National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

Major Thomas Bell

Canada Under Attack – An Analysis of Canada's Adversaries' Capabilities in the Cyber Domain and How Canada Can Learn or Respond

JCSP 47

Exercise Solo Flight

Disclaimer

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

PCEMI 47

Exercice Solo Flight

Avertissement

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

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 47 – PCEMI 47
2020 – 2022

Exercise Solo Flight – Exercice Solo Flight

Major Thomas Bell

Canada Under Attack – An Analysis of Canada's Adversaries' Capabilities in the Cyber Domain and How Canada Can Learn or Respond

CANADA UNDER ATTACK: AN ANALYSIS OF CANADA'S ADVERSARIES' CAPABILITIES IN THE CYBER DOMAIN AND HOW CANADA CAN LEARN OR RESPOND

Thesis Statement

Canada has ceded the initiative in the cyber domain to its adversaries. In order to gain the initiative, Canada should adopt an offensive mindset in the cyber domain, while emulating and seeking to surpass its adversaries technologically, organizationally, and with superior policies and doctrine.

Abstract

This paper examines Canada's cyber capabilities in relation to two of its adversaries: China and Russia[1]. Comparisons are made between these nations' cyber capabilities across the metrics of technology, organization, and doctrine.[2] A key capability gap identified involves the structure of the Canadian Government including the Communications Security Establishment (CSE) and Canadian Armed Forces (CAF) with regards to conducting cyber operations, most notably when compared to China. Another key area of asymmetry are policies, governance, and doctrinal differences whereby both Russian and Chinese offensive cyber forces are unleashed to conduct operations throughout NATO's depth (including Canada) while Canadian capabilities are more restricted. The paper concludes that Canadian cyber capabilities could be brought towards parity with its adversaries through improvements in both organization and Canadian policies governing cyber operations. This could include a limited restructure of parts of the Federal Government with a focus on bringing responsibility for cyber operations under one strategic vision, maximizing well-suited yet scarce resources, and a re-evaluating applicable

[1] The word adversaries is used instead of "potential adversaries" as these two states are currently actively attacking Canada in the cyber domain as will be discussed.
[2] Where open-source material is limited, inferences as to the technological and other capabilities are drawn from cyber activities and attacks documented in open-source reporting.

policies. These changes would aim to move Canada towards adopting an offensive mindset and gaining the initiative in what may well be the vital ground of the coming decades: the cyber domain.

Introductory Quotes

> "Russian state-sponsored threat actors are targeting the following industries and organizations in … Western nations: COVID-19 research, governments, election organizations, healthcare and pharmaceutical, defense, energy, video gaming, nuclear, commercial facilities, water, aviation, and critical manufacturing."[3]
>
> "The Chinese government…engages in malicious cyber activities to pursue its national interests. Malicious cyber activities attributed to the Chinese government …continue to target, a variety of industries and organizations in the United States, including healthcare, financial services, defense industrial base, energy, government facilities, chemical, critical manufacturing (including automotive and aerospace), communications, IT (including managed service providers), international trade, education, video gaming, faith-based organizations, and law firms… China is conducting operations worldwide to steal intellectual property and sensitive data from critical infrastructure organizations, including organizations involved in healthcare, pharmaceutical, and research sectors working on COVID-19 response…"[4]

Canada is not currently under the *threat* of cyber attack; it is *under attack* by its adversaries in the cyber domain. Canada has been criticized for a "too-little too-late" response to the severity and scope of cyber-attacks.

> "…an overemphasis on resiliency, emergency management and disaster recovery, at the possible expense of defensive and offensive cyber operations, has left the CAF trailing allies and adversaries in certain cyber defence capabilities. While China and Russia have proven their ability to launch attacks that cripple critical systems in seconds or quietly collect intelligence for years, the CAF has only recently received approval to engage in active and offensive operations at scale …Adversaries and allies have also demonstrated their ability to deploy new cyber capabilities in months

[3] "Russia Cyber Threat Overview and Advisories." CISA. (n.d.), Accessed April 13, 2022. https://www.cisa.gov/uscert/russia
[4] "China Cyber Threat Overview and Advisories." CISA. (n.d.). Accessed April 13, 2022. https://www.cisa.gov/uscert/china

or weeks, while the CAF remains burdened by a years-long and sometimes decades-long procurement cycle."[5]

