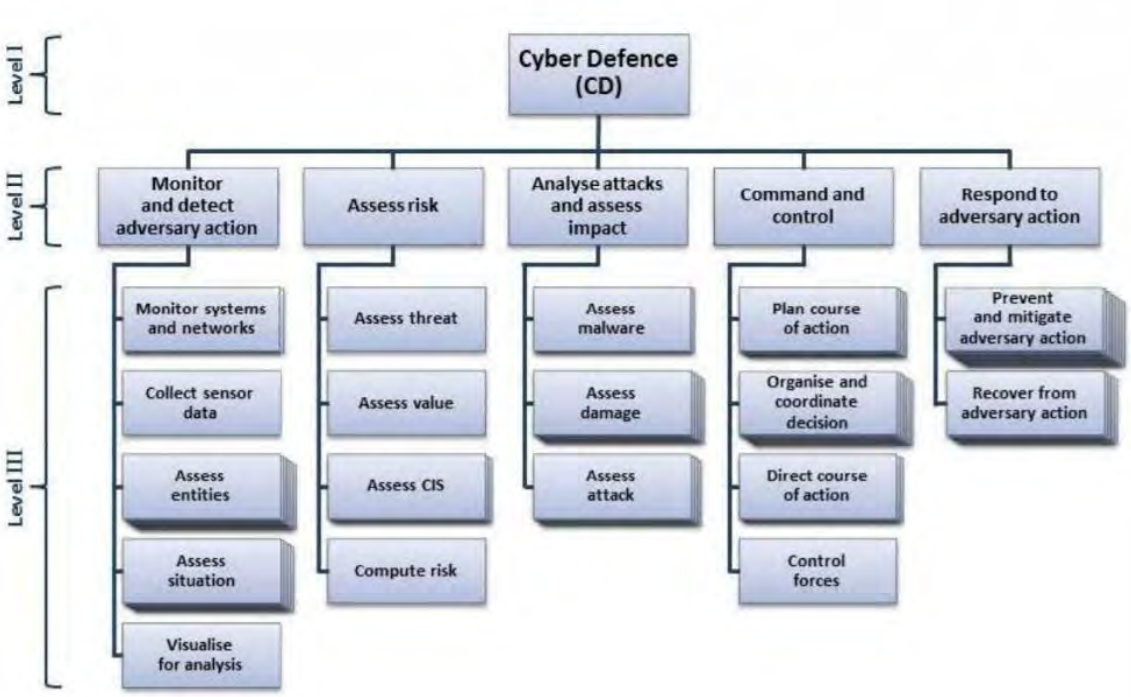

Figure 7 - NCIA CIS Cyber Defence Capabilities

This list of capabilities is then translated into a set of cyber defence capabilities that would look more familiar and directly applicable to the CAF OPP[92].

These capabilities would still require a cyber advisor in order to translate these high-level capabilities into specific tasks but should be much easier to understand for non-cyber trained personnel. It is worth noting that most of these capabilities and the resulting tasks would typically fall under the category of "implied tasks" that would be required regardless of the assigned mission and tasks since the defence of one's own forces and information tend to be required in most operations to date. Though many may argue that Canada is seeing this traditional position change with our participation in Operation Reassurance. In contrast, offensive cyber capabilities and tasks will be much more situation dependent and will likely be the part of the planning process where combat arms planners will need to have a better understanding of how to incorporate cyber factors into their planning process.

To help illustrate how cyber capabilities can be leveraged in order to achieve effects in the battlespace, we will review a couple of the easiest examples of offensive cyber capabilities that translate directly to traditional mission task verbs. A more complete and comprehensive analysis of offensive capabilities (referred to as "active measures" in SSE) and tasks is recommended in order to properly prepare planners and commanders to leverage cyber capabilities in operations. The mission task verbs Destroy, Deny, and Disrupt are probably the easiest for non-cyber trained personnel to understand

[92] Melanie Bernier and Kathryn Perrett, "Mission-Function-Task Analysis for Cyber Defence," Defence Technical Information Centre, 0AD, https://apps.dtic.mil/dtic/tr/fulltext/u2/1017005.pdf, 10.

the analogous effects in the cyber domain. STANAG 2287 provides the following definitions for these mission task verbs[93]:

> **Destroy** - Damage an object or an enemy force so that it is rendered useless to the enemy until reconstituted. (Measure: enemy force unable to fight)
>
> **Deny** – Prevent enemy use of a specified thing. (Measure: enemy unable to use specified thing)
>
> **Disrupt** – Break apart an enemy's formation and tempo, interrupt the enemy timetable, cause premature and/or piecemeal commitment of forces. (Measure: enemy actions uncoordinated and off-balance)

A commander could issue planning guidance to their staff including a task along the lines of "<Destroy, Disrupt, or Neutralize> enemy command and control (C2) systems no later than D-1 in order to Degrade enemy effectiveness during allied offensive operations." This is a good example because these effects could be delivered through kinetic (physical destruction), cyber (rendering infrastructure unusable on a temporary or permanent basis), or a combination thereof. Planners would need to evaluate several factors including, but not limited to:

- Potential physical collateral damage
- Potential cyber collateral damage
- Physical vulnerability of C2 infrastructure
- Cyber vulnerability of C2 infrastructure
- Is the infrastructure required for subsequent operations?
- Is the infrastructure shared with the civilian population?

Depending on the operational situation, planners can recommend different courses of action with varying advantages and disadvantages to each. In situations where a

---

[93] NATO, ″e-Library,″ NATO, 2018, https://www.nato.int/cps/en/natohq/publications.htm.

temporary or reversible effect is required, it is likely that non-kinetic options such as cyber and electronic warfare capabilities would be the best options for a commander to leverage. For cyber capabilities to be fully institutionalized in the CAF, more detailed analysis (or obtaining classified planning considerations developed by allies) will be required to ensure that CAF commanders and planners understand how cyber capabilities can provide additional options for achieving effects on the battlespace. This will include the development of many basic controls and guidelines that have been in place on the kinetic side of the battlespace including but not limited to:

- Guidelines for the development of rules of engagement
- Authorities for engaging high risk targets
- Guidelines for understanding political or diplomatic impacts

Recommendation #5 – Incorporate cyber planning, targeting, and effects into CAF leadership courses and OPP in higher HQ to enable effective integration of the capability.

TALENT MANAGEMENT - SOURCING AND RETAINING SKILLED PLANNERS AND OPERATORS

If we assume that National Defence Headquarters (NDHQ) planners overcome the challenges of prioritizing the allocation of resources to stand up the cyber capability, then the next step would be to ensure that those organizations are filled with qualified personnel. Intuitively, one may think that the biggest obstacles to building out a cyber capability for the forces would be political, technical or financial, whereas talent acquisition and retention will likely be two of the biggest obstacles for the CAF to overcome while building its cyber capabilities. Once the organizational structures have been defined, command structures put in place, and tools and technology acquired, the CAF will need to recruit, train, and retain highly skilled personnel to staff and operate this new (or modified) organization. Personnel management implications associated with building a cyber capability were identified as early as 2009 in the "CF Cyber Operations in the Future Cyber Environment Concept" document[94], but these were limited to the administrative details of creating new trades and training programs. The biggest challenges that the CAF will face in recruiting and retaining cyber operators may be competing with the private sector and other government agencies that are recruiting from the same talent pools. Cybersecurity consulting firm The Herjavec Group recently published the "The Cybersecurity Jobs Report" which predicts that the world will face a shortage of cyber security professionals upwards of 3.5 million by 2021.[95] To properly understand and mitigate the risk of facing a small pool of candidates from which to

[94] Melanie Bernier and Joanne Treurniet, "CF Cyber Operations in the Future Cyber Environment Concept," December 2009, http://cradpdf.drdc-rddc.gc.ca/PDFS/unc92/p532776.pdf.
[95] Cybersecurity Ventures, "Cybersecurity Jobs Report 2018-2021," Cybercrime Magazine, November 16, 2018, https://cybersecurityventures.com/jobs/.

recruit, the CAF will need to conduct a detailed analysis of the cyber security job market and operational needs of the CAF in order to design recruiting and retention programs to properly staff this critical function.

