TRIPLE HELIX

Following the Digital Snail's Trail: The Short History of Canadian Armed Forces Cyber Operations

By Alexander Rudolph

March 2026

POLICY PERSPECTIVE

Following the Digital Snail's Trail: The Short History of Canadian Armed Forces Cyber Operations

by
Alexander Rudolph

March 2026

Prepared for Triple Helix
Suite 200, 8 York Street, Ottawa, ON K1N 5S6

www.cgai.ca/triple_helix

Following the Digital Snail's Trail: The Short History of Canadian Armed Forces Cyber Operations

By Alexander Rudolph

Introduction

In September 2024, the Department of National Defence (DND) and the Canadian Armed Forces (CAF) officially created CAF Cyber Command (CAFCYBERCOM). For many Canadians, this may be the first time they have heard about the CAF's development of cyber capabilities, but CAFCYBERCOM is the culmination of nearly 25 years of development. Indeed, CAFCYBERCOM is a significant milestone to be applauded. However, achieving this milestone was no easy feat and has been filled with struggles since the start of the CAF's cyber defence operations in 1999. Although there was persistent effort from within DND/CAF's cyber and information management organization to push for the changes needed, a lack of buy-in and institutional resistance meant that major change and progress in CAF cyber operations would only occur when internal DND/CAF and international pressures reached a critical point to motivate the Government of Canada to make the changes needed to improve cyber defence. Despite this long history, the creation of CAFCYBERCOM has led to an elevated profile of cyber defence and operations in national defence, and is quickly building institutional inertia to be proactive in Canadian cyber defence as opposed to being responsive.

Ancient Times – 1990s to 2009

In 1999, DND/CAF recognized that their networks and information systems could be attacked, which led directly to the creation of the Information Protection Centre, which comprised the DND Computer Incident Response Team and National Vulnerability Assessment Team. This would become the CAF's primary computer network defence and cyber security capability as it joined its North Atlantic Treaty Organization (NATO) allies in Afghanistan in 2001. By this point, the United States was already deeply involved in digitizing its forces and integrating elements of network-centric warfare, which emphasized the integration of computers and networking to improve the speed of command and control. DND/CAF were digitizing as well, but not at the pace nor scale of the United States. This served as a motivation for greater digitization within DND/CAF to maintain its ability and advantage of working alongside the United States and because they saw and wanted these networked benefits for the CAF.

In Canada, the Communications Security Establishment (CSE) acquired approval in 2002 to conduct penetration tests of government networks, starting with DND/CAF. CSE and internal

DND/CAF penetration tests informed the creation of the Canadian Forces Network Operations Centre in 2004 by highlighting any areas for improvement that centralizing network operations would support. Following the creation of the Canadian Forces Network Operations Centre, there is little public information about DND/CAF's development of the CAF's cyber capabilities throughout the 2000s. A significant reason for this is that the CAF viewed cyberspace as a subcomponent of C4ISR, not as a domain of operations. This is problematic, as it views cyberspace as a tool and overlooks activity in and through cyberspace as a domain. As a comparison, this would be akin to looking at the air domain by only looking at airports; you miss everything that happens in the air. DND/CAF's lack of conceptual and definitional understanding of cyberspace contributed to a lack of digital transformation throughout the forces. However, this lack of development was not ignored, and there were internal and external pressures to shift the policy to develop the CAF's cyber capabilities.

By the late 2000s, Canada and its NATO allies were under increasing attack through cyberspace, which began to motivate strategic and organizational change in both Canada and NATO. One of the first major incidents was the cyber attacks on Estonia in 2007, which motivated NATO allies to create the Cyber Defence Management Authority and Cooperative Cyber Defence Centre of Excellence at the 2008 Bucharest Summit. The Cyber Defence Management Authority centralized the cooperation and management of allied responses to cyber attacks while the Cooperative Cyber Defence Centre of Excellence helped to research and develop long-term doctrine and strategy on cyber defence. In addition to creating these organizations, NATO pushed allies to do more to improve their cyber defence. The member that took the lead on cyber defence was the United States, which began the initial phases of developing United States Cyber Command, which was completed in 2010. While this occurred, CSE found rampant penetration and data theft by adversarial states, including Russia and China, across the Government of Canada networks. These events helped influence the release of the Government of Canada's first National Cyber Security Strategy in 2010.

