CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

Canada's Active Cyber Defence is Anything But Active

by Alexander Rudolph

July 2021

POLICY PERSPECTIVE

CANADA'S ACTIVE CYBER DEFENCE IS ANYTHING BUT ACTIVE

by Alexander Rudolph

July 2021

CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

Prepared for the Canadian Global Affairs Institute
1800, 150 – 9th Avenue S.W., Calgary, AB T2P 3H9
www.cgai.ca

ISBN: 978-1-77397-203-9

Canada's Active Cyber Defence is Anything But Active

Much has been said of the Canadian government's 2017 defence policy, *Strong, Secure, Engaged* (SSE). However, the implementation of its active cyber policy in the Canadian Armed Forces (CAF) lacks analysis. SSE established that the federal government will develop the means to conduct active cyber operations as part of an assertive posture to operate strategically in cyberspace, including offensively with the Department of National Defence (DND) and the CAF. This commitment comes after the North Atlantic Treaty Organization (NATO) declared that cyberspace is a warfighting domain in 2016 and NATO's Cyber Defence Pledge, which reaffirmed the need for NATO members to enhance cyber defence as part of their collective defence commitment. Now, nearly four years after SSE, what is the state of Canada's cyber defence and has the government met its obligations? Unfortunately, the CAF's development of new active cyber capabilities has been anything but active.

The active cyber provisions in SSE were a significant policy change over previous Canadian government administrations which focused on cyber security over cyber defence. Cyber defence is a more active approach that emphasizes engagement against threats to national defence through the use of cybercraft - "the skillful management of cyber ways and means to achieve your ends." Active cyber capabilities are used to engage threats to Canadian defence using offensive cyber operations (OCOs) and defensive cyber operations (DCOs). SSE has a tacit understanding of these approaches when it separates cyber security and situational awareness from other active capabilities, including offensive operations.

SSE only refers to specific target capabilities related to the development of active or offensive operations in the CAF when it states that it will develop the means to "target, exploit, influence, and attack in support of military operations" in cyberspace as part of a broad improvement in information capabilities. "Active cyber operations" is a creative term that broadly refers to "response activities and operations conducted on or through the global information infrastructure to influence, interfere, degrade or disrupt the capabilities, intentions or activities of an adversary." Although active cyber operations are not exclusively offensive, their use in a military context centres on both defensive and offensive capabilities.

Despite these obligations and commitments under SSE and NATO provisions, recent interviews, reports and information gathered through open-source intelligence indicate that the government and the DND/CAF are failing to meet their goals to develop active cyber capabilities. Further, there are indications that the CAF is not only behind in developing these capabilities but is potentially more than a decade behind its key allies on integrating these capabilities into the armed forces. The DND and CAF are unable to claim they can secure Canada in cyberspace or engage in OCO in support of the military unless they become serious about their cyber-defence policy and cyber-force development.

Canadian Cyber-Defence Policy History: Under-promise, Under-deliver

In contrast to SSE, the Harper government's 2010 Cyber Security Strategy saw state cyber operations as a tertiary threat. The strategy emphasized a generalized approach led by Public Safety Canada, which focused on the economic need to secure Canadians in cyberspace. While the strategy notes threats from state actors, it labels them as tertiary. Front and centre is a recognition of the need to "defend Canada's sovereignty, national security and economic interests" in cyberspace. The strategy was criticized due to the delay in developing such a policy and for its lack of urgency or reflection on the scope of challenges. Further, the strategy was also criticized for a lack of action in addressing the use of cyberspace by revisionist and adversarial powers, including Russia and China, for aggressive and authoritarian purposes.

Although the strategy addressed cyber defence and set goals for the DND, its goals were not ambitious, nor did they keep pace with cyber-defence capabilities internationally. In 2010, both the United States and United Kingdom had begun the process of institutionalizing co-operation between their signal intelligence organizations and militaries to develop active capabilities in the armed forces. It would take another seven years for Canada to announce co-operation in the same manner, and one more before it was legally possible, but full institutional co-operation between the two remains non-existent. On Canada's side, the 2010 development of offensive cyber capabilities looked more like what the U.S had done in the 1990s. The strategy's commitments to strengthening cyber security in the military produced three deliverables: the creation of a Canadian Forces cyber task force and director general cyber; the development of information exchange with allies; and the strengthening of the capacity to defend networks.