In addition to the overall shortage of talent available in the market, the CAF has additional operational considerations including physical fitness, security clearances, and the "ramp up" time required for an operator to become effective. The typical CAF career management cycle sees members rotated to new roles every 2-4 years which may require special consideration for cyber operators due to the highly-specialized tool sets and skills required to be proficient in the respective roles[96]. The CAF may also encounter challenges on the types of individuals that excel in the cyber domain being culturally, and often physically, very different from the average soldier. The US Army has already encountered this culture clash when training cyber operators under officers and non-commissioned members accustomed to the traditional command and control structure[97]. Commanders of these units will likely have to adapt their leadership styles to allow and even promote more open and free communication and collaboration across ranks and functional areas. Physical fitness standards may be another challenge due to the Universality of Service Requirements for CAF members[98] where Cyber Operator is not listed among the groups within the CAF excluded from part or all the requirements outlined in DAOD 5023-1, Minimum Operational Standards Related to Universality of

---

[96] Melanie Bernier and Joanne Treurniet, "CF Cyber Operations in the Future Cyber Environment Concept," December 2009, http://cradpdf.drdc-rddc.gc.ca/PDFS/unc92/p532776.pdf.
[97] Sean D. Carberry, "New Cyber Warriors Face Culture Shock," FCW, March 24, 2017, https://fcw.com/articles/2017/03/24/cyber-forces-carberry.aspx.
[98] Department of National Defence, "DAOD 5023-0, Universality of Service," DAOD 5023-0, Universality of Service, October 15, 2015, http://www.forces.gc.ca/en/about-policies-standards-defence-admin-orders-directives-5000/5023-0.page.

Service[99]. A quick review of trade requirements of Infantryman[100] and Cyber Operator[101] reveal a very little overlap between the two which recognizes that Cyber Operators need not be as strong or fit as Infantryman, but these standards may still limit the potential selection pool from an already limited pool. A recent study in the US estimates that over 71% of American youths are ineligible for enrolment leaving only 1% of the entire US population that is both eligible and being inclined to join[102].

The CAF Cyber Recruitment Pool Analysis

In order to fill the ranks of cyber operator and planner roles, the CAF ultimately has a few talent pools that it can target with different advantages, disadvantages, and lead times for training in order to generate useful cyber capabilities. For the purposes of this analysis, I will break down the potential talent pools into five groups.

- Active CAF Member - Cyber Ready
- Active CAF Member - Skill Upgrade Required
- Non-CAF Candidate - Cyber Ready
- Active CAF Member - Training Required
- Non-CAF Member - Training Required

While there are certainly more categories of potential cyber recruits, these categories allow for a relatively simple statistical analysis of CAF members and the

---

[99] Department of National Defence, "DAOD 5023-1, Minimum Operational Standards Related to Universality of Service," Government of Canada, National Defence, October 15, 2015, http://www.forces.gc.ca/en/about-policies-standards-defence-admin-orders-directives-5000/5023-1.page.
[100] Department of National Defence, "Task Statement for Military Occupational Structure Identification - 00010 Infantryman," Government of Canada, National Defence, January 5, 2017, http://www.forces.gc.ca/en/about-policies-standards-medical-occupations/mosid010-infantryman.page.
[101] Department of National Defence, "Task Statement for Military Occupational Structure Identification - 00378 Cyber Operator," Government of Canada, National Defence, March 15, 2017, http://www.forces.gc.ca/en/about-policies-standards-medical-occupations/mosid378-cyber-operator.page.
[102] Nolan Feeney, ″71% Of U.S. Youth Don't Qualify for Military Service, Pentagon Says,″ Time, June 29, 2014, http://time.com/2938158/youth-fail-to-qualify-military-service/.

general Canadian population to help paint a picture of how few candidates CAF recruiters will be able to target to fill its cyber vacancies. The magnitude of this problem cannot be over emphasized. In 2016, the Information Systems Audit and Control Association, (ISACA) projected a global cybersecurity talent shortage of over two million and a more recent study from The Herjavec Group estimates that this gap will grow to over 3.5 million by 2021[103]. This highlights the broader cyber talent market conditions that will create additional headwinds for the CAF as it will be forced to compete with the private sector and other government agencies for a limited talent pool of qualified cyber professionals. With that in mind, let us better quantify the problem with some statistical analysis of the potential cyber talent pool. The following values from Statistics Canada and other industry sources can be used in order to derive reasonable approximations of cybersecurity professionals in the CAF and in the Canadian population within the age range for recruitment. In light of the minimum age for enrolment in the CAF of 17 and the compulsory retirement age of 60, the target ages for recruitment are assumed to be seventeen to fifty in order to allow for several years of service following the large investment in training that will be required for many cyber operators and planners.

[103] Cybersecurity Ventures, "Cybersecurity Jobs Report 2018-2021," Cybercrime Magazine, November 16, 2018, https://cybersecurityventures.com/jobs/.

Working aged personnel in Canada (15-64)[104]	**24,244,100**
Percentage of workforce in Information Technology (IT)[105]	2.10%
Percentage of IT spend on Cybersecurity[106]	10.60%
Canadian Workers Aged 50-64[107]	5,258,599
Estimated Canadian Workers Age 15-17[108]	735,060
Active CAF Members (2018-Regular + Reserve)[109]	95,000

Table 2 - Canadian Cyber Workforce Demographics

Using these values, we can derive an estimated number of cybersecurity qualified professionals across Canada that fall within the target recruiting age range defined above. Taking the total working aged personnel in Canada less those over 50 and under 17, we can then multiply that value by the percentage of the workforce employed in IT and finally by the percentage of IT spend on cybersecurity. This leaves us with only an estimated 40,625 potential cybersecurity qualified personnel across Canada within our recruitment parameters. We can then use this value in order to derive the percentage of the workforce that has cybersecurity experience, which we have given the label of "Cyber Ready." This evaluates to 0.22% of the workforce being "Cyber Ready" and can be used to determine values for "Active CAF Member - Cyber Ready" and "Active CAF Member - Skill Upgrade Required" if we assume that the percentage of cybersecurity personnel in the CAF is proportional to that of the rest of Canada. These estimated values can help to

[104] Federal Reserve Bank of St. Louis, "Working Age Population: Aged 15-64: All Persons for Canada," FRED (Federal Reserve Bank of St. Louis, December 19, 2018), https://fred.stlouisfed.org/series/LFWA64TTCAM647S.
[105] Statistics Canada, "Labour in Canada: Key Results from the 2016 Census," Women and Paid Work (Government of Canada, Statistics Canada, November 29, 2017), https://www150.statcan.gc.ca/n1/daily-quotidien/171129/dq171129b-eng.htm.
[106] Statista, "IT Security Spending Relative to Total IT Budgets FY2005-FY2017 | Statistic," Statista, April 2018, https://www.statista.com/statistics/536764/worldwide-it-security-budgets-as-share-of-it-budgets/.
[107] Statistics Canada, "Labour Force Characteristics by Sex and Detailed Age Group, Annual (x 1,000)1," Statistics Canada (Government of Canada, Statistics Canada, 2018), https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=1410001801.
[108] Ibid.
[109] Department of National Defence, "Frequently Asked Questions," DND CAF, October 29, 2018, http://www.forces.gc.ca/en/about/faq.page.

paint a picture of what a potential talent pool pipeline could look like for CAF recruiters to target. We can then combine these numbers with estimated times to train or complete skill upgrades on order to generate actual capabilities for the CAF cyber force. Figure 8 below incorporates some assumptions regarding the time required to train different target audiences of potential recruits but should help to illustrate that generating cyber capabilities for the CAF will be a multi-year process.