One Step Forward, Two Steps Back– 2010 to 2016

The National Cyber Security Strategy was a significant milestone in improving Canadian cyber defence, but there was little specific direction for DND/CAF in this first strategy. DND/CAF was given three tasks as part of the National Cyber Security Strategy: Strengthen DND/CAF's cybersecurity capabilities to improve the defence of networks; create a Canadian Forces Cyber Task Force and a Director General Cyber organization; and learn about cyber best practices from allies. The strategy received $244 million in funding, but 84% of which went to the CSE to "enhance its ability to defend government systems and networks," meaning DND/CAF would have to make do with existing resources. By the end of 2010, DND/CAF had created an ad hoc Cyber Task Force and Director General Cyber positions and was actively engaged in improving cyber defence and learning best practices from allies. Still, problems

would begin to show in how DND/CAF managed its cyber capabilities. The problem in question was overlapping, redundant, and unclear authorities, responsibilities, and accountabilities across multiple Assistant Deputy Ministers and organizations in DND/CAF. By 2012, there were multiple Level 1 or Level 2 organizations handling at least some portion of DND/CAF cyber capabilities, including Assistant Deputy Minister Information Management and Director General Cyber, who reported to the Vice Chief of the Defence Staff, and was also the Director Cyber Force Development and reported to the Chief of Force Development. The Cyber Task Force created to streamline cyber capabilities and enable further cyber force development ultimately failed because of a lack of command authority; unclear authorities, responsibilities, and accountabilities; and insufficient buy-in from DND/CAF culturally and as an institution.

Shared Services Canada

Just as the Cyber Task Force and DG Cyber were created and attempted to navigate the conflicting authorities, responsibilities, and accountabilities to optimize the CAF's cyber capabilities, their efforts were severely hampered by the creation of Shared Services Canada. Shared Services Canada was created in 2012 to centralize the management of the Government of Canada's information technology infrastructure and services, including networks belonging to DND and the CAF. By most accounts, Shared Services Canada's takeover and management of these services was a disaster. Military officers described Shared Services Canada as having caused "significant inefficiency at every level including in service delivery, procurement, resource management and delegation of authority." It was only because of the dedicated work of DND/CAF that there was no severe impact on operations, but it was noted that there was deterioration in Army training.

Changing Tides

In 2013, Chief of the Defence Staff Thomas Lawson issued guidance that sought more joint capabilities, the creation of a cyber force, and recognition of cyberspace as a domain, but this led to little significant progress due to the existing issues with authorities, responsibilities, and accountabilities, and Shared Services Canada, as well as a lack of institutional buy-in. This guidance represents the first tacit recognition by the CAF that cyberspace is a domain of operations, but this would not be institutionalized until years later. As this was occurring, international pressures were increasing. NATO's 2014 Wales Declaration stated that NATO Article 5 can apply to cyber attacks. By 2016, DND/CAF had grown its digital and cyber capabilities and services, but progress remained limited as the institutional problems were unresolved and other capabilities were prioritized. In 2016, NATO's Warsaw Declaration formally recognized that cyberspace is a domain of operations and adopted the Cyber Defence Pledge, through which NATO members agreed to strengthen cyber defence. In parallel, the United States military achieved its initial operating capability with its Cyber Mission Force. Additionally, the United States also began to develop and implement the initial strategic concepts

of persistent engagement, a more confrontational approach to cyber conflict. The influence of these pressures is quite evident as the developments NATO called for were included in Canada's *Strong, Secure, Engaged* (SSE) defence policy in 2017.

Slow Start – 2017 to 2022

The release of SSE in 2017 was a significant milestone for the CAF's development of cyber capabilities. SSE included three primary policy actions defining this initial maturation period of the CAF's cyber force structures. The first major action was fully recognizing that cyberspace is a domain of operations akin to land, air, sea, and space. Next, SSE laid out the plan to create a Cyber Force by establishing a new Cyber Operator occupation trade and further developing career prospects for cyber defence experts. With this Cyber Force, Canada would assume an "assertive posture" by improving cyber defence and developing offensive cyber capabilities. The last component of the new Canadian cyber defence approach was adopting a deterrence framework. This is problematic, as the underlying mechanisms of deterrence are rooted in forms of conflict that do not translate appropriately to cyberspace because they fail to account for its unique technical traits and dimensions.