NATO has officially published doctrine guiding the conduct of operations in the cyber domain,[6] shortly after recognizing the cyber domain as an operational domain (along with space, air, sea, and land).[7] Accordingly, Canada has developed several policies[8,9] and organizations[10,11] to protect Canadians and to conduct activities in the cyber domain. Canada is also moving towards developing the capability to integrate cyber operations with those across other domains.[12,13] However, Canada's efforts to date in this regard have not kept pace with its adversaries Russia and China. While relatively even with Canada technologically[14], both Russia and China have exceeded Canada in their capability to conduct large scale and coordinated cyber operations. This has been enabled by major defense restructuring (most notably in China). It has also been achieved by policies tightly regulating cyber activities to enable cyber defense, and actively promoting offensive cyber activities, to the point of partnering with organizations operating in the "grey zone" of conflict. Both China and Russia have partnered with fringe organizations and assimilated skilled personnel from criminal organizations to conduct cyber

[5] "From Bullets to Bytes: Industry's Role in Preparing Canada for the Future of Cyber Defence," Canadian Association of Defence and Security Industries 2019 Report. https://www.defenceandsecurity.ca/UserFiles/Uploads/publications/reports/files/document-24.pdf
[6] NATO. *Allied Joint Publication-3.20: Allied Joint Doctrine for Cyberspace Operations*, *January 2020*. (NATO Standardization office: NATO Standardization Document Database, 2020).
[7] Stevens, T., Ertan, A., Floyd, K.,Pernik, P., eds. *Cyber Threats and NATO 2030: Horizon Scanning and Analysis.* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, January 2021), 127.
[8] Canada, *National Cyber Security Strategy,* (Public Safety Canada, 2018)
[9] Canada. *National Cyber Security Action Plan (2019-2024)*, (Public Safety Canada, 2019)
[10] "Mandate." Communications Security Establishment, Canada, accessed 9 May 2022. https://www.cse-cst.gc.ca/en/corporate-information/mandate
[11] "Canadian Centre for Cyber Security." Canada, accessed 9 May 2022. Accessed at https://cyber.gc.ca/en/
[12] Canada. *Strong Secure Engaged - Canada's Defense Policy* (Department of National Defense, 2017).
[13] Canada. *Pan-Domain Force Employment Concept* (Department of National Defense, draft)
[14] Stevens, T., Ertan, A., Floyd, K.,Pernik, P., eds. *Cyber Threats and NATO 2030: Horizon Scanning and Analysis.*47.

operations on behalf of the state government. [15,16] Canada is not in a position to directly emulate these illegal activities employed with such great affect by its adversaries. However, Canada can learn from, and react to, certain aspects of both China and Russia's cyber capabilities to potentially improve its own. Firstly, both China[17] and Russia[18] have adopted policies that promote and embrace offensive cyber activities to disrupt civil and military systems and personnel in several NATO countries (including Canada). Through improved civil-military integration and cooperation in the fields of hacking and other cyber activities below the threshold of war and in the "grey zone," Canada might more rapidly develop its capabilities to both defend against offensive cyber activities and deploy its own in a disruptive and pre-emptive capacity. Secondly, through increased funding and expansion of portions of the Department of National Defense, and larger Defense Portfolio, Canada might emulate China's optimized structure with regards to cyber operations. This could include the expansion of organizations such as the Communications Security Establishment (CSE) and elements of the CAF responsible for enabling and integrating cyber operations with CAF operations. It could also include re-tasking of elements of the Reserve force who may be well suited to the task. This would augment Canada's cyber capabilities towards a level more comparable with China's.

Both China and Russia have enacted policies and practices that promote both internal cyber security and offensive cyber capabilities. Some of these policies are stated publicly, and some must be inferred by the actions of these states. The scope and scale of Chinese and Russian

[15] U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States.* (Official Transcript, 17 Feb 2022), 85.
[16] Stevens, T., Ertan, A., Floyd, K.,Pernik, P., eds. *Cyber Threats and NATO 2030: Horizon Scanning and Analysis.* 32.
[17] "China Cyber Threat Overview and Advisories." CISA.
[18] "Russia Cyber Threat Overview and Advisories." CISA.

offensive cyber activities against the west (including Canada) is quite extensive. Attacks against all types of civilian systems and infrastructure, with little or no evidence of ethical oversight, suggests that targeting and strike authority may have been decentralized and delegated to a lower level than permissible in Canada. Canada adheres to its own laws and all international laws in conducting cyber activities.[19] The Cybersecurity and Infrastructure Security Agency (CISA) summarizes the hostile cyber activities of Russia and China respectively as follows:

