STRATEGIC PERSPECTIVES

NAADSN
North American and Arctic Defence and Security Network

naadsn.ca

January 21, 2021

An Opportunity for NORAD Modernization in a Joint CA-US Cyber Component

Kristen Csenkey[1]
NAADSN Graduate Fellow
2020 WiDS-CGAI Fellow

MCpl Dominique Philippe Genest[2]
Canadian Intelligence Corps

Executive Summary

- This paper explores the creation of a bi-national Joint Interagency Cyber Component at North American Aerospace Defense Command (NORAD) (JICC-NORAD), to address cyber threats to the North American continent.
- The JICC-NORAD could bolster NORAD modernization and provide an operational arm with the authority as well as the means to address modern threats to, and provide opportunities for, North American continental defence.
- Cyber threats to continental defence present a rising challenge that must be proactively addressed. Offensive cyber operations (OCO) are both conventional and asymmetric, and therefore require novel approaches to addressing a complex threat environment.
- Current structures address cyber threats, but lack the necessary integration for Canada to ensure that national interests are represented in continental cyber defence.
- The establishment of the JICC-NORAD could address continental defence shortcomings in the cyber domain by providing early warning of cyber threats against North America, conducting defensive cyber operations (DCO) in support of NORAD operations, and acting as a hub for agencies, departments, and the private sector to deconflict and coordinate continental cyber defence.
- The JICC-NORAD could provide the opportunity for Canada to reassert its participation in North American continental defence, while managing resources and the political risks associated with increased military contribution.

Introduction

This *Strategic Perspective* explores the creation of a Joint Interagency Cyber Component (JICC) in the North American Aerospace Defense Command (NORAD) as an option to proactively modernize approaches to continental defence and address emerging threats as part of the future of hybrid conflict. The importance of continental defence and NORAD modernization was recently emphasized by US President Joe Biden in his first official call to Prime Minister Justin Trudeau.

Currently, NORAD does not explicitly address cyber threats nor engage in cyber operations (CO) directly. We see the JICC as a potential way to respond to these threats, and as a new avenue for Canadian contribution to NORAD. NORAD is a bi-national organization that includes Canada and the US, with a focus on defending North America through maritime warning and aerospace warning and control. We suggest that the creation of a cyber component integrated in NORAD might help Canada and the US move towards a more pan-domain approach to continental defence.

The JICC-NORAD concept is important to Canada and Canada-US defence cooperation through NORAD, because it could:

1. aid in the development of assets to increase cyber resiliency, capacity, and situational awareness;
2. contribute to NORAD modernization that addresses and keeps pace with emerging threats in a pan-domain environment; and
3. efficiently manage resources and political risks while providing key contributions to North American defence.

The JICC-NORAD is a novel approach to addressing the dynamic continental threat environment. The JICC is fundamentally about enhancing collaboration within NORAD. The JICC-NORAD focuses on utilizing national expertise, fostering a bi-national approach to proactively address cyber threats, and formally facilitating cooperation through dedicated cyber assets. It serves NORAD as an early warning to identify and resolve cyber threats through DCO.

We articulate this concept by first providing a brief outline of the current NORAD organizational structure and mandate. This includes a description of domestic Canadian and US contributions to cyber defence and approaches to continental defence. Following this, we outline the current continental defence threat environment, and briefly show how NORAD modernization has attempted to address gaps in capabilities. After these sections, we introduce the details of and justification for the JICC-NORAD. We conclude by reiterating the importance of this concept and providing comments on next steps.

Continental (Cyber) Defence

NORAD follows a tri-command framework between NORAD, Canadian Joint Operations Command (CJOC), and US Northern Command (USNORTHCOM). NORAD is concerned with continental defence, operates within the aerospace and maritime domains, and is mandated to "deter, detect and defeat air threats to Canada and the

United States" in cooperation with the US. Currently, NORAD does not explicitly address cyber-related threats; however, air domain operations include "coordinating cyber and info ops and developing recommendations on future requirements." NORAD's current organizational structure places cyber-related continental defence threats within the mandate of two US commands.

There are three regions within NORAD: 1) Alaskan NORAD Region (ANR), 2) Canadian NORAD Region (CANR), and 3) Continental US NORAD Region (CONR). CANR focuses on the surveillance, identification, control, and warning of aircraft entering Canadian airspace and directs air defence forces within Canada. In addition, Canada cooperates with the US through NORAD via joint operations, training, and exercises. Within the context of continental defence within NORAD, cyber-related threats are currently addressed by the US Cyber Command (USCYBERCOM) and the US Army Cyber Command (ARCYBER).