The Cyber Force was quickly established by creating the Cyber Operator trade, built upon the work of preceding years. The first few years following SSE are characterized by an initial phase of slow development to build out DND/CAF's capacity for cyber operations, which was itself a victim of DND/CAF's overall lack of digital modernization. One success in building the Cyber Force during this period was the establishment of the training program for Cyber Operators, with the first class graduating in 2021. From 2020 to 2022, audits evaluating DND/CAF's information management, the Cyber Forces, and Defence IM/IT Programme all stated that DND/CAF's management of cyber and digital capabilities was deeply disjointed and obstructed due to not well-defined or understood authorities, responsibilities, and accountabilities. This would help push DND/CAF to begin work to resolve these problems. Although many of these issues were known for nearly a decade, their identification in the audits helped to convince DND/CAF leadership that change was needed to ensure the success of DND/CAF cyber defence.

Building an Advanced Persistent Threat – 2022 to Present

Like so much else, Russia's invasion of Ukraine in 2022 had a massive influence on Canada's cyber defence posture and its thinking about cyber operations overall. Canada has consistently been a strong supporter of Ukraine through efforts such as Operation UNIFIER, a military training and capacity-building mission assisting Ukraine, but cyber operations and cyber security support were traditionally not significant components of this assistance. Following the invasion of Ukraine and Russia's prolific use of cyber operations against Ukraine and NATO allies, the United States and NATO encouraged allies to contribute more to address threats

through cyberspace. Prime Minister Justin Trudeau promised that Canada would respond to Russia's aggression, including its cyber attacks. Two major actions immediately followed.

Canada's Latvian Hunt Forward Operation

On 17 March 2022, the Minister of National Defence signed two Ministerial Orders that designated Latvia's and Ukraine's network and information systems as systems of importance. This classification is important because the *CSE Act* allows CSE to operate in Latvia's and Ukraine's networks as well as share critical intelligence to help defend those networks. At some point after these Ministerial Orders, the CAF began a hunt forward operation as part of Operation REASSURANCE and Canada's commitment to the NATO enhanced Forward Presence in Latvia. Hunt forward operations are joint cyber operations in which a military conducts computer network defence operations with a host country, in this case being Latvia. These operations serve multiple purposes, including intelligence gathering, training, sharing best practices, and enhancing the cyber defence relationship between the two countries. This timeline of events aligns with a United States Cyber Command press release in May 2023, which stated that a hunt forward operation in Latvia conducted with the CAF and Latvia had just concluded.

Authorities Review

Parallel to the development of the Latvian operation, Minister of Defence Anita Anand ordered a review of the Prime Minister's Office and Cabinet's authorities to order cyber operations. The review found that the authorities for defensive and offensive cyber operations is rooted in crown prerogative, which is the same authority from which the Government of Canada derives its ability to deploy the CAF. This means that in any context where the Government of Canada can deploy the armed forces, it can also deploy CAF cyber operations. The government's response following this review is measurable as DND/CAF's 2022-23 Departmental Results state that the CAF conducted its first offensive cyber operation in cooperation with CSE. This admission of the CAF conducting its first offensive cyber operation, alongside the ongoing hunt forward operation in Latvia represented a major shift in how Canada would use the CAF for cyber operations. DND/CAF's transparency in reporting its first offensive cyber operation is noteworthy because the Government of Canada could have withheld this information on national security grounds, similar to when special operations forces are deployed. In addition, whereas

CSE is legally required to report when it conducts cyber operations, they are not reported as such when conducted with the CAF. When CSE uses its Technical and Operational Assistance mandate to assist the CAF to conduct offensive cyber operations, these operations are reported as "Technical and Operational Assistance" and not as a foreign cyber operation that CSE is required to report separately. This is effectively a legal loophole for the Government of Canada to hide when CSE conducts offensive cyber operations.