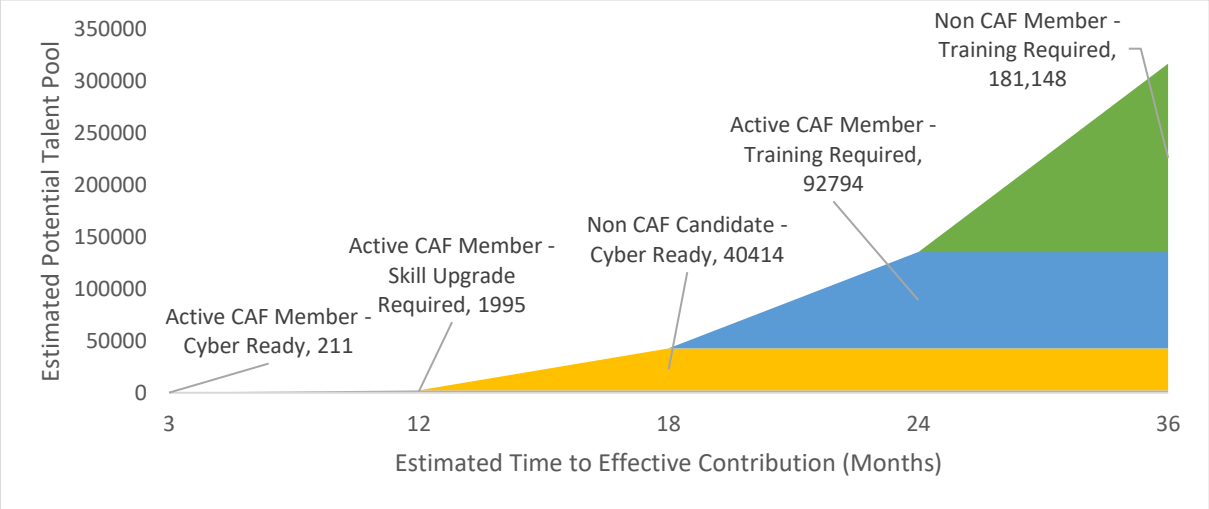

Figure 8 - CAF Cyber Recruitment Talent Pool Pipeline to Capability Realization

For the CAF to generate cyber capabilities, recruiters and planners will need to take a multi-pronged approach to acquiring talent. Near-term capability generation will need to focus on identifying and securing talent from the first two categories of personnel that can likely contribute in a meaningful way in less than twelve months. The "Active CAF Member - Cyber Ready" and "Active CAF Member - Skill Upgrade Required" categories represent the members who already have cybersecurity experience or transferrable skills that would require some additional training to be effective. These members should be able to be identified by leveraging the respective chains of command and will likely be more heavily concentrated in the Primary Reserves due to their civilian

employment. There will likely be multiple challenges to be overcome in the identification and allocation of these members due to the motivations of commanders at different levels and of the individual members. As identified in previous sections, military commanders are often faced with more tasks than they have resources to complete and therefore must allocate their resources in a way that best aligns to the accomplishment of their mission and key tasks. This means that many tasks, requests for information, and other initiatives passed down from higher headquarters get filtered out at various levels of the chain of command and may never make it to individual members of Primary Reserve units. It is imperative that any attempts to identify and allocate members of the Primary Reserve to support cyber capability generation for the CAF very clearly prioritize this activity as a "no-fail task" otherwise potential cyber recruits may never even become aware of the opportunity to contribute. Commanders may also be reluctant to identify "Cyber Ready" personnel in their organizations for fear of losing those resources for extended periods of time.

The next best source of talent will be the "Non-CAF Candidate - Cyber Ready" category of personnel which simultaneously provides likely the greatest opportunity to acquire strong talent combined with some of the most difficult obstacles to overcome. Introduction of the cyber domain is not the first time that the CAF has been presented with a role that may never need to be field deployable, but it is the first situation where the CAF needs to seriously consider whether the operational requirement to acquire talent will override the long-standing requirement for Universality of Service as prescribed by

Defence Administrative Orders and Directive 5023[110]. There will be some individuals in this category that are physically fit, healthy, and not concerned about monetary compensation for their work; however there will be many who don't fit that description. For potential recruits who do not meet the Universality of Service requirements to join the Regular Force or Primary Reserves, we will analyze different options available in greater detail within the section titled "Overcoming Policy Barriers to Acquiring Cyber Talent." In this section, we will also explore policy challenges pertaining to monetary compensation of members. While not the primary motivation for many potential recruits, the military model of compensation that is directly tied to rank will also present a challenge for the acquisition and retention of talent in a competitive job market.

Finally, the categories of "Active CAF Member - Training Required" and "Non-CAF Member - Training Required" have the longest lead times for recruitment and training and will face similar, and likely more intense, challenges that highly technical roles in the CAF have faced for decades. Trades that provide highly specialized training will need to institute strict mandatory service clauses for recruits that will require multiple years of investment in order to become fully qualified cyber operators. These contracts should ideally exclude "buy out" clauses that could allow private sector firms to reap the rewards of CAF investment in cyber operators and undermine efforts to build capabilities and capacity. Many private sector firms are accustomed to paying six figure "buy outs" in order to secure top talent for their teams in competitive job markets such as cyber. It should be made clear to new cyber recruits that administrative means such as

---

[110] Department of National Defence, ″DAOD 5023-0, Universality of Service,″ DAOD 5023-0, Universality of Service, October 15, 2015, http://www.forces.gc.ca/en/about-policies-standards-defence-admin-orders-directives-5000/5023-0.page.

Queen's Regulations and Orders 15.07 are not to be leveraged in order to secure more lucrative private employment prior to the end of their obligatory service and ideally written into their contract.

There is one additional talent pool that should be considered for the longer-term strategic interests for Canada and that is the under 17 demographic that will feed into the prime recruitment ages in the years to come. Cybersecurity solutions provider Palo Alto Networks recognized the importance of developing both the interest in cybersecurity and skills at young ages and partnered with Girl Scouts of the USA to introduce 18 cybersecurity badges[111]. These types of partnerships should be encouraged by the CAF and Government of Canada, but are likely best suited to be led by youth organizations and partnerships with private industry. A natural step for the Department of National Defence following the introduction of the cyber domain to the CAF would be the introduction of a cyber cadet corps. The UK announced their own cyber cadet program in September of 2018 with a target of training 2,000 cadets per year in order to fill the scarce talent pipeline for both the private sector and their armed forces. With the UK setting initial funding at an estimated investment of just £1 million, setting up a similar program in Canada would likely cost less and should be an obvious initiative to invest in for our future.

Although each of these target audiences for recruitment will have different lead times for acquisition, training, and return on investment, the CAF will need to execute on recruiting from these talent pools simultaneously in order to start building capacity. The

[111] Palo Alto Networks, "Palo Alto Networks and Girl Scouts of the USA Announce Collaboration for First-Ever National Cybersecurity Badges," June 13, 2017, https://www.paloaltonetworks.com/company/press/2017/palo-alto-networks-and-girl-scouts-of-the-usa-announce-collaboration-for-first-ever-national-cybersecurity-badges.

early acquisition of "Cyber Ready" personnel will be able to help to form training cadres and provide initial operational capabilities while the talent pipeline gets filled.