USCYBERCOM and NORAD

ARCYBER is the USCYBERCOM mission team tasked to support the combatant USNORTHCOM (among other combatant commands) when it comes to defensive cyber operations (DCO) and OCO. USNORTHCOM focuses on US domestic defence efforts and on continental North America, including Canada. The overarching element of cyber support goes through the Cyber Operations-Integrated Planning Elements (CO-IPE) teams. These cells (or USCYBERCOM detachments) are integrated within USNORTHCOM and provide cyber options for the commander, as well as deconflicting cyberspace with other cyber entities. However, according to open-source literature, they do not have endemic cyber assets because they task back to their home unit.

Canadian Contributions to NORAD and Cyber Defence

Canada's contribution to continental defence takes shape as financial resources, personnel, and assets to NORAD. Through NORAD, Canada is able to focus on surveillance and operational control over domestic airspace to maintain sovereignty. The bi-national nature of the command allows Canada to respond to threats in a cost-effective way that serves domestic interests and fosters cooperation to collectively defend North America. Canadian personnel serve alongside their American counterparts in NORAD-related activities, mainly to support aerospace operations in the North. Internally, Canada contributes to NORAD via CJOC, the Strategic Joint Staff, Vice Chief of Defence Staff, and the Royal Canadian Air Force[3].

Canada addresses cyber threats through the Communications Security Establishment (CSE), the Canadian Centre for Cyber Security (the Cyber Centre), and the Department of National Defence (DND)/Canadian Armed Forces (CAF). CSE is mandated through the *Communications Security Establishment Act* (CSE Act, or see Bill C-59) to protect and defend Canadian cyber systems, acquire foreign intelligence, conduct defensive foreign and active foreign COs, as well as assist domestic law enforcement and security agencies and DND/CAF. The Cyber Centre focuses on defending Government of Canada (GoC) networks from cyber threats and supporting the protection of critical infrastructure (CI) and Canadians online through expert advice, services, and publicly available assessments. The CAF's main cyber unit is the Canadian Forces Network Operations Centre (CFNOC), which is "tasked to conduct defensive operations within DND/CAF's cyberspace to detect, defeat, and/or mitigate offensive and exploitive actions to maintain freedom of action." This unit collaborates closely with the Cyber

Centre to enable DCO. In 2018, the CAF created the Cyber Operator trade, dedicating cyber-trained members to work collaboratively with domestic departments and agencies and international allies to detect and respond to cyber threats, in support of the operational requirements of the Navy, Army, and Air Force. This nascent capability, however, has yet to become fully operational. Current cyber capability development is managed through the Director General Information Capabilities Force Development, under BGen. Patrice Sabourin.

Canada-US Cyber Cooperation

Canada and the US cooperate on cyber-related defence issues, but this cooperation does not fall explicitly within the purview of continental defence or occur through NORAD. There are several informal and formal avenues for current US-Canada cyber cooperation: first, through the Five Eyes (FVEY) (Australia, Canada, New Zealand, the US, and the United Kingdom) cooperation; second, through the Canadian-US focus on CI protection, and information and resource sharing. For example, this is seen through the Cybersecurity Action Plan between Public Safety (PS) and the US Department of Homeland Security. These avenues of cyber cooperation come with both opportunities and challenges for Canada. The JICC-NORAD could provide a more formalized and structured contribution for Canada-US cooperation on continental cyber defence, and help Canada achieve its cyber defence goals.

Canadian Cyber Goals

According to *Strong, Secure, Engaged* (SSE), DND/CAF's vision for their role in cyber is to "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." DND/CAF also seeks to invest in joint capabilities that include "cyber security and situational awareness projects, cyber threat identification and response, and the development of military-specific information operations and offensive cyber operations capabilities able to target, exploit, influence, and attack in support of military operations."

Canada aims to enhance cyber engagement in national defence and continental defence activities. DND/CAF participates in continental defence through NORAD, but this participation must appreciate the full breadth of the threat spectrum, beyond the aerospace and maritime domain-related threats.

Threat Environment

Cyber threats to continental defence present a rising challenge that must be addressed to the same extent as current and emerging aerospace and maritime threats. Offensive cyber capabilities are fielded by both traditional state and non-state adversaries, through conventional and persistent asymmetric vectors, and are flexible enough to affect targets inside and outside a conventional spectrum.

Due to their range and ability to significantly affect CI and key C4I (Command, Control, Communications, Computers, Intelligence) nodes, we assess that offensive cyber capabilities have the possibility of becoming a strategic threat to North American continental defence. When compared to ballistic or hypersonic weapons, offensive cyber capabilities offer key advantages that increase their likelihood to be used against North

American targets. These "cyber weapons" (and their supporting infrastructure) have low engineering and maintenance costs compared to conventional strategic weapons, while having relatively unlimited range and large-scale disruptive capabilities. Cyber effects do not automatically result in loss of life or physical damage, can possibly be reversed by the originator, and are sometimes difficult to attribute. These aspects make offensive cyber capabilities ideal for conflicts below the threshold of war, and are the current and foreseeable trend when it comes to conflict between major cyber actors.