> "The Russian government engages in malicious cyber activities to enable broad-scope cyber espionage, to suppress certain social and political activity, to steal intellectual property, and to harm regional and international adversaries….Russian state-sponsored threat actors are targeting the following industries and organizations in the United States and other Western nations: COVID-19 research, governments, election organizations, healthcare and pharmaceutical, defense, energy, video gaming, nuclear, commercial facilities, water, aviation, and critical manufacturing. The same reporting associated Russian actors with a range of high-profile malicious cyber activity, including the 2020 compromise of the SolarWinds software supply chain, the 2020 targeting of U.S. companies developing COVID-19 vaccines, the 2018 targeting of U.S industrial control system infrastructure, the 2017 NotPetya ransomware attack on organizations worldwide, and the 2016 leaks of documents stolen from the U.S. Democratic National Committee…."Russia continues to target critical infrastructure, including underwater cables and industrial control systems, in the United States and in allied and partner countries, as compromising such infrastructure improves—and in some cases can demonstrate—its ability to damage infrastructure during a crisis." The Assessment states that "Russia almost certainly considers cyber attacks an acceptable option to deter adversaries, control escalation, and prosecute conflicts."[20]
>
> "The Chinese government…engages in malicious cyber activities to pursue its national interests. Malicious cyber activities attributed to the Chinese government …continue to target, a variety of industries and organizations in the United States, including healthcare, financial services, defense industrial base, energy, government facilities, chemical, critical manufacturing (including automotive and aerospace), communications, IT (including managed service providers), international trade, education, video gaming, faith-based organizations, and law firms… China is conducting operations worldwide to steal intellectual property and sensitive data from critical infrastructure organizations, including organizations involved in healthcare, pharmaceutical, and research sectors working on COVID-19 response…

[19] "International Law Applicable in Cyberspace," Canada's Efforts to Address Global Issues, Canada, accessed 9 May 2022, https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng
[20] "Russia Cyber Threat Overview and Advisories." CISA.

> "China presents a prolific and effective cyber-espionage threat, possesses substantial cyber-attack capabilities, and presents a growing influence threat." … "China can launch cyber attacks that, at a minimum, can cause localized, temporary disruptions to critical infrastructure within the United States." … "China's cyber-espionage operations have included compromising telecommunications firms, providers of managed services and broadly used software, and other targets potentially rich in follow-on opportunities for intelligence collection, attack, or influence operations."[21]

Among the targets listed, attacks against healthcare systems and infrastructure stand out as a particularly unethical and hostile actions. Malicious and indiscriminate attacks are being perpetrated against every conceivable target on the open networks. "All devices reachable via cyberspace could be potential targets and potential threats."[22] The volume and nature of these attacks perpetrated by both Russia and China suggests either a large state-run cyber force constantly seeking and exploiting vulnerabilities, a reward system where non-governmental criminal elements are rewarded by these states for perpetrating these activities on behalf of the state (officially or unofficially), or both.

Closed networks and tightly controlled cyber activity within China and Russia are shaping a cyber domain that resembles a national territory with closed and protected borders. Russia is pursuing this theory to the extreme and seeks to establish a "Russian segment of the internet," where a technologically independent and self-sufficient Russia plans to gain a decisive defensive advantage in the cyber domain over open-networked states.

> "The Russian Federation is constructing a closed national network. If successfully completed, this state-controlled, technologically independent, and self-sufficient segment of the internet can be disconnected from the global internet by 2024. The segment is based on a national system-of-systems of information security and defence that will protect the Russian regime against internal and external information threats. It will also provide a source of power in the ever-continuing great power struggle and even a decisive advantage on a strategic level in the cyber domain." [23]

---

[21] "China Cyber Threat Overview and Advisories." CISA.
[22] NATO. *Allied Joint Publication-3.20: Allied Joint Doctrine for Cyberspace Operations*, *January 2020*. (NATO Standardization office: NATO Standardization Document Database, 2020).
[23] Stevens, T., Ertan, A., Floyd, K.,Pernik, P., eds. *Cyber Threats and NATO 2030: Horizon Scanning and Analysis.* 9.

The construction of this network is a stark contrast to the open networks of western democracies like Canada's. In an open network, each user and each piece of software connected to the internet are responsible for their own security against any and all threats from threat actors connected to the network. In open networks, resources must be stretched to protect the millions of individual users. In a closed network, threat actors must first penetrate the network itself before seeking to exploit individuals or programs within it. In closed networks resources could be focused mainly on protecting entry points. If seeking to do more to respond to these attacks, Canada might emulate elements of these Russian policies. For example, additional segments of Canada's open networks might be closed, similar to the Defense Wide Area Network (DWAN), to facilitate security measures in critical areas like healthcare. While limiting or restricting open networks in Canada is not in-line with the freedom of information and liberty loved by so many in the West, the threat landscape has developed to the point that further security is warranted. Measures like this might become increasingly necessary as these adversaries persist in tirelessly seeking and exploiting vulnerabilities.