Overcoming Policy Barriers to Acquiring Cyber Talent

Figure 9 – Common Cartoon Depiction of Cyber Operators[112]

The caricature above became widely used around the world to draw attention to the elevation of cybersecurity to a mission critical function not just for banks and technology companies, but also for nation states. The image also depicts some of the common stereotypes associated with cybersecurity professionals that are now presenting serious challenges for recruiters and even commanders at the highest level of armed forces around the world. These challenges discussed briefly in previous sections can be broken into a few categories that each presents a significant policy or organizational obstacle we can analyze separately below:

- Physical fitness and other medical considerations (universality of service)
- Compensation directly linked to rank
- Cultural misalignment

[112] Florian Roth, "What Will the Warrior Guardian of the Future Look like?," Twitter (Twitter, September 5, 2015), https://twitter.com/cyb3rops/status/640195285424177153.

Likely the first obstacle in the way of recruiting cyber talent that comes to mind for many people is that people who spend a lot of time behind computers often seem to end up with polarized body compositions (either very slim and weak or obese) with poor physical fitness. While these stereotypes are not warranted for many members of the cybersecurity profession, governments around the world have recognized that they would exclude a material portion of a small talent pool without making changes to their policies. The UK MoD was an early mover in this space waiving physical fitness requirements for cyber operators as far back as 2013,[113] Australia in 2015[114], and the US appears to be getting close to granting physical fitness waivers for many high-demand skills such as cyber[115]. Policy frameworks and administrative orders such as DAOD 5023 vary greatly from one nation to the next; however, the waiver mechanism is used widely across the CAF in order to override mandatory requirements in support of meeting operational requirements. In light of multiple Commonwealth nations having already waived physical fitness requirements for cyber operator recruitment and the US likely to grant even more broad waivers for high-demand skills, the author strongly recommends that CAF commanders and planners grant similar waivers for CAF cyber operators. There are a few other options available to the CAF if granting a blanket waiver is either unpalatable or not possible for some reason. Section 3.4 of DAOD 5023-1 "Applicability of Minimum Operational Standards to Groups" states that Canadian Rangers, Cadet Organizations

---

[113] Graham Templeton, "UK Military Drops Physical Requirements for Cyberwarfare Specialists," Geek.com, July 5, 2013, https://www.geek.com/news/uk-military-drops-physical-requirements-for-cyberwarfare-specialists-1561168/.

[114] John Hilvert, "Defence Willing to Relax Rules, Offer More Cash to Recruit Cyber Experts," iTnews, June 18, 2015, https://www.itnews.com.au/news/defence-willing-to-relax-rules-offer-more-cash-to-recruit-cyber-experts-405391.

[115] Leo Shane, "Congress Could Give Fitness Waivers to More Troops as It Targets High-Demand Skills," Military Times (Military Times, March 1, 2018), https://www.militarytimes.com/news/pentagon-congress/2018/03/01/congress-could-give-fitness-waivers-to-more-troops-as-it-targets-high-demand-skills/.

Administration and Training Service (COATS), and Supplementary Reserve members "are not required to meet the minimum operational standards unless attached, seconded or transferred on consent to the Reg F or P Res."[116] Since section 3.5 allows for members of the Canadian Rangers and COATS to be placed on active service within Canada, the CAF could enrol cyber operators into one of these elements without the requirement for policy exceptions or waivers. Due to the longer-term career and deployment restrictions, it is the opinion of the author that these options should only be considered as short-term solutions until a permanent solution can be implemented.

Recommendation #6 – Exclude cyber operators from universality of service requirements that are not relevant to the role.

Another challenging policy issue to overcome will be compensating future cyber operators at levels that will entice more than just patriots with a strong sense of duty to enrol and serve for many years to come. In the previous section, we discussed the requirement to include mandatory service requirements and exclude "buy out" clauses for cyber operators that are trained by the CAF. The combination of free education and unique job experience will likely suffice to attract and retain the "Non-CAF Member - Training Required" demographic, but many of the individuals classified as "cyber ready" will not likely be satisfied with the $42,354 as a Second Lieutenant[117] or $35,061 as a Private[118]. Candidates at the intermediate level will typically be earning between $81,000

[116] Department of National Defence, "DAOD 5023-1, Minimum Operational Standards Related to Universality of Service," Government of Canada, National Defence, October 15, 2015, http://www.forces.gc.ca/en/about-policies-standards-defence-admin-orders-directives-5000/5023-1.page.
[117] Department of National Defence, "Pay Rates for Non-Commissioned Members," Canada.ca (Innovation, Science and Economic Development Canada, December 14, 2018), https://www.canada.ca/en/department-national-defence/services/benefits-military/pay-pension-benefits/pay/non-commissioned.html#reserve.
[118] Ibid.

to $116,000 per year with many senior professionals earning $200,000 and up[119]. The US Marine Corps flagged similar challenges this spring to the Cybersecurity subcommittee of the Senate Armed Services Committee and highlighted that bringing qualified cybersecurity professionals in at the lowest commissioned and non-commissioned ranks without the ability to recognize their civilian skill sets will not set the service up for success[120]. Many military organizations around the world already have programs in place offering signing bonuses and recognition of civilian qualifications and accelerated promotion schemes in order to attract and retain individuals with specialized qualifications such as doctors. The CAF currently offers signing bonuses upwards of $225,000 and accelerated promotion schemes for qualified medical doctors seeking employment in the CAF[121] which means that similar programs could be created for cyber talent acquisition. These incentives could help to get cyber talent in the door and then the CAF could explore special pay allowance schemes similar to those recently implemented by the US Army Cyber Command. Base pay scales and advanced promotions are admittedly difficult to implement; however, the introduction of "Assignment Incentive Pay" and "Special Duty Assignment Pay" have allowed the US Army to better compensate its cyber operators without making fundamental changes to their rank structure or base pay scales[122]. In order to attract and retain a robust and effective cyber

---

[119] Chris Brook, "Cyber Security Salary Guide: What Does Today's Cyber Security Workforce Make?," *Digital Guardian*, October 11, 2018, https://digitalguardian.com/blog/cyber-security-salary-guide-what-does-todays-cyber-security-workforce-make.
[120] Lauren C. Williams, "Military Looks to Boost Pay for Cyber Talent," *Defense Systems*, March 20, 2018, https://defensesystems.com/articles/2018/03/19/cyber-pay-armed-forces.aspx.
[121] Department of National Defence, "Medical Officer," *Canada.ca* (Innovation, Science and Economic Development Canada, August 29, 2018), https://www.canada.ca/en/department-national-defence/services/caf-jobs/career-options/fields-work/health-care/medical-officer.html.
[122] Jim Tice, "Assignment, Special Duty Pays OKd for Cyber Soldiers," *Army Times* (Army Times, August 7, 2017), https://www.armytimes.com/news/your-army/2015/04/21/assignment-special-duty-pays-okd-for-cyber-soldiers/.

capability, the CAF will likely have to execute more than one of the options outlined above or face significant recruiting and retention challenges. Putting aside all the pay and administrative challenges, there is one aspect of the cyber operator role that no other employer in Canada can offer to aspiring cyber operators. The work experience and opportunities to develop new skills are certainly unique and highly desirable for many candidate cyber operators[123], and this should be exploited by CAF recruiters. The cyber domain is unique in that cyber operators could theoretically be on the "front lines" of operations without leaving Canadian soil.