Adversarial actors have means, intent, and opportunity to threaten North America. Some have integrated cyber options into their conventional military doctrine and offensive capabilities. China, for example, "considers cyber capabilities a critical component in its overall integrated strategic deterrence posture, alongside space and nuclear deterrence," and seeks to use cyber capabilities to target command and control (C2) nodes, logistic networks, and CI, in order to constrain an adversary. Similarly, Russia has integrated cyber capabilities within its "hybrid warfare" concept and has demonstrated their use during conflicts in Georgia and Ukraine.

Persistent asymmetric threats delivered through cyber means are another major challenge for North American continental defence. Adversarial state actors are using cyber capabilities in operations below the threshold of war: such capabilities were used in the Information Operations (IO) sphere, influencing democratic processes and political and economic decisions. The same is being observed with cyber espionage, stealing technical expertise, data, intellectual property (IP), and sensitive technologies from other countries. Moreover, CSE's National Cyber Threat Assessment 2020 indicates that the convergence of Operational Technologies (OT) and Information Technologies (IT) puts CI at a higher risk of cyber disruption by a third party. The current pandemic has laid open these vulnerabilities of our CI and economy to cyber disruption, ransomware, cybercrime, and cyber espionage. Both the Canadian and US governments have stepped up their efforts to counter state and non-state actors' cyber attacks against the COVID-19 vaccine's distribution and logistic networks.

This evolution of the conventional and asymmetric threat landscape echoes Gen (ret.) Terrence O'Shaughnessy and BGen Peter Fesler's (the current NORAD Deputy Director of Operations) concerns in *Hardening the SHIELD*; as much as new hypersonic capabilities represent a rising threat, the surge of conventional and asymmetric cyber offensive capabilities also challenges North American continental defence and requires NORAD to modernize in order to maintain its relevance and early warning capabilities.

Visions of Modernization

Canada's current vision of NORAD modernization focuses on addressing emerging threats, with a heavy emphasis on renewing the North Warning System (NWS). As per SSE,

> "...we intend to engage the United States to look broadly at emerging threats and perils to North America, across all domains, as part of NORAD modernization...Canada will work with the United States to modernize the Command to meet these and other challenges to continental defence...Canada and the United States will jointly examine options to renew the North Warning

> System and modernize the Command, which is integral to fulfilling the NORAD mandate of aerospace warning and control, as well as maritime warning."

Within this context, the purpose of modernization is crafted as a way to address emerging threats to continental defence; however, new technologies and shifting domestic defence priorities will impact these modernization priorities in the future, and thus the vision of NORAD modernization remains contested.

As argued elsewhere, this understanding of NORAD modernization could be expanded to include cyber operational capacity and cyber-specific joint operations, to reflect the dynamic, interconnected, and constantly evolving threat environment. In this paper, we argue that the concept of NORAD modernization could be expanded to include organizational and knowledge-based updates. Although initiatives such as Pathfinder are helpful steps in the management of sensor data, NORAD modernization should include increasing capabilities to deter, detect, and defeat threats to continental defence. These threats include CO by key adversaries, and NORAD does not currently address cyber threats directly.

As we have shown in the previous section, cyber threats are present in this landscape. In order to address these threats, modernization could take shape as a joint component. We propose that NORAD should consider the JICC to address threats within domains outside of its current mission mandate and combine the domestic defensive cyber strengths of both countries.

Exploring the Idea of a NORAD Joint Interagency Cyber Component

Simply put, continental defence includes cyber defence, and continental cyber defence is a joint affair. The JICC-NORAD could focus on cyber defence through DCO and support to civilian authorities, as well as the contributions of Canadian and US military personnel.

The key functions of the JICC-NORAD could be to:

1. Provide early warning of cyber threats against North America;
2. Conduct DCO in support of NORAD operations; and
3. Act as a hub for agencies, departments, and the private sector to deconflict and coordinate continental cyber defence.

Why It Is Important

As a bi-national cyber organization, the JICC-NORAD could ensure that Canada has a voice in the operational planning and prioritization of continental cyber defence, especially when North American CI (i.e. telecommunications, logistical networks, power grids) are vulnerable to cyber disruption as they become increasingly integrated. Canada's contribution and leadership in continental cyber defence could demonstrate our reliability as a partner and our foresight of strategic threats, as well as help Canada to move past the strategy of "defence against help."

Centralizing cyber resources and stakeholders at the JICC-NORAD could provide a much-needed contribution to the modernization of cross-domain capabilities, or JADC2 (Joint All-Domain Command and Control). Data collected through cyber means during DCO and cyber early-warning operations could provide key intelligence, especially when put in context with collection from other platforms. This increased volume of collected data could also encourage NORAD to streamline the adoption of processing systems using quantum computing and Artificial Intelligence (AI). As stated by Charron and Fergusson:

> The more domains surveilled under the NORAD commander, the more information the commander has, in theory, to take decisions presumably farther out in time and space. In other words, an expanded range of missions sets allow NORAD to see and react farther away on the threat to 'bang' continuum.