China holds competitions to encourage the discovery of software vulnerabilities. However, whereas in other parts of the world, vulnerabilities identified at these types of competitions are immediately reported to the software developers, the Chinese government instead utilizes them for its own nefarious purposes.

> "China holds a hacking competition, the Tianfu Cup, for their top hackers to find vulnerabilities. However, unlike equivalent competitions elsewhere, which commonly disclose the flaws directly to impacted companies, flaws found at Chinese hacking competitions are given to the Chinese government before companies even hear about them. A flaw in Apple software reported at Tianfu Cup in 2018 was used

> in Chinese cyber espionage campaigns for two months before the vulnerability was discovered and fixed." [24]

Hacking competitions could be used by the Canadian government to recruit talent and strengthen the links between government and civilian cyber professional circles.

The Chinese government has demonstrated its willingness to take action against domestic and international individuals or organizations in support of state objectives or in response to non-compliance with Chinese policies. Monitoring of individual and commercial cyber activity enables the governments of both China and Russia to maintain tight control of their populations and gain advanced notice of vulnerabilities that may be exploited in support of state objectives. Where it is common practice in the Westernized international community to report software vulnerabilities that may impact individual information or sensitive data directly and immediately to the software developer, China enforces mandatory reporting of software vulnerabilities first to the Chinese government so that they may have an opportunity to exploit the vulnerability before it is rectified. Failure to follow government cyber directives can result in penalties.

> "…when an engineer at Alibaba found a vulnerability in Log4j, he reported it directly to Apache (the U.S. vendor responsible) instead of to the Chinese government. This was one of the most serious vulnerabilities last year, impacting millions of websites and applications. Instead of rewarding the engineer, the Chinese government suspended its information-sharing partnership with Alibaba Cloud for six months and cited improper disclosure of Log4j as the primary reason"[25]

As a comparison, the Canadian government responded to the Log4j vulnerability by issuing an advisory,[26] but it is unclear if further action was taken to sanction those responsible.

---

[24] U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States.* (Official Transcript, 17 Feb 2022), 17.
[25] U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States.* (Official Transcript, 17 Feb 2022), 17.
[26] Canada. "Active Exploitation of Apache Log4j Vulnerability." Canadian Centre for Cyber Security, 10 Dec 2021, accessed 9 May 2022, https://cyber.gc.ca/en/alerts/active-exploitation-apache-log4j-vulnerability

There are also many examples of vulnerabilities that have been reported to the Chinese government and that have been subsequently exploited. [27]

Some have argued in the west that western nations should do more than just "naming and shaming" of organizations identified as perpetrating illegal cyber activities.

> "One of my top recommendations is to impose costs and consequences that actually have a bearing and will prevent these actors from undertaking these operations. I don't believe that there has been anything that has necessarily dissuaded China from carrying out these operations. And it is clear that the naming and shaming strategy that we've [the US] pursued over the past few years is relatively ineffective at curbing cyber espionage, and is basically akin to handing their intelligence services a report card on how their operations are functioning."[28]

Canada could also consider more proactive policies in responding to hostile attacks. Canada might consider suspending information sharing partnerships, other sanctions, or even offensive cyber activities against individuals or organizations working against Canada's national interest in the cyber domain. Canada has stated that international laws are, from its perspective, applicable in cyber space,[29] however it has not demonstrated a preparedness to take punitive action if nations like China continue to violate these laws. For example, the fact that there is a Chinese policy of penalizing companies for not reporting vulnerabilities to the Chinese government could justify legal action or sanctions by Canada or the international community. In extreme cases, Canada does have the capabilities to shut down servers or devices used in perpetration of these violations,[30] but is not known to use the capabilities frequently or publicly.

---

[27] U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*. (Official Transcript, 17 Feb 2022), 17.
[28] U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*. (Official Transcript, 17 Feb 2022), 159.
[29] "International Law Applicable in Cyberspace," Canada's Efforts to Address Global Issues, Canada, accessed 9 May 2022
[30] "Cyber Operations." Communications Security Establishment, Canada, accessed 9 May 2022. https://www.cse-cst.gc.ca/en/mission/cyber-operations

One possible counter-argument to the suggestion that Canada should take more action with regards to its cyber policy is that of escalation. It stands to reason that by enacting more proactive cyber policies, Canada might trigger an ever-increasing escalation that leads to open hostilities with these adversaries. However, it has been argued that this increased level of competitive interaction is the new normal, and that persistent engagement in the cyber domain does not justify fear of escalation. "…competitive interaction in cyberspace short of armed conflict in an agreed competition, as opposed to spiraling escalation, best explains the dynamic from persistent engagement and, consequently, prevailing concerns of escalation are unwarranted."[31] Therefore, Canada might reasonably strengthen its policies and enable more proactive cyber responses and defense without a credible threat of escalation.