Recommendation #7 – Find a way to provide fair compensation for cyber expertise (signing bonuses, special allowances, specialty pay, etc.)

The final major obstacle that the CAF is likely to encounter in the attraction and retention of cyber operators will be one of cultural misalignment. The US Air Force identified this as an emerging, multi-faceted issue that warrants deeper analysis and consideration[124]. The first thoughts that come to the minds of many who would think of culture clashes between "cyber geeks" and the centuries of tradition on which military organizations have been built is that of appearance, grooming standards and dress. Interestingly, there are advocates expressing that concessions beyond recent relaxations in the CAF to grow beards and smoke marijuana[125] should be considered to include further liberalizations of standards to allow for other personal appearance preferences

[123] Benchmark Executive Search, "Cyber Talent: Hiring Ex-Spies Requires More Than Just High Pay," *Benchmark Executive Search*, April 26, 2017, https://www.benchmarkes.com/2017/04/cyber-talent-hiring-ex-spies-requires-just-high-pay/.
[124] Sean D. Carberry, "New Cyber Warriors Face Culture Shock," *FCW*, March 24, 2017, https://fcw.com/articles/2017/03/24/cyber-forces-carberry.aspx.
[125] Paul Szoldra, "Canadian Troops Can Now Grow Beards and Smoke Weed," *Business Insider* (Business Insider, September 28, 2018), https://www.businessinsider.com/canadian-troops-can-now-grow-beards-and-smoke-weed-2018-9.

such as non-natural hair colors like bright blue[126]. It is the opinion of the author that these are minor details that should be possible to resolve between cyber operators and their respective chains of command and that the much larger and more difficult issue will be the clash between traditional military chain of command and the more collaborative working environments found in the technology sector. The US Air Force identified the risk of young, talented cyber officers quickly being "crushed" by the traditional command and control style of planning and execution in which the Air Force has been accustomed to operating[127]. In order to mitigate these serious risks to retention of scarce cyber talent, the US Air Force has implemented a few innovative ideas to create and nurture a working environment that is both closer aligned to the wants and needs of cyber operators but also more closely aligned to the way that top technology firms operate in order to get optimum results from their technology teams[128]. The US Air Force incorporated "innovation education" and partnerships with private industry in order to promote rapid and collaborative approaches to problem solving. However, expanding this type of training to commanders that will need to rely on or integrate cyber effects into their planning process would also be extremely beneficial for the broader operationalization of cyber across the CAF.

Innovative Approaches to Cyber Talent Recruitment

Other nations such as Russia have allegedly taken an innovative approach to closing the gap on their own cyber talent pool shortage by leveraging cyber operators

---

[126] Jacqulyn Schneider, "Blue Hair in the Gray Zone," *War on the Rocks*, January 10, 2018, https://warontherocks.com/2018/01/blue-hair-gray-zone/.
[127] Sean D. Carberry, "New Cyber Warriors Face Culture Shock," *FCW*, March 24, 2017, https://fcw.com/articles/2017/03/24/cyber-forces-carberry.aspx.
[128] Ibid.

from organized crime groups[129] which is an effective approach for them, but not likely one to be replicated in North America or most NATO states. The US Defense Secretary Ash Carter has taken a very innovative and bold approach to provide a meaningful contribution to projects of vital importance to the defence of the US by enlisting the support of civilian experts on a term basis in a new program called the Defense Digital Service[130]. This is a program where professionals who "… may not all want to serve in the military, but they may want to serve the public purpose"[131] work on challenging projects that have meaningful impacts towards ensuring the security of US national interests. Considering the talent management challenges identified above in building an integral military cyber capability, a similar program may be feasible in Canada to realize rapid advancements with a shorter ramp-up period. A common theme that is materializing across NATO nations is a balanced and diverse approach to sourcing cyber talent. Both the UK[132] and US have adopted cyber talent sourcing strategies that include a mix of Regular, Reserve (or equivalent), Defence civilians, and contract labour in order to overcome the challenges identified elsewhere in this paper with recruiting, training, and retaining uniformed soldiers for specialized roles such as cyber.

---

[129] Mark Galeotti, "Crimintern: How the Kremlin Uses Russia's Criminal Networks in Europe," European Council on Foreign Relations, April 18, 2017, http://www.ecfr.eu/publications/summary/crimintern_how_the_kremlin_uses_russias_criminal_networks_in_europe.

[130] Sydney J. Freedberg, "SecDef Carter Wants YOU For The Defense Digital Service," Breaking Defense, September 14, 2016, http://breakingdefense.com/2016/09/ash-carter-wants-you-for-the-defense-digital-service/.

[131] Ibid.

[132] Ministry of Defence (UK), "Joint Doctrine Note 1/18: Cyber and Electromagnetic Activities ," Gov.UK, February 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf, 28.

CONCLUSION

There is no longer any doubt in the minds of our politicians, military commanders, and the much of the Canadian population that cyber-attacks against critical infrastructure, government agencies, and even major corporations could cause serious harm to national interests. It is also now widely understood and accepted that Canada's current cyber capabilities are not adequate to sustain effective cyber operations in defence of Canadian interests. Significant progress has been made towards understanding the gaps in CAF cyber capabilities, but little has been released publicly regarding a new national strategy, changes to foreign policy, or concrete plans backed by funding to execute. Even once these pieces have fallen into place, the CAF will face many challenges in building and retaining its new cyber capabilities due to talent scarcity and onerous procurement processes. To equip this coming generation of cyber operators for success, CAF leaders will need to innovate and be more agile in order to remain relevant in the rapidly changing cyber domain. Finally, the success of all of these elements relies on a clear strategy and a strong mandate from the Government of Canada to empower commanders across the CAF to defend Canada's interests in the cyber domain.

In summary, adopting the following recommendations will lay a strong foundation upon which the CAF can build a world-class cyber capability without succumbing to the missteps experienced by our allies and our own IA capability development efforts:

1. Technology acquisition and implementation enabling cyber capability development and support must be completed in months, not years

2. Resist the urge to "Canadianize" – leverage established standards and frameworks versus developing our own
3. Create an annual feedback loop into budget and establishment planning to enable adaptation of capabilities to match the changing contemporary operating environment
4. Create a separate cyber command with centralized command and control with decentralized execution
5. Incorporate cyber planning, targeting, and effects into CAF leadership courses and OPP in higher HQ to enable effective integration of the capability
6. Exclude cyber operators from universality of service requirements that are not relevant to the role
7. Find a way to provide fair compensation for cyber expertise (signing bonuses, special allowances, specialty pay, etc.)

By looking at the innovative approaches adopted by some of Canada's closest allies and learning lessons from our past, the CAF can rapidly close the current capability gap to achieve our strategic objectives. Doing so will require adopting different approaches to planning, procurement, and execution to keep pace with the rapidly changing threat landscape.

BIBLIOGRAPHY

Auditor General of Canada. “2002 April Report of the Auditor General of Canada.” Government of Canada, Office of the Auditor General of Canada., April 16, 2002. http://www.oag-bvg.gc.ca/internet/English/parl_oag_200204_03_e_12376.html.

BBC News. “Stuxnet Worm Hits Iran Nuclear Plant Staff Computers.” BBC News. BBC, September 26, 2010. https://www.bbc.com/news/world-middle-east-11414483.

Benchmark Executive Search. “Cyber Talent: Hiring Ex-Spies Requires More Than Just High Pay.” Benchmark Executive Search, April 26, 2017. https://www.benchmarkes.com/2017/04/cyber-talent-hiring-ex-spies-requires-just-high-pay/.