While all three of the deliverables were achieved, their effectiveness is doubtful. Despite guidance from the chief of the defence staff (CDS) in 2013 to support the task force and its mission, the task force struggled to accomplish any of its goals due to a severe lack of personnel, institutional and force structures to enable its mission. Also, command authority to conduct these operations was dispersed across different departments and directorates with conflicting authorities, priorities and mandates. While information exchange did and does occur, Canada did not join some critical information exchange venues. This includes NATO's Cooperative Cyber Defence Centre of Excellence, its primary instrument for information exchange on cyber defence, which Canada did not join until 2020. Last, although the Canadian Forces Network Operations Centre (CFNOC) has existed for some time to secure the DND/CAF's networks and was bolstered during this time, the CFNOC does not have the mission to conduct OCOs.

The CAF's difficulties in developing cyber defence under the 2010 strategy persisted into Prime Minister Justin Trudeau's administration, leading to the eventual policy change in SSE. Under SSE, the Trudeau government sought to address these issues and provide DND/CAF the means and mandate to develop a cyber defence and offensive cyber capabilities. SSE only refers to the development of active or offensive operation-specific capabilities in the CAF when it states that it will develop the capabilities to "target, exploit, influence, and attack in support of military operations" in cyberspace as part of a broad improvement in information capabilities. These are the foundational categories of cyber capabilities meant to deliver effects in cyberspace, which are

more comparable with skills or knowledge that are developed and trained rather than just a checklist of capabilities.

Present: Where Are We Now?

Four years after SSE, recent interviews with DND/CAF personnel on cyber-force development and departmental plans have clarified that progress is (technically) being made. The DND/CAF's 2019-2020 departmental plan results report indicate that the CSE and the CAF have been working together to develop active cyber capabilities, and to some apparent success. However, the only success noted is for targeting, and it is stressed that "more work is required to generate targeted effects within the Information domain." While this is progress towards improving capabilities in the armed forces, it is far below the necessary threshold set out in SSE to exploit and attack in cyberspace.

Although there has been progress in some capabilities related to cyber-threat intelligence, attribution and targeting, the extent and knowledge of these capabilities lack specificity. Cyber-threat intelligence and attribution are related to understanding who the threat actors are and determining who conducted an attack, which are largely associated with DCOs. While these capabilities are integral to the armed forces' ability to project force in cyberspace, they do not amount to the DND/CAF possessing offensive capability. The severity of this growing capabilities gap is highlighted by the fact that the CAF achieved 98 per cent of its objectives in 2019-2020, with two per cent not achieved due to COVID-19 and because "the CAF continues to refine its ability to integrate cyber enabled effects in CAF-led operations."

The DND and CAF are aware of the cyber-capabilities gap. In an episode of the podcast, "Defence Deconstructed," Brig.-Gen. Patrice Sabourin, director general information capabilities force development, explained the motivation behind the recent title change from director general cyberspace. He noted this change reflected the CAF being "more attuned [to] our new roles and responsibilities because we need to look at not only developing our cyber capabilities, but everything else we do." However, we should be cautious about how this relates to the DND/CAF's offensive cyber capabilities and strategic posture in cyberspace when discussions remain focused on institutionalizing and centralizing organizational control of their data infrastructure. Institutional structures that enable co-operation between the DND/CAF and the CSE are needed beyond the current informal, ad hoc process.