China and Russia have optimized their organization for both central and decentralized cyber operations layered into operations across the other domains of conflict. As already discussed, Russian pursuit of a dedicated segment of the internet is ongoing. This is not just a policy initiative but structural as well. There will be many different advantages gained by Russia if it is successful:

> "The advantage is based on the differences in freedom of action, common operational picture, command and control and resilience between one nation closing its networks and other nations leaving their networks open and their critical information infrastructure unprotected. These differences create strategic-level structural cyber asymmetry which can influence the way force is used in a state-to-state conflict."[32]

[31] Michael P. Fischerkeller, and Richard J., Harknett. "Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation." The Cyber Defense Review , November 14-15, 2018: Cyber Conflict During Competition (2019): 267.
[32] Stevens, T., Ertan, A., Floyd, K.,Pernik, P., eds. *Cyber Threats and NATO 2030: Horizon Scanning and Analysis.* 9.

While not without economic costs, as removing itself from the international network seems likely to disrupt trade and the exchange of capital and goods so reliant on the internet, this change would undoubtedly increase Russia's cyber security.

China has completed a major restructuring of both its governmental structure and its military that enables coordination across the domains of conflict including the cyber domain. The Chinese government has established at least one department (the National Defense Mobilization Department), and a dedicated branch of the military known as the Peoples' Liberation Army Strategic Support Force (PLASSF) responsible for information, political, space, network, and psychological warfare.[33]

> "In terms of the *Central Military Commission* (CMC), the reorganization saw an expansion from the previous four general departments to fifteen departments, commissions, and offices…. The creation of some of the new departments and commissions also reflects the elevation of key areas to prominence. In particular, the establishment of the CMC National Defense Mobilization Department reflects the growing importance of not only mobilization planning for the PLA, but also the effort at integrating civilian and military efforts in a variety of areas. Chinese concepts of mobilization extend beyond mobilization of manpower and some industrial facilities to the ability to employ key infrastructure for military ends, and the mobilization of key personnel, equipment, and facilities to supplement military forces. This would be especially important in the context of "civil-military fusion" of information warfare resources, including Chinese telecoms, cyber security firms, and information technology industries."[34]

This restructuring has key characteristics that could be emulated by Canada. For example, China has elevated the cyber domain to prominence in its national and military structure. This enables a greater capacity for the conduct of offensive and defensive cyber operations, and layering of these operations with operations in the other domains. China has also elevated the

[33] U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*. (Official Transcript, 17 Feb 2022), 38.
[34] U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*. (Official Transcript, 17 Feb 2022), 35-36.

concept of civil-military integration to a great extent with the creation of the National Defense Mobilization Department. Clearly the Chinese totalitarian government is better situated to civil-military integration than Canada's, however this is a challenge that Canada should recognize and address. Elements of Canada's civilian cyber industries could be integrated into Canada's national cyber capabilities, through reporting requirements, collective training, or collaboration in other ways. Planning could be conducted proactively at the strategic level as to how these industries might integrate into military activities should it become necessary. Civil-Military fusion is not a popular concept in freedom-loving peacetime Canada, but it is not without precedent. During the World Wars, civil military fusion was achieved as the nation was united towards a common cause. If the frequency of these malicious attacks continue in the cyber domain, integration and fusion should also be give increased consideration.

China has also established an organization within its military identified as the People's Liberation Army Strategic Support Force (PLASSF). The PLASSF is responsible for directing and synergizing effects in space with information, electronic, network, psychological, and political warfare.

> "2015, when the PLA underwent the most extensive reorganization since its founding. Almost every aspect of its structure was affected….Relative to the goal of fighting "informationized local wars," a key organization is the new PLA Strategic Support Force (PLASSF). This entity brings China's space, network warfare, and electronic warfare forces under a single structure. The PLASSF's forces are responsible for achieving space dominance, network dominance and electronic dominance, which are in turn essential to establishing information dominance. Notably, the PLASSF also incorporated … the PLA's sole organization that is publicly known to focus on psychological warfare." Political warfare, by influencing perceptions and assessments of military and political decision-makers, complements all other operations. The PLASSF is very much the PLA's Information Warfare Force."[35]

[35] U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States.* (Official Transcript, 17 Feb 2022), 35-38.

This structure enables the PLASSF to apply a large number of personnel and resources towards its strategic vision across all of its areas of responsibility, and ensure that activities are complimentary or mutually supporting.

Canada could partially emulate China's structure with regards to Cyber operations. This could include restructure of government and CAF elements to elevate cyber to a level of resourcing and attention in line with the level of the threat.