Bernier, Melanie, and Joanne Treurniet. “CF Cyber Operations in the Future Cyber Environment Concept .” Tech. *CF Cyber Operations in the Future Cyber Environment Concept* , December 2009. http://cradpdf.drdc-rddc.gc.ca/PDFS/unc92/p532776.pdf.

Bernier, Melanie, and Kathryn Perrett. “Mission-Function-Task Analysis for Cyber Defence.” Defence Technical Information Centre, 0AD. https://apps.dtic.mil/dtic/tr/fulltext/u2/1017005.pdf.

Biggs, John. “Heartbleed, The First Security Bug With A Cool Logo – TechCrunch.” TechCrunch. TechCrunch, April 9, 2014. https://techcrunch.com/2014/04/09/heartbleed-the-first-consumer-grade-exploit/.

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

Boutilier, Alex. “Former Electronic Spy Chief Urges Ottawa to Prepare for 'Cyber War'.” thestar.com, September 1, 2016. https://www.thestar.com/news/canada/2016/09/01/former-electronic-spy-chief-urges-ottawa-to-prepare-for-cyber-war.html.

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

Brook, Chris. “Cyber Security Salary Guide: What Does Today's Cyber Security Workforce Make?” Digital Guardian, October 11, 2018. https://digitalguardian.com/blog/cyber-security-salary-guide-what-does-todays-cyber-security-workforce-make.

Callaghan, Shaun, Kyle Hawke, and Carey Mignerey. “Five Myths (and Realities) about Zero-Based Budgeting.” McKinsey & Company, October 2014. https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/five-myths-and-realities-about-zero-based-budgeting.

Carberry, Sean D. “New Cyber Warriors Face Culture Shock.” FCW, March 24, 2017. https://fcw.com/articles/2017/03/24/cyber-forces-carberry.aspx.

Carucci, Ron. “Organizations Can't Change If Leaders Can't Change with Them.” Harvard Business Review, October 24, 2016. https://hbr.org/2016/10/organizations-cant-change-if-leaders-cant-change-with-them.

CB Insights Research. “The History Of CVC: From Exxon And DuPont To Xerox And Microsoft, How Corporates Began Chasing 'The Future'.” CB Insights Research, 2017. https://www.cbinsights.com/research/report/corporate-venture-capital-history/.

CGI. “Cybersecurity Litigation.” *Cybersecurity Law*, 2017, 1–7. https://doi.org/10.1002/9781119231899.ch2.

Chouinard-Prévost, R.A.D. “CYBER CAPABILITY DEVELOPMENT: CONSIDERATIONS FOR OPTIMIZING ORGANIZATIONAL FORM IN THE DND/CAF.” Canadian Forces College, 2017. https://www.cfc.forces.gc.ca/259/290/402/305/chouinard-prevost.pdf.

Chuter, Andrew, and Aaron Mehta. “How the UK's Joint Forces Command Is about to Change - and Why It Won't Be Easy.” Defense News. Defense News, April 26, 2019. https://www.defensenews.com/global/europe/2019/04/25/how-the-uks-joint-forces-command-is-about-to-change-and-why-it-wont-be-easy/.

Clow, Ryan. “PSYCHOLOGICAL OPERATIONS: THE NEED TO UNDERSTAND THE PSYCHOLOGICAL PLANE OF WARFARE.” Canadian Military Journal. Government of Canada, National Defence, Canadian Defence Academy, August 27, 2008. http://www.journal.forces.gc.ca/Vo9/no1/05-clow-eng.asp.

CNN. “2016 Presidential Campaign Hacking Fast Facts.” CNN. Cable News Network, November 24, 2018. https://www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html.

Cohen, Eliot A., and John Gooch. *Military Misfortunes: the Anatomy of Failure in War*. Free Press, 2012.

Communications Security Establishment Canada. “ITS Advice and Guidance.” ITS Advice and Guidance, November 28, 2016. https://www.cse-cst.gc.ca/en/group-groupe/its-advice-and-guidance.

Communications Security Establishment. “Canadian Centre for Cyber Security.” Canadian Centre for Cyber Security, October 16, 2018. https://cse-cst.gc.ca/en/backgrounder-fiche-information.

Communications Security Establishment. “Communications Security Establishment: What We Do and Why We Do It.” Communications Security Establishment, March 8, 2017. https://www.cse-cst.gc.ca/en/inside-interieur/what-nos.

Cybersecurity Ventures. “Cybersecurity Jobs Report 2018-2021.” Cybercrime Magazine, November 16, 2018. https://cybersecurityventures.com/jobs/.

Davies, Charles. “Why Defence Procurement so Often Goes Wrong.” Policy Options, January 20, 2016. http://policyoptions.irpp.org/magazines/january-2016/why-defence-procurement-so-often-goes-wrong/.

Department of National Defence. “DAOD 5023-0, Universality of Service.” Defence Administrative Orders and Directives , September 18, 2018. http://www.forces.gc.ca/en/about-policies-standards-defence-admin-orders-directives-5000/5023-0.page.

Department of National Defence. “DAOD 5023-1, Minimum Operational Standards Related to Universality of Service.” Government of Canada, National Defence, October 15, 2015. http://www.forces.gc.ca/en/about-policies-standards-defence-admin-orders-directives-5000/5023-1.page.

Department of National Defence. “Organizational Structure - Royal Canadian Air Force Reserve.” Royal Canadian Air Force, September 27, 2017. http://www.rcaf-arc.forces.gc.ca/en/air-reserve/organizational-structure.page.

Department of National Defence. “Pay Rates for Non-Commissioned Members.” Canada.ca. Innovation, Science and Economic Development Canada, December 14, 2018. https://www.canada.ca/en/department-national-defence/services/benefits-military/pay-pension-benefits/pay/non-commissioned.html#reserve.

Department of National Defence. “Task Statement for Military Occupational Structure Identification - 00378 Cyber Operator.” Government of Canada, National Defence, March 15, 2017. http://www.forces.gc.ca/en/about-policies-standards-medical-occupations/mosid378-cyber-operator.page.

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

Department of National Defence. “Cyber Operator - Job Description.” Canada.ca, June 18, 2018. https://www.canada.ca/en/department-national-defence/services/caf-jobs/career-options/fields-work/other-specialty-occupations/cyber-operator.html.

Department of National Defence. “DAOD 5023-0, Universality of Service.” DAOD 5023-0, Universality of Service, October 15, 2015. http://www.forces.gc.ca/en/about-policies-standards-defence-admin-orders-directives-5000/5023-0.page.

Department of National Defence. “Defence Investment Plan 2018: Ensuring the Canadian Armed Forces Is Well-Equipped and Well-Supported.” Government of Canada, June 2018. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/defence-investment-plan-

2018.html?utm_campaign=not-applicable&utm_medium=vanity-url&utm_source=canada-ca_Defence-Investment-Plan.

Department of National Defence. “Defensive Cyber Operations Decision Support.” Government of Canada, National Defence, May 26, 2016. http://www.forces.gc.ca/en/business-defence-acquisition-guide-2016/joint-and-other-systems-401.page.

Department of National Defence. *Department of National Defence and the Canadian Armed Forces 2017-18 Departmental Plan*, March 9, 2017. http://www.forces.gc.ca/assets/FORCES_Internet/docs/en/dp-2017-18-_-final_eng.pdf.

Department of National Defence. “Execution - Defence Plan 2018-2023.” Canada.ca. Innovation, Science and Economic Development Canada, May 17, 2018. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/defence-plan-2018-2023/execution.html.