Keeping in mind that cyber capabilities can be used both standalone or in conjunction with other weapon systems, or capabilities of coercion, a component with dedicated attention to the cyber domain would provide NORAD's commander with extended situational awareness. Others (see Babb) have argued for the idea of expanding opportunities for increased cyber collaboration within NORAD and extended engagement with the private sector. However, further integration of cyber means at NORAD is currently limited.

More generally, the JICC-NORAD could provide the opportunity for Canada to reassert its participation in North American continental defence, while managing resources and the political risks usually associated with an increased military contribution. Canada's investment in DCO expertise and infrastructure for the benefit of North American defence presents a pertinent and practical alternative to other continental defence weapon systems, especially when Canada "has traditionally eschewed pre-emption mainly because of political and resource constraints, as well as the much smaller size and reach of its military."

In addition, a Canadian investment in NORAD cyber defence capabilities is generally a politically safe opportunity. At home, it could likely manage political sensitivities usually irritated by Canada's possible participation in the US' ballistic missile defence program. At the international level, investment in cyber defence rather than ballistic weaponry could be less likely to impact Canada's advocacy for disarmament, especially with Russia, China, or Iran.

How It Could Work

By relying on interagency assets, the JICC-NORAD could aim to integrate civilian agencies such as the National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), CSE, and Cyber Centre, in addition to DND/CAF and the US Department of Defense (US DoD). The JICC-NORAD concept is a *component* (as opposed to a Command) because it could work as a subunit under NORAD/USNORTHCOM, and could be composed of members from various Canadian and US cyber organizations. In addition, this organization could become a bridge with private and academic interests, fostering the necessary relationships to drive innovation and unity of effort.

Although both Canada and the US address national cyber threats, when viewed through the lens of continental defence, more collaboration is needed. Threats to continental defence are a collaborative effort and are handled by NORAD. Thus, following this reasoning, cyber threats to continental defence should be handled by a subcomponent at NORAD. This structure would allow Canada to contribute expertise, break down silos in defence planning, and increase participation in the defence cooperation.

Investment in and development of the cyber domain are priorities and requirements for national defence. Leveraging the existing relationships with an ally on which we are already highly dependent leads to a cost-effective solution to further developing our cyber defence capabilities. Due to its primarily military nexus, the JICC-NORAD could pave the way for the CAF to mature faster in the domain of cyber operations that is mostly controlled, in Canada, by CSE.

Final Thoughts: Why Establishing the JICC-NORAD is Important, and Next Steps

Canada's current contributions to NORAD and vision of modernization need to be expanded to truly address emerging threats to continental defence; however, this revisioning does not need to come with a heavy price tag or unnecessary constraints or redundancy. Although the threats are present, the cyber expertise and knowledge base exists in both states to address these challenges.

It is important for Canada to continue to engage with the US on collective defence-related matters, and collaboration through NORAD is a key part in achieving this goal. Albeit, Canada and the US cooperate on defence and cyber-related issues elsewhere, yet the JICC-NORAD offers a novel approach to increase flexibility and capacity. The JICC-NORAD aims to bring this collaboration to the next level of continental defence. It may also open up future opportunities for collaboration with other partners, including trusted private sector actors and other stakeholders, as well as further promote information sharing and best practises between allies. Additionally, the structure of the JICC-NORAD will ensure that Canada has the opportunity to pursue its interests and contribute equally through the component format. This is because it is not an attachment unit or guided by the directives of a foreign chain of command (CoC).

We have laid out an actionable plan for the JICC-NORAD concept, including its importance and justification. Articulating a cyber strategy for continental defence is an additional step in the revisioning process for NORAD. Another important step is revisiting the NORAD Agreement and introducing a cyber mandate within. The JICC-NORAD is a long-term goal with multiple phases of planning involved. Canada could lead the way in the process of de-siloing domains and integrating a cyber perspective within NORAD's mission to deter, detect, and defeat threats to continental defence.

Notes

[1] The author wishes to thank Ehren Edwards for his dedication to fostering the connections between academic expertise and government. The authors would like to thank Dr. Shannon Nash for providing the opportunity to write this paper and Dr. Andrea Charron for her insightful comments on earlier versions of this piece.

[2] The views expressed in this document are his alone and do not represent the Department of National Defence or the Canadian Armed Forces.

[3] In December 2020, Canadian CF-18 Hornet pilots were tasked with tracking and escorting Santa on the Canadian portion of his global Christmas mission through the annual NORAD Tracks Santa program.