National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

NORAD IS MISSING A PART OF THE WATCH

Major Anil Sheehan

JCSP 44

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 44

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 44 – PCEMI 44
2017 – 2019

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

NORAD IS MISSING A PART OF THE WATCH

Major Anil Sheehan

“This paper was written by a candidate attending the Canadian Forces College in fulfilment of one of the requirements of the Course of Studies. The paper is a scholastic document, and thus contains facts and opinions, which the author alone considered appropriate and correct for the subject. It does not necessarily reflect the policy or the opinion of any agency, including the Government of Canada and the Canadian Department of National Defence. This paper may not be released, quoted or copied, except with the express permission of the Canadian Department of National Defence.”

« La présente étude a été rédigée par un stagiaire du Collège des Forces canadiennes pour satisfaire à l'une des exigences du cours. L'étude est un document qui se rapporte au cours et contient donc des faits et des opinions que seul l'auteur considère appropriés et convenables au sujet. Elle ne reflète pas nécessairement la politique ou l'opinion d'un organisme quelconque, y compris le gouvernement du Canada et le ministère de la Défense nationale du Canada. Il est défendu de diffuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense nationale. »

NORAD IS MISSING A PART OF THE WATCH

INTRODUCTION

For over 60 years, NORAD has been providing aerospace warning and control to protect against and in response to air threats. Prior to the events of 11 September 2001, NORAD was primarily focused on the strategic Cold War threat, notably of Russia launching cruise missiles via their long-range bombers. Post 9/11, NORAD's mission inevitably progressed to also defend against domestic air threats. In 2006, NORAD added maritime warning as its latest mission to round out the binational defence of North America with respect to air and maritime threats.[1]

Since 2006, threats to North America have continued to evolve, leading to the formation of gaps in the combined defence of North America. The most pressing of emerging vulnerabilities are found within the cyber domain, where shared critical infrastructure and NORAD systems are exposed to cyber attacks.[2] These shortfalls might best be addressed by taking advantage of the 60 years of cooperation between Canada and the United States.

While many who work in the cyber domain feel that cyber warning is a function of national military and intelligence personnel, this paper asserts that the unique binational relationship shared by Canada and the U.S. within NORAD would greatly benefit from the addition of a cyber warning mission. Firstly, the paper will address current gaps in cyber warning from a defence of North America perspective. Secondly, it will substantiate why NORAD should play a key role in coordinating cyber warning for

[1] North American Aerospace Defense Command, "NORAD History," last accessed 20 May 2019. https://www.norad.mil/About-NORAD/NORAD-History/

[2] Andrea Charron and James Fergusson, "From NORAD to NOR[A]D: The Future Evolution of North American Defence Co-operation," *Canadian Global Affairs Institute Policy Paper* (May 2018): 12.

Canadian and U.S. Armed Forces as well as whole of government partners. Finally, the paper will describe how the potential addition of a cyber warning mission would keep NORAD relevant in countering emerging threats to North America.

GAPS IN CYBER WARNING (THE EMERGING THREAT)

NORAD has a long history of "having the watch" by providing both U.S. and Canadian leadership with warnings of physical threats to North American. Moreover, NORAD has taken pride in its ability to evolve in order to meet emerging threats, whether that is in response to adversary weapon advances or changes in tactics.[3] Unlike any military relationship the world has ever seen, the 1958 NORAD Agreement created a binational organization that placed peacetime military personnel from two countries under a single command. At the time of its creation, many benefits ensued from sharing the responsibility to watch, warn and, under certain circumstances, to respond to air domain threats to North America. After facing limitations of a bilateral cooperation construct in the 10 years preceding the agreement, NORAD was perceived as a solution to promote unity of effort and command between two great nations.[4]

Working together in a binational construct, NORAD seamlessly performed cross-border operations in order to monitor the vast amount of geography and to share the cost burden of the expensive world of aerospace defence.[5] During its first 40 years, NORAD was primarily concerned with the threat of the former Soviet Union encroaching on North

[3] North American Aerospace Defense Command, "NORAD History," last accessed 20 May 2019. https://www.norad.mil/About-NORAD/NORAD-History/

[4] *Ibid*.