Department of National Defence. “Frequently Asked Questions.” DND CAF, October 29, 2018. http://www.forces.gc.ca/en/about/faq.page.

Department of National Defence. “Medical Officer.” Canada.ca. Innovation, Science and Economic Development Canada, August 29, 2018. https://www.canada.ca/en/department-national-defence/services/caf-jobs/career-options/fields-work/health-care/medical-officer.html.

Department of National Defence. “Pay Rates for Officers.” Canada.ca. Innovation, Science and Economic Development Canada, December 14, 2018. https://www.canada.ca/en/department-national-defence/services/benefits-military/pay-pension-benefits/pay/officers.html#classab.

Department of National Defence. “QR&O: Volume I - Chapter 15 Release.” Canada.ca, November 24, 2017. https://www.canada.ca/en/department-national-defence/corporate/policies-standards/queens-regulations-orders/vol-1-administration/ch-15-release.html#cha-015-07.

Department of National Defence. “Task Statement for Military Occupational Structure Identification - 00010 Infantryman.” Government of Canada, National Defence, January 5, 2017. http://www.forces.gc.ca/en/about-policies-standards-medical-occupations/mosid010-infantryman.page.

Department of National Defence. “The Canadian Forces Operational Planning Process (OPP) .” The Canadian Forces Operational Planning Process (OPP) , 2008. http://publications.gc.ca/collections/collection_2010/forces/D2-252-500-2008-eng.pdf.

Development, Concepts and Doctrine Centre, Ministry of Defence (MoD). “Joint Concept Note 1/17 Future Force Concept.” Joint Concept Note 1/17 Future Force Concept, 2017.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643061/concepts_uk_future_force_concept_jcn_1_17.pdf.

Devlin, P.J. “Canadian Army Influence Activities Interim Implementation Directive.” Ottawa: National Defence Headquarters, June 7, 2013.

Federal Reserve Bank of St. Louis. “Working Age Population: Aged 15-64: All Persons for Canada.” FRED. Federal Reserve Bank of St. Louis, December 19, 2018. https://fred.stlouisfed.org/series/LFWA64TTCAM647S.

Feeney, Nolan. “71% Of U.S. Youth Don't Qualify for Military Service, Pentagon Says.” Time, June 29, 2014. http://time.com/2938158/youth-fail-to-qualify-military-service/.

Freedberg, Sydney J. “DIU(X) Funds Brain-Hacking Headset; Boston Branch Opens.” Breaking Defense, July 26, 2016. http://breakingdefense.com/2016/07/diux-funds-brain-hacking-headset-boston-branch-opens/.

Freedberg, Sydney J. “SecDef Carter Wants YOU For The Defense Digital Service.” Breaking Defense, September 14, 2016. http://breakingdefense.com/2016/09/ash-carter-wants-you-for-the-defense-digital-service/.

Galeotti, Mark. “Crimintern: How the Kremlin Uses Russia’s Criminal Networks in Europe.” European Council on Foreign Relations, April 18, 2017. http://www.ecfr.eu/publications/summary/crimintern_how_the_kremlin_uses_russias_criminal_networks_in_europe.

Gibson, Sarah Katherine. “Dreams of a 'Fireproof House'.” The Kingston Whig-Standard, September 16, 2013. https://www.thewhig.com/2013/09/16/dreams-of-a-fireproof-house/wcm/795ec0d9-7cc4-80ff-8ac4-5767d5c86049.

Gilmore, Scott. “Military Procurement Is a National Disgrace.” Macleans.ca, June 24, 2015. http://www.macleans.ca/news/canada/military-procurement-is-a-national-disgrace/.

Government of Canada, Office of the Auditor General of Canada, . “2016 Spring Reports of the Auditor General of Canada Report 5-Canadian Army Reserve-National Defence.” Report 1-Phoenix Pay Problems, 2016. http://www.oag-bvg.gc.ca/internet/English/parl_oag_201602_05_e_41249.html.

Hall, Stephen, Dan Lovallo, and Reinier Musters. “How to Put Your Money Where Your Strategy Is.” McKinsey & Company, March 2012. https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-to-put-your-money-where-your-strategy-is.

Heftye, Erik. “Multi-Domain Confusion: All Domains Are Not Created Equal.” The Strategy Bridge, May 2017. https://thestrategybridge.org/the-bridge/2017/5/26/multi-domain-confusion-all-domains-are-not-created-equal.

Hilvert, John. “Defence Willing to Relax Rules, Offer More Cash to Recruit Cyber Experts.” iTnews, June 18, 2015. https://www.itnews.com.au/news/defence-willing-to-relax-rules-offer-more-cash-to-recruit-cyber-experts-405391.

Influence Activities Task Force. “MASTER IMPLEMENTATION DIRECTIVE INFLUENCE ACTIVITY FORCE GENERATION AND EMPLOYMENT.” Kingston, ON: Influence Activities Task Force, 2013.

International Information System Security Certification Consortium. “Cybersecurity Workforce Shortage Projected at 1.8 Million by 2022.” (ISC)2 Blog, February 15, 2017. http://blog.isc2.org/isc2_blog/2017/02/cybersecurity-workforce-gap.html.

Ismail, Nick. “Global Cybercrime Economy Generates over $1.5 Trillion.” Information Age, June 20, 2018. https://www.information-age.com/global-cybercrime-economy-generates-over-1-5tn-according-to-new-study-123471631/.

Joint Chiefs of Staff, and Department of Defence (2005). https://apps.dtic.mil/dtic/tr/fulltext/u2/a476464.pdf.

Joint Chiefs of Staff, and Department of Defense (2009). https://apps.dtic.mil/dtic/tr/fulltext/u2/a493960.pdf.

Kindervag, John. “Zero Trust Networks.” *Zero Trust Networks*. Lecture presented at the Zero Trust Networks, April 19, 2017.

MacDonald, Corinne. “THE CANADIAN ARMED FORCES: THE ROLE OF THE RESERVES.” Government of Canada publications, November 29, 1999. http://publications.gc.ca/collections/Collection-R/LoPBdP/BP/prb9911-e.htm#b.%20Militiatxt.

MacIsaac, David. “Air Warfare.” Encyclopædia Britannica. Encyclopædia Britannica, inc., July 18, 2016. https://www.britannica.com/topic/air-warfare.

McDonough, David, and Tony Battista. “Fortress Canada: How Much of a Military Do We Really Need?” iPolitics, April 27, 2016. http://ipolitics.ca/2016/04/27/fortress-canada-how-much-of-a-military-do-we-really-need/.

McGill, Chris. “Benefits of New CAF Software.” Trident Newspaper, March 13, 2018. https://tridentnewspaper.com/benefits-new-caf-software/.

Ministry of Defence (UK). “Joint Doctrine Note 1/18: Cyber and Electromagnetic Activities .” Gov.UK, February 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf.

Ministry of Defence. “Defence Secretary Reveals New Generation of 'Cyber Cadets'.” GOV.UK. GOV.UK, September 30, 2018.

https://www.gov.uk/government/news/defence-secretary-reveals-new-generation-of-cyber-cadets.

Morgan, Steve. “Cybercrime Damages Expected to Cost the World $6 Trillion by 2021.” CSO Online, August 22, 2016. http://www.csoonline.com/article/3110467/security/cybercrime-damages-expected-to-cost-the-world-6-trillion-by-2021.html.

Morse, Eric. “Canadian Defence Procurement Still Looks like Massive Case of Charlie Foxtrot.” iPolitics, January 3, 2017. http://ipolitics.ca/2017/01/03/canadian-defence-procurement-still-looks-like-massive-case-of-charlie-foxtrot/.