Digital Services Group & CAF Cyber Command

By 2024, the trajectory, capacity, and potential of DND/CAF's cyber capabilities and cyber operations were dramatically improved with the creation of the Digital Services Group and Cyber Command. Nearly a decade after the authorities, responsibilities, and accountabilities issues were first identified, DND/CAF was making significant changes to its institutional structure to address issues associated with authorities, responsibilities, and accountabilities that have been acknowledged for at least a decade. The Digital Services Group combined the Chief Information Officer Group and the Digital Transformation Office into a Level 1 organization to manage the whole of DND/CAF's digital and cyber landscape. The Digital Services Group also exists to provide support to the newly created CAFCYBERCOM, which was designed to elevate the role of cyber operations in the CAF, refine command and control so that the CAF Cyber Commander reports directly to the Chief of the Defence Staff, and consolidate the CAF's Cyber Forces, Signals Intelligence, and Joint Electronic Warfare into one organization. CAFCYBERCOM is unique not only because its domain of operations is comparatively new and complex, but also because of its structure, in which it derives a significant amount of its support from the Digital Services Group as opposed to the CAF. CAFCYBERCOM is not a Level 1 organization but exists as a separate command that reports directly to the Chief of the Defence Staff, similar to the CAF Special Operations Forces Command. This unique structure is what allowed CAFCYBERCOM to stand up quickly without any change or disruption to operations.

Conclusion

A consistent theme through Canada's history of military cyber defence is that change does not occur in cyber defence policy or in the force development of cyber capabilities until international and domestic pressure reaches a threshold. Waiting until pressure from the United States, NATO, CSE, and DND/CAF reached a critical point effectively meant that the force development of CAF cyber capabilities has struggled to keep pace with cyber threats. Further complicating this has been overlapping authorities, responsibilities, and accountabilities problems that made achieving the minimum needs for cyber security and cyber defence inefficient and slow. After 25 years, the consolidation of DND/CAF's digital and cyber management organizations into Digital Services Group and CYBERCOM is a major positive

step, but this is just the beginning. CAFCYBERCOM and Digital Services Group are not automatically positioned to enable CAF cyber defence; they must build their organizations based on lessons learned from the past 25 years. The creation and position of CAFCYBERCOM and Digital Services Group in DND/CAF's overall structure enables them to better manage the cyber capabilities and assets of DND/CAF, but they must now apply change management to align the disparate parts of what these organizations used to be into a unified CAFCYBERCOM/Digital Services Group. The challenges for Digital Services Group and CAFCYBERCOM in the coming years are twofold: complete the change management processes within Digital Services Group and CAFCYBERCOM while using its new streamlined structure and authorities to improve the

CAF's capacity and capability to conduct cyber operations. After CAFCYBERCOM's first year, there is optimism about DND/CAF's new cyber defence posture, but there is still a lot of work to be done.

About the Author

Alexander Rudolph is a Ph.D. Candidate in the Department of Political Science at Carleton University and an expert on Canadian cyber policy. His research examines the grand strategy, conflict, and competition in cyberspace and how states attempt to maintain their monopoly on violence in the digital domain. He applies sociology, information security, and open-source intelligence methods to investigate the strategic thought and doctrine of cyber conflict and how it influences the creation of cyber force structures in military and intelligence organizations. He obtained his MA in Political Science at Carleton University, where he wrote his thesis on Canada's emerging offensive cyber operations posture following Strong, Secure, Engaged. His methods improve existing methods of analysis of cyber conflict by introducing hacker-informed perspectives on cyberspace and cyber conflict.

In addition to his academic work, Alex is an American-Canadian ex-pat and a frequent contributor to Canadian and international discussions on cyber conflict. He has more than 10 years of experience working for non-profits in the public education and advocacy sectors as a project manager and analyst. Recently, he has worked as a researcher and market analyst in defence consulting and presently works in Ottawa as a policy advisor and consultant.

As one of Canada's leading Canadian Armed Forces cyber defence policy researchers, Alex created Canadian Cyber in Context, the first newsletter dedicated to following updates and providing in-depth analysis of Canadian cyber defence.

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 postCold 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.