> "Currently, Canada addresses cyber threats through the Communications Security Establishment (CSE) (including the Canadian Centre for Cyber Security) and the Department of National Defence (DND)/Canadian Armed Forces (CAF). The CAF's main cyber unit is the Canadian Forces Network Operations Centre (CFNOC). CSE, the Cyber Centre, DND/CAF, and CFNOC also work with domestic partners to protect Canada from cyber threats."[36]

The Canadian Ministry of public safety is currently responsible for public safety in the cyber domain. This is achieved through the Canadian Centre for Cyber Security (CCCS) which is a combined operational organisation responsible for cyber defense across the whole of government and fulfilling the mandates of Public Safety Canada, Shared Services Canada, and the Communications Security Establishment with regards to Cyber security.[37] The Ministry of public safety has issued a National cyber security Strategy,[38] and a National cyber security action plan.[39] These documents have a domestic and inherently defensive focus. With regards to international cyber monitoring and Canada's offensive Cyber activities, one must look at the

[36] Kristen Csenkey, "Protecting Canada and improving cyber defence: three challenges." *Hill Times*, 24 May 2021. Accessed 3 May 2022, https://www.hilltimes.com/2021/05/24/protecting-canada-and-improving-cyber-defence-three-challenges/298196

[37] "About the Cyber Centre." Canada, Canadian Centre for Cyber Security, Accessed 9 May 2022. Accessed at https://cyber.gc.ca/en/about-cyber-centre

[38] Canada, *National Cyber Security Strategy,* (Public Safety Canada, 2018)

[39] Canada. *National Cyber Security Action Plan (2019-2024)*, (Public Safety Canada, 2019)

CSE within the Defense Portfolio.[40] Reporting to the Minister of National Defense (MND) the CSE is responsible for international Signals Intelligence (SIGINT) including collection of intelligence from the global communications infrastructure (networks and the internet). The CSE is tasked to "degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security."[41] This organization is Canada's primary means of actively or offensively protecting Canadians from cyber threats when required. In the case of the CAF, the DND has the Assistant Deputy Minister of Information Management (ADM(IM)), who is responsible for the cyber security of the DND itself including the CAF.[42] Within this portfolio is also the CFNOC which is a unit sized organization commanded by a Lieutenant Colonel.[43] "CFNOC's Mission is to gain and maintain Cyber superiority within the DND/CAF's Cyber AOR in order to assure friendly forces freedom of action."[44] In Strong Secure Engaged, Canada's Defense Policy, the vision is clear that DND will develop an offensive cyber capability and use it within all applicable laws and conventions.

> "We will assume a more assertive posture in the cyber domain by hardening our defences, and by conducting active cyber operations against potential adversaries in the context of government-authorized military missions. Cyber operations will be subject to all applicable domestic law, international law, and proven checks and

[40] "Defence Portfolio." Canada, National Defense. Accessed 9 May 2022. https://www.canada.ca/en/department-national-defence/corporate/defence-portfolio.html

[41] "Mandate." Canada, Communications Security Establishment, accessed 9 May 2022. https://www.cse-cst.gc.ca/en/corporate-information/mandate

[42] "Assistant Deputy Minister (Information Management)," National Defense Organizational Structure - ADM (IM) mandate and DND, Canada, Accessed 30 Apr 2022. https://www.canada.ca/en/department-national-defence/corporate/organizational-structure/assistant-deputy-minister-information-management.html

[43] "Director General Information Management Operations/Deputy CF-J6." Canada, About ADM(IM), Organization and Leadership, accessed 9 May 2022. http://admim-smagi.mil.ca/en/about/organization/dgimo.page

[44] "Director General Information Management Operations/Deputy CF-J6." Canada, About ADM(IM), Organization and Leadership, accessed 9 May 2022. http://admim-smagi.mil.ca/en/about/organization/dgimo.page

balances such as rules of engagement, targeting and collateral damage assessments."[45]

The mandates and structures are clear, however the dispersal of these organizations between the CAF and other establishments under the MND does not allow for the level of flexibility and synergy across domains that are possible within China's cyber structure. China's PLASSF is structured to conduct information, political, space, network, and psychological warfare and is integral to the Chinese Military as part of the PLA. There is no single organization within the CAF or DND that can conduct operations in these areas and synergize their effects under one common strategic military aim. Canada could consider establishing its own version of the PLASSF within the CAF for operational support to the CSE in peacetime, and to enhance its capability to conduct and coordinate these activities in a military context should the need arise.