NATO Cooperative Cyber Defence Centre of Excellence. “Cyber Definitions.” CCDCOE, April 28, 2015. https://ccdcoe.org/cyber-definitions.html.

NATO. “e-Library.” NATO, 2018. https://www.nato.int/cps/en/natohq/publications.htm.

NATO. “The History of Cyber Attacks - a Timeline.” NATO, 2013. https://www.nato.int/docu/review/2013/cyber/timeline/en/index.htm.

Palo Alto Networks. “Palo Alto Networks and Girl Scouts of the USA Announce Collaboration for First-Ever National Cybersecurity Badges,” June 13, 2017. https://www.paloaltonetworks.com/company/press/2017/palo-alto-networks-and-girl-scouts-of-the-usa-announce-collaboration-for-first-ever-national-cybersecurity-badges.

Parsons, Christopher, and Tamir Israel. “Canada's National Security Consultation: Digital Anonymity & Subscriber Identification Revisited... Yet Again.” The Citizen Lab, November 17, 2016. https://citizenlab.org/2016/10/digital-anonymity-subscriber-identification-revisited-yet-again/.

Platt, Victor. “Still the Fire-Proof House? An Analysis of Canada's Cyber Security Strategy.” *International Journal* 67, no. 1 (2011): 155–67. http://www.jstor.org/stable/23265971.

Public Safety Canada. “Action Plan 2010-2015 for Canada's Cyber Security Strategy.” Action Plan 2010-2015 for Canada's Cyber Security Strategy, December 3, 2015. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/index-en.aspx.

Public Safety Canada. *CYBER REVIEW CONSULTATIONS REPORT*, January 17, 2017. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2017-cybr-rvw-cnslttns-rprt/2017-cybr-rvw-cnslttns-rprt-en.pdf.

Public Safety Canada. “National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age.” National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age, June 12, 2018. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx.

Public Safety. *Canada's Cyber Security Strategy: for a Stronger and More Prosperous Canada*. Ottawa, Ont.: Government of Canada, 2010.

https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf.

Pugliese, David. “Canadian Army Cuts Enrollment Time for Reserves – New Process to Take Just Weeks.” Ottawa Citizen, April 4, 2017. https://ottawacitizen.com/news/national/defence-watch/canadian-army-cuts-enrollment-time-for-reserves-new-process-to-take-just-weeks.

Roth, Florian. “The Newcomer's Guide to Cyber Threat Actor Naming – Florian Roth – Medium.” medium.com. medium, March 25, 2018. https://medium.com/@cyb3rops/the-newcomers-guide-to-cyber-threat-actor-naming-7428e18ee263.

Roth, Florian. “What Will the Warrior Guardian of the Future Look like?” Twitter. Twitter, September 5, 2015. https://twitter.com/cyb3rops/status/640195285424177153.

Schneider, Jacqulyn. “Blue Hair in the Gray Zone.” War on the Rocks, January 10, 2018. https://warontherocks.com/2018/01/blue-hair-gray-zone/.

Shackelford, Scott J., Scott Russell, and Jeffrey Haut. “BOTTOMS UP: A COMPARISON OF ‘VOLUNTARY’ CYBERSECURITY FRAMEWORKS,” February 16, 2016. https://www.nist.gov/sites/default/files/documents/2017/02/14/20160216_scott_j._shackelford_scott_russell_jeffrey_haut.pdf.

Shane, Leo. “Congress Could Give Fitness Waivers to More Troops as It Targets High-Demand Skills.” Military Times. Military Times, March 1, 2018. https://www.militarytimes.com/news/pentagon-congress/2018/03/01/congress-could-give-fitness-waivers-to-more-troops-as-it-targets-high-demand-skills/.

Shimooka, Richard. “Canada Has the Worst Military Procurement System in the Western World.” The Hill Times. The Hill Times, January 18, 2019. https://www.hilltimes.com/2019/01/21/canada-worst-military-procurement-system-western-world/184060.

Sjouwerman, Stu. “Global Cyber Security Spending to Top $114bn in 2018, Says Gartner.” KnowBe4, August 16, 2018. https://blog.knowbe4.com/global-cyber-security-spending-to-top-114bn-in-2018-says-gartner.

Smith, Marie-Danielle. “Sajjan Faces 'Two Burdens': Military, Angered by His Boast, Also Expects His Defence Policy Review to 'Fall Short'.” National Post, May 3, 2017. http://news.nationalpost.com/news/canada/canadian-politics/sajjan-faces-two-burdens-military-angered-by-his-boast-also-expects-his-defence-policy-review-to-fall-short.

Solomon, Howard. “Shared Services Canada Defends Progress in Merging IT Systems, Vows to Do Better.” IT World Canada, October 13, 2016.

http://www.itworldcanada.com/article/shared-services-canada-defends-progress-in-merging-it-systems-vows-to-do-better/387384.

Statista. “IT Security Spending Relative to Total IT Budgets FY2005-FY2017 | Statistic.” Statista, April 2018. https://www.statista.com/statistics/536764/worldwide-it-security-budgets-as-share-of-it-budgets/.

Statistics Canada. “Labour Force Characteristics by Sex and Detailed Age Group, Annual (x 1,000)1.” Statistics Canada. Government of Canada, Statistics Canada, 2018. https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=1410001801.

Statistics Canada. “Labour in Canada: Key Results from the 2016 Census.” Women and Paid Work. Government of Canada, Statistics Canada, November 29, 2017. https://www150.statcan.gc.ca/n1/daily-quotidien/171129/dq171129b-eng.htm.

Szoldra, Paul. “Canadian Troops Can Now Grow Beards and Smoke Weed.” Business Insider. Business Insider, September 28, 2018. https://www.businessinsider.com/canadian-troops-can-now-grow-beards-and-smoke-weed-2018-9.

Teck, Woon. “Cyber Threat Has No Borders.” RSM Global, May 26, 2017. https://www.rsm.global/insights/rsm-global-blog/cyber-threat-has-no-borders.

Templeton, Graham. “UK Military Drops Physical Requirements for Cyberwarfare Specialists.” Geek.com, July 5, 2013. https://www.geek.com/news/uk-military-drops-physical-requirements-for-cyberwarfare-specialists-1561168/.

Tice, Jim. “Assignment, Special Duty Pays OKd for Cyber Soldiers.” Army Times. Army Times, August 7, 2017. https://www.armytimes.com/news/your-army/2015/04/21/assignment-special-duty-pays-okd-for-cyber-soldiers/.

Trudeau, Rt. Hon. Justin. “Minister of National Defence Mandate Letter.” Prime Minister of Canada, November 13, 2015. http://pm.gc.ca/eng/minister-national-defence-mandate-letter.

USCYBERCOM. “Joint Publication 3-12 Cyberspace Operations.” Federation of American Scientists, June 8, 2018. https://fas.org/irp/doddir/dod/jp3_12.pdf.

Watkins, Rose HollisterMichael D. “Why Companies Won't Let Bad Projects Die.” Harvard Business Review, August 21, 2018. https://hbr.org/2018/09/too-many-projects.

Williams, Lauren C. “Military Looks to Boost Pay for Cyber Talent.” Defense Systems, March 20, 2018. https://defensesystems.com/articles/2018/03/19/cyber-pay-armed-forces.aspx.

Yusof, Nordin. “Part 2: High Technology Warfare.” Essay. In *Space Warfare: High-Tech War of the Future Generation*, 11–12. Penerbit Universiti Teknologi Malaysia, 1999.