[5] Andrea Charron and James Fergusson, NORAD in Perpetuity? Challenges and Opportunities for Canada, *Centre for Defence and Security Studies, University of Manitoba*, 31 March 2014, 6.

American sovereignty via the north. The integrated air defence capabilities of two nations provided a combined show of strength in deterring Soviet aggression.[6]

The effectiveness and strength of the binational relationship remained unaltered until adversary circumstances forced it to be amended. After 9/11, a massive gap in NORAD's ability to provide its primary missions of aerospace warning and control surfaced. NORAD had to evolve, and did so by coordinating with the Federal Aviation Authority (FAA) and NAV CANADA.[7] This collaboration was vital in obtaining the civilian air picture required to deal with the new asymmetric internal threats to North America, thus helping to prevent the occurrence of any future 9/11 type attacks. The significance of NORAD's partnership with other agencies in the provision of North American defence forecasted the developing requirement for partnering outside of the traditional NORAD military-to-military cooperation. For example, by adding maritime warning as an official mission in 2006, NORAD took a logical step toward creating the same cooperation and unity of effort in defending maritime approaches and waterways as it did in defending air approaches.

Today, North America is subject to non-traditional threats that require a defensive posture that extends beyond physical approaches. The most active threat comes in the form of cyber attacks, which pose a serious risk to networks and critical infrastructure within the U.S. and Canada.[8] Although each nation's military is striving to defend its own networks and to build a holistic approach to cyber event response in conjunction with

[6] Alex Herd, The Canadian Encyclopedia, s.v. "Canada and the Cold War", last modified March 22, 2019, https://www.thecanadianencyclopedia.ca/en/article/cold-war

[7] Andrea Charron and James Fergusson, "From NORAD to NOR[A]D: The Future Evolution of North American Defence Co-operation," *Canadian Global Affairs Institute Policy Paper* (May 2018): 1.

[8] The Canadian Association of Defence and Security Industries "*From Bullets to Bytes, Industry's Role in Preparing Canada for the Future of Cyber Defence*," 2019 Annual Report, 7.

public and private sector support, the critical infrastructure that extends across the border is not well understood or defended. For example, there is neither a combined cyber defence policy nor any kind of combined consequence management plan for the electrical grid, a shared resource. In other words, there is no sole organization that is providing consolidated cyber warning to our respective national authorities from a defence of North America perspective.

Cyber threats have changed the landscape significantly with countries such as Russia, China, North Korea, and Iran actively targeting mission systems and taking advantage of vulnerabilities in our critical infrastructure.[9] The current bilateral relationship between our operation commands, CJOC and USNORTHCOM, falls short in coming together to address many of these emerging cyber threats to North America. The 2018 Department of Defense Cyber Strategy stated that the department must react to these activities by "exposing, disrupting, and degrading cyber activity threatening U.S. interests, strengthening the cybersecurity and resilience of key potential targets, and working closely with other departments and agencies, as well as with our allies and partners."[10] Furthermore, the Canadian Defence Policy calls for the Department of National Defence to be "secure in North America, active in a renewed defence partnership in NORAD and with the United States." [11]

Cyber threats transcend borders and appeal to leadership for the creation of more cross-border cooperation in the defence of our networks and critical infrastructure. Just as the binational relationship provides benefit in the air and maritime domains, the extension

[9] President of the United States, "The National Cyber Strategy of the United States of America," September 2018, 3.

[10] Department of Defense, "*Summary of DoD Cyber Strategy*," 2018, 2.