One other way in which Canada might emulate China's civil-military integration in support of Cyber activities is through a re-tasking of some of the Reserve force. It has been argued in the past that Reserve soldiers might be well suited to the role of cyber operator.[46] Due to equipment shortages and training bottlenecks, some combat trades (especially in the Reserves) struggle to maintain sufficient troops and the required readiness levels.[47] Some reservists are also tech savvy students or Information Technology (IT) professionals in their careers outside of the military.[48] Cyber operations might synergize more naturally with many reservists' civilian

---

[45] Canada. *Strong Secure Engaged - Canada's Defense Policy* (Department of National Defense, 2017). 15.

[46] Bill Williams, "Cyber Warriors: Army Reserve units take up mission task of cyber operators," *Canadian Army Today,* Feb 2020. Accessed Apr 2022. https://canadianarmytoday.com/cyber-warriors-army-reserve-units-take-up-mission-task-of-cyber-operators/

[47] Ashley Burke, "Military Readiness 'one of the things that keeps me awake at night,' says Canada's top soldier," *CBC News*, 20 March 2022. https://www.cbc.ca/news/politics/canada-military-state-of-readyness-1.6380922

[48] Bill Williams, "Cyber Warriors: Army Reserve units take up mission task of cyber operators," *Canadian Army Today,* Feb 2020. Accessed Apr 2022. https://canadianarmytoday.com/cyber-warriors-army-reserve-units-take-up-mission-task-of-cyber-operators/

training than some other roles like the combat arms. If cyber operations could be conducted from Canada, reservists could serve in operational detachments as shift workers either in the evenings or on weekends in addition to their civilian employment. By engaging these soldiers in cyber operations they could be an active part of Canada's defense and combine their military and civilian training while reducing the log-jam of reservists moving through the system to be trained in other roles.

Canada remains relatively evenly matched technologically with its adversaries. However, both China and Russia have surpassed Canada in their willingness to embrace policies and implement structures that enable cyber activities and the integration of cyber activities with operations in other domains. Russia has surpassed Canada in terms or its policy governing defensive cyber operations. If it is successful in establishing its own "segment of the internet" Russia will gain a notable defensive advantage in the cyber domain. Elements of this policy and this mindset could and should be incorporated into Canadian cyber policies and practices to start to close the capability gap that exists. Critical sections of Canada's cyber domain could be protected within closed networks where possible, with a view towards establishing a cyberspace with defensible chokepoints on which to focus national resources. Additional partnerships could be established or planned between the Canadian government and Canada's civilian cyber organizations in order to share best practices, conduct cross-training and prepare for increased civil-military integration should the need arise. If an escalation were to occur in which Canada needed to match adversaries' frequency and volume of offensive operations in the cyber domain, Canada may need to explore the delegation of strike authority to levels more comparable with its adversaries. This could help prevent bottle-necks at the decision making level in a domain where rapid decisive action is critical. China has optimized its cyber structure with the establishment of

a Department of Civil-Military integration, as well as the PLASSF. These organizations are disruptive in their capacity to synergize effects across multiple domains and integrate all levels of the Chinese civil industry (including Cyber) into the military if required. Specifically the PLASSF is a large organization spanning several key areas of responsibility and able to integrate effects in multiple domains into military operations. Canada could establish a military force with similar capabilities, by either expanding on existing organizations or creating a new one. Additionally, the DND and CAF could explore the option of dedicating additional reserve force personnel, from trades facing critical equipment shortages, to reinforce efforts to expand the CAF's cyber capability. Ultimately, Canada should act quickly, learning from the advancements of these adversaries, emulating where possible, and responding strongly when required to move towards parity in the cyber domain.

BIBLIOGRAPHY

NATO. *Allied Joint Publication-3.20: Allied Joint Doctrine for Cyberspace Operations*, *January 2020*. NATO Standardization office: NATO Standardization Document Database. https://www.gov.uk/government/publications/allied-joint-doctrine-for-cyberspace-operations-ajp-320

Major Neil B. Marshall "Offensive Cyber in the Canadian Armed Forces: Opportunities from Bill C-51." Canadian Forces College, 2016. https://www.canada.ca/en/army/services/line-sight/articles/2022/02/offensive-cyber-in-the-canadian-armed-forces-opportunities-from-bill-c-51.html

Stevens, T., Ertan, A., Floyd, K.,Pernik, P., eds. *Cyber Threats and NATO 2030: Horizon Scanning and Analysis.* Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, January 2021. https://kclpure.kcl.ac.uk/portal/en/publications/cyber-threats-and-nato-2030-horizon-scanning-and-analysis(3724c535-e782-45cf-9272-046670e7100f).html

CISA. (n.d.). "Russia Cyber Threat Overview and Advisories." Cybersecurity and Infrastructure Security Agency. Accessed April 13, 2022. https://www.cisa.gov/uscert/russia