The lethargic progress of cyber-defence capabilities is no surprise to those who have been following these developments. In 2019, a Canadian Association of Defence and Security Industries (CADSI) report stated: "CAF is trailing allies and adversaries in certain cyber defence capabilities." CADSI highlights that the threats to the DND/CAF span vulnerabilities in domestic critical infrastructure, combat systems and equipment that have some form of cyber connectivity. CADSI notes that a key reason for this is distrust between the cyber-defence industry and Canada, emanating from years of unproductive engagement, lack of communication and a lack of understanding of each other's capabilities. While admittedly an industry group like CADSI may

have certain interests in mind, the government's failure to address these gaps is not limited to the DND.

Implications

If the DND/CAF cannot conduct active cyber-defence operations, they may have to rely upon the CSE. Bill C-59, an *Act Respecting National Security Matters*, which received royal assent in 2019, states that the CSE can provide technical assistance to the DND for active operations. If the CSE is requested to operate in this fashion, it would be assuming dual authority on behalf of both itself and the DND and would fall under the laws which cover both. This collaboration is not bad in theory, but is the common mode of developing cyber-force structures among NATO countries due to its niche knowledge and skill set required. The most well-known example of this is the United States Cyber Command, which is a collaboration between the National Security Agency, the United States' signal intelligence organization, and the United States Department of Defense. Recent information indicates that the CSE and the DND/CAF are in the planning stages towards a similar type of organization, but public information remains limited on a timeline for its creation. The lack of information on this initiative also raises serious implications for the CSE's civilian employees.

A significant policy concern related to the CAF's deprioritized force development of cyber capabilities is an increased reliance on its intelligence organizations, particularly the CSE. If the CAF's lack of capabilities is of no concern, Canadians and the government need to grapple with the idea of civilians in the CSE conducting military cyber operations on behalf of the Canadian military. The idea of the CAF having to call civilians partners to conduct operations in cyberspace, either abroad or domestically, has implications for domestic and international law concerning the use of force in cyberspace. Leah West has explored some of the legal implications of the CSE's expanded mandate to support its CAF partners in active cyber operations, including the implications of civilians conducting operations on behalf of the military and being considered combatants. West says that "[as] combatants, CSE employees could not only lawfully support the conduct of lethal operations and benefit from prisoner of war status, they could also be legally targeted."

The July 2020 cyberattack on the Royal Military College (RMC) and the Colonial Pipeline attack can shed light on what would happen if Canada came under attack in cyberspace from an advanced persistent threat (APT), a highly capable threat actor often sponsored by a state. The RMC suffered a ransomware attack that reportedly led to the release of financial information in a folder entitled "Student DB." This was a comparatively small breach. On May 9, President Joe Biden declared a state of emergency in 17 states after a ransomware attack forced the Colonial Pipeline to shut down, cutting off 45 per cent of the supply of fuel consumed by the East Coast. In both incidents, the perpetrators were cybercriminals, and the RMC and Colonial Pipeline had to work with federal government partners for assistance. In the event of a similar attack by a state

or an APT, the Canadian military would have significant difficulty in defending itself and responding on its own.

The Future of CAF's Cyber Force

Despite the bleak picture presented here, there is some cause for optimism for greater coherency in cyber doctrine and force development of capabilities. The best news for cyber-policy watchers is the promotion of Lt.-Gen. Frances J. Allen to vice-chief of the defence staff (VCDS). Allen previously held positions commanding the CFNOC and the Canadian Forces Information Operations Group, and has served as director general cyberspace and director general information management. Allen understands the nuance of cyber beyond being just a toolset, but rather as a domain of operations that requires persistent action to develop capabilities and defend Canadians from threats in cyberspace.

Allen has shown incredible leadership and insight in developing the CAF's information capabilities and may be the type of leader needed to break the stagnation on the DND's cyber portfolio. The DND/CAF have predominantly been reactionary in their force development of cyber capabilities, but there is a potential shift in thinking about that and big changes could be on the horizon. Sabourin discussed the development of an information capabilities roadmap for improvements, which comes as part of an awareness of the growing information capabilities gap. As we near four years post-SSE, the fact that a capabilities roadmap is only now in development is perhaps the most significant recent testament to how far behind Canada is in developing basic cyber defence in the armed forces.