[11] Department of National Defence,"*Canadian Defence Policy, Strong Secure and Engaged*," 2017, 14.

of the binational relationship within NORAD to include cyber warning would fill a major seam in combined defence.

Cyber warning for NORAD is not a new idea; in 2015, both Admiral Gortney and Admiral Rodgers, Commanders of NORAD & USNORTHCOM and of USCYBERCOM, discussed the potential for additional binational cooperation within the cyber domain. They agreed there would be benefit in forming a binational approach but found that both sides needed to mature with respect to their own national cyber response.[12] Since such time, each nation has taken strides in improving cyber awareness and response, and this paper asserts that we are now in a position to reinvigorate the discussion and to modify the NORAD Agreement to include a cyber warning mission.

In 2016, Randall DeGering, wrote an article on NORAD's role in military cyber attack warning and recommended that NORAD play a much larger role on this stage.[13] DeGering proposed three courses of action that, at the time, should have been investigated in order to expand NORAD's role in cyber warning. Unfortunately, there was little appetite to conduct any staff work to implement his recommendations. Also in 2016, the Permanent Joint Board on Defence directed NORAD to study, within the tri-command construct of NORAD, USNORTHCOM and CJOC, the multidomain threat problem set. This multidomain study is now known as the Evolution of North American Defence (EvoNAD) white paper, a classified domain by domain study on gaps within North American defence. The EvoNAD team quickly realized that the status quo in cyber would see adversaries outpace North American defence, and recommendations to

[12] Defence Security Technology, "Do we need a Cyber NORAD," Vanguard, 29 April 2015, last accessed 20 May 2019. https://vanguardcanada.com/2015/04/29/do-we-need-cyber-norad/

[13] Randall DeGering,"What is NORAD's Role in Military Cyber Attack Warning?." *Homeland Security Affairs* 12, Essay 5 (May 2016). https://www.hsaj.org/articles/10648

evolve are vital.[14] Moreover, Ferguson and Charron's 2018 study on the changes to North American defence indicated much support for binational cyber warning. They stated that, "similar to the other environmental domains, the cyber-threat to North America cannot be managed effectively and efficiently nationally, and the need for enhanced bilateral co-operation itself begs an ultimate bi-national solution."[15]

Furthermore, in 2016, the NORAD Terms of Reference (TOR) were updated to include the requirement to conduct defensive cyber operations on NORAD networks in both the U.S. and Canada. For the first time, the TOR recognized the importance of protecting NORAD's mission systems via the written commitment of action from both nations.[16] The updated TOR paved the way to create binational Defensive Cyber Operations (DCO) policy in the form of a binational DCO Memorandum of Understanding (MOU) and a binational DCO Concept of Operations (CONOPS), thus allowing for cross-border cyber operations.

The binational cooperation in cyber is beginning to take shape; however, it is noted that the efforts made to date pale in comparison to the resources or the recognition that would come from a full commitment to add cyber warning as an official NORAD mission. The creation of the MOU and CONOPS is a piecemeal approach that only scratches the surface in addressing an active threat that puts our nations' military, economic, and political institutions at risk.

WHY CYBER WARNING FOR NORAD

[14] North American Aerospace Defense Command, "The Need to Evolve North American Defense," EvoNAD Point Paper 2017, 2.

[15] Andrea Charron and James Fergusson, "From NORAD to NOR[A]D: The Future Evolution of North American Defence Co-operation," *Canadian Global Affairs Institute Policy Paper* (May 2018): 12.

[16] North American Aerospace Defense Command, "*Terms of Reference*," 28 April 2016, 9.

The need for increased cooperation coincides with the fact that the cyber domain is the most active warfighting domain. The amount of activity in the cyber domain is outnumbering all other threats as malicious cyber actors are challenging Canadian and U.S. interests to gain military, political, and economic advantage. [17] When unchecked, adversaries are waging campaigns without even needing to physically cross our borders.[18]

As noted, extensive coordination with partner organizations already exists in air and maritime domains; thus, these well-established warning processes in other domains can be mirrored to facilitate how timely cyber event information can be relayed to Canadian and U.S. militaries and governments. Given that it is linked to the public sector, it is logical that cyber warning be included in NORAD. Just as the FAA and NAV CANADA data was added after 9/11, cyber event data from military, private, and public entities could be provided to NORAD in order to conduct an assessment on the overall threat. Providing a focal point for cyber events and issues that affect both countries would allow for a unity of effort and a timely response to the threat.

NORAD has been successful in bringing together public and private entities in order to perform response operations. Take Operations Noble Eagle (ONE) for example: ONE is the coordinated response to rogue or adversary aircraft with the help of private and public entities. The processes for conducting ONE are akin to what is required for cyber warning, albeit there is normally more time afforded to cyber event characterization than to rogue or adversary aircraft. Given the similarities in potential processes, cyber warning would likely carry the same efficiencies in collaboration.

[17] Department of Defense, "*Summary of DoD Cyber Strategy," 2018, 2.*

[18] President of the United States, "The National Cyber Strategy of the United States of America," September 2018, 11.

Cyber warning at NORAD would be advantageous to both Canada and the U.S. through the institutionalization of the cyber cooperation processes, in turn allowing for the integration of cyber situational awareness for all stakeholders. In the past, national cyber warning and response missions have taken priority, which can cause the benefits that stem from binational cyber warning to be overlooked. However, the disparate event monitoring from entities like USCYBERCOM, NSA, DHS, ADM(IM), CSE, and Public Safety Canada could be integrated at NORAD to allow for national or potentially binational cyber forces to respond. In order to achieve this reality, resource commitments in personnel and technology would have to be made. As it stands, national caveats make combined cyber warning difficult as the preference for cooperation in cyber tends to be conducted bilaterally. For the sake of unity of effort in cyber warning, many of the information sharing barriers would have to be broken. Due to our geography and interdependence of mission systems and infrastructure, a risk in one country usually extends to the other. Vulnerability sharing and mitigation actions taken in one nation should be communicated freely as to protect the other nation from the same weaknesses.

The power of binational cooperation in protecting the physical geography of Canada and the U.S. has made NORAD a viable and effective defensive command that can assess threats to North America and warn the highest level of government leadership. These assessments inform the national or binational response which often encompasses private and public mission partners from both countries in the conduct of cross-border operations. The benefits of the NORAD relationship were expressed eloquently in a Canadian Global Affairs Institute policy paper on transforming NORAD into a multidomain North American defence. The paper stated that NORAD "provides a foundation for integrating the private-public-military domains, a catalyst for enhanced Canada-U.S. co-operation, and a valuable North American perspective, rather than a national, bilateral one".[19] Hence, NORAD is a practical organization in the provision of cyber threat warning to defend North America.

HOW CYBER WARNING WILL HELP KEEP NORAD RELEVANT

NORAD is uniquely postured to provide a holistic North American perspective in dealing with the cyber threats that affect both nations. The binational relationship that has been successful in other domains is missing an opportunity to evolve in order to key in on the most pervasive threats affecting the overall defence of the continent. As physical attacks on the homelands become increasingly less likely due to improved security and technology, our adversaries are focusing their efforts on the cyber domain.[20]

The networks and critical infrastructure that link our collective defence and economies are constantly at risk, yet very little risk management is being conducted within the partnership. The cyber domain should be attributed at least as much of a sense of urgency that is given to the protection against threats in the physical domains. Although the cyber effects that we see are typically below the level of armed conflict, they still are a direct threat to our sovereignty and require characterization and warning. Unprotected systems and critical infrastructure is already at risk, and yet we have not determined how to defend ourselves or to implement a successful cyber deterrence plan.

[19] Andrea Charron and James Fergusson, "From NORAD to NOR[A]D: The Future Evolution of North American Defence Co-