U.S.-China Economic and Security Review Commission. "Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States." Official Transcript. 17 Feb 2022. https://www.uscc.gov/hearings/chinas-cyber-capabilities-warfare-espionage-and-implications-united-states

CISA. (n.d.). "China Cyber Threat Overview and Advisories." Cybersecurity and Infrastructure Security Agency. Accessed April 13, 2022. https://www.cisa.gov/uscert/china

CADSI. *From Bullets to Bytes: Industry's Role in Preparing Canada for the Future of Cyber Defence*. Canadian Association of Defence and Security Industries, 2019. Accessed at https://www.defenceandsecurity.ca/UserFiles/Uploads/publications/reports/files/document-24.pdf

Canada. *Department of National Defense and the Canadian Armed Forces 2019-2020 Departmental Results Report*. Ottawa: Department of National Defense, 2020. https://www.canada.ca/content/dam/dnd-mdn/documents/departmental-results-report/2019-20-drr/english/DRR%202019-20_DND_English_FINAL%204%20Nov%202020%20-%20PDF%20Website.pdf

Perry, Dave. “Developing the CAF’s Cyber Force.” Interview with BGen Patrice Sabourin Director General Information Capabilities Force Development at the Department of National Defense. *Defence Deconstructed Podcast,* Canadian Global Affairs Institute. January, 2021. https://www.cgai.ca/developing_the_cafs_cyber_force

Canada. “National Cyber Security Strategy.” Public Safety Canada. 2018. Accessed at https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx

Williams, Bill. “Cyber Warriors: Army Reserve units take up mission task of cyber operators.” *Canadian Army Today,* Feb 2020. Accessed Apr 2022. https://canadianarmytoday.com/cyber-warriors-army-reserve-units-take-up-mission-task-of-cyber-operators/

Canada. “Active Exploitation of Apache Log4j Vulnerability.” Canadian Centre for Cyber Security. 10 Dec 2021. https://cyber.gc.ca/en/alerts/active-exploitation-apache-log4j-vulnerability

Canada. “Assistant Deputy Minister (Information Management)”. National Defense Organizational Structure - ADM (IM) mandate and DND. Accessed 30 Apr 2022. https://www.canada.ca/en/department-national-defence/corporate/organizational-structure/assistant-deputy-minister-information-management.html

UK. *Joint Doctrine Note 1/18 Cyber and Electromagnetic Activities*. Concepts and Doctrine Centre, 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

Ashley Burke, “Military Readiness ‘one of the things that keeps me awake at night,’ says Canada’s top soldier,” *CBC News*, 20 March 2022. https://www.cbc.ca/news/politics/canada-military-state-of-readyness-1.6380922

Canada. Pan-Domain Force Employment Concept – Prevailing in an Uncertain World. Department of National Defense. DRAFT.

Canada. “International Law Applicable in Cyberspace,” Canada’s Efforts to Address Global Issues Canada. Accessed 9 May 2022. https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng

Communications Security Establishment Act S.C. 2019, c. 13, S. 76. (2019). Accessed at https://laws-lois.justice.gc.ca/eng/acts/C-35.3/page-1.html

Canada. “Mandate.” Communications Security Establishment. Accessed 9 May 2022. https://www.cse-cst.gc.ca/en/corporate-information/mandate

Canada. “National Cyber Security Action Plan (2019-2024).” Public Safety Canada, 2019. Accessed at https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/index-en.aspx

Canada. “Canadian Centre for Cyber Security.” Accessed 9 May 2022. Accessed at https://cyber.gc.ca/en/

Canada. *Strong Secure Engaged - Canada’s Defense Policy*. Department of National Defense, 2017.

Canada. “Cyber Operations.” Communications Security Establishment. Accessed 9 May 2022. https://www.cse-cst.gc.ca/en/mission/cyber-operations

Kristen Csenkey, “Protecting Canada and improving cyber defence: three challenges.” *Hill Times*, 24 May 2021. Accessed 3 May 2022. https://www.hilltimes.com/2021/05/24/protecting-canada-and-improving-cyber-defence-three-challenges/298196

Canada. “Defence Portfolio.” National Defense. Accessed 9 May 2022. https://www.canada.ca/en/department-national-defence/corporate/defence-portfolio.html

Canada. “Director General Information Management Operations/Deputy CF-J6.” About ADM(IM), Organization and Leadership, accessed 9 May 2022. http://admim-smagi.mil.ca/en/about/organization/dgimo.page

Fischerkeller, Michael P., and Richard J., Harknett. “Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation.” The Cyber Defense Review , SPECIAL EDITION: International Conference on Cyber Conflict (CYCON U.S.), November 14-15, 2018: Cyber Conflict During Competition (2019), pp. 267-287