Ultimately, the appropriate people and title mean little for a lack of institutional structures which enable greater co-operation between the CSE and the DND/CAF. Some of Canada's key allies, including the U.S., the U.K., Australia and many others, began integrating offensive cyber capabilities into their armed forces more than a decade ago. In some cases, it is two (or nearing three) decades. The key trait among these allies, which Canada lacks, is institutional structures between the CSE and the DND/CAF to develop and implement these capabilities. In the coming year, major changes may be coming to how the DND/CAF organize their command structures related to their cyber capabilities. The DND/CAF 2021-2022 Departmental Plan indicates that they, along with the CSE, will develop capabilities under a "unified leadership and management structure". No information exists on what this unified structure will look like. The longer that structures are absent, the longer Canadian cyber defence will suffer. As VCDS, Allen has a mandate to "[provide] strategic direction across the Defence team and [monitor]… progress in achieving key priorities." This positions Allen as one of the most influential people to direct the reorganization of the management structure to institutionalize offensive operations in the CAF.

Although Allen has been on the job for less than a year, hints of what a unified cyber-command structure could look like come from Allen's 2002 master's thesis on the integration of computer network attack and exploit capabilities in the CAF. Allen makes a strong case for the integration of these capabilities into the CAF's special operations command structure where they should be

treated as special operations capabilities. As Allen noted in 2002, special operations' close co-operation and mutual support with the intelligence community offer parallels to similar training and command-and-control structures in adopting active cyber capabilities in the armed forces.

About the Author

Alexander Rudolph *is a Ph.D. student in the Department of Political Science at Carleton University. Alex's research explores grand strategy, conflict, and competition in cyberspace. As part of his research, Alex incorporates methodologies from sociology and information security to inform research into the strategic thought of cyberspace, comparative cyber defense policy, and Canadian cyber defence policy (or lack thereof).*

Outside of his academic work, Alex is an American-Canadian ex-pat and regularly contributes to Canadian and international discussions on cyber conflict. Alex has more than 10 years of experience working for non-profits in the public education and advocacy sectors as a project manager and analyst. Presently, Alex is Vice-President of Emerging Leaders in Canadian Security, a non-profit dedicated to supporting young and new professionals in Canadian security and defence, and works in Ottawa as a research coordinator in defence consulting.

Canadian Global Affairs Institute

The Canadian Global Affairs Institute focuses on the entire range of Canada's international relations in all its forms including (in partnership with the University of Calgary's School of Public Policy), trade investment and international capacity building. Successor to the Canadian Defence and Foreign Affairs Institute (CDFAI, which was established in 2001), the Institute works to inform Canadians about the importance of having a respected and influential voice in those parts of the globe where Canada has significant interests due to trade and investment, origins of Canada's population, geographic security (and especially security of North America in conjunction with the United States), social development, or the peace and freedom of allied nations. The Institute aims to demonstrate to Canadians the importance of comprehensive foreign, defence and trade policies which both express our values and represent our interests.

The Institute was created to bridge the gap between what Canadians need to know about Canadian international activities and what they do know. Historically Canadians have tended to look abroad out of a search for markets because Canada depends heavily on foreign trade. In the modern post-Cold War world, however, global security and stability have become the bedrocks of global commerce and the free movement of people, goods and ideas across international boundaries. Canada has striven to open the world since the 1930s and was a driving factor behind the adoption of the main structures which underpin globalization such as the International Monetary Fund, the World Bank, the World Trade Organization and emerging free trade networks connecting dozens of international economies. The Canadian Global Affairs Institute recognizes Canada's contribution to a globalized world and aims to inform Canadians about Canada's role in that process and the connection between globalization and security.

In all its activities the Institute is a charitable, non-partisan, non-advocacy organization that provides a platform for a variety of viewpoints. It is supported financially by the contributions of individuals, foundations, and corporations. Conclusions or opinions expressed in Institute publications and programs are those of the author(s) and do not necessarily reflect the views of Institute staff, fellows, directors, advisors or any individuals or organizations that provide financial support to, or collaborate with, the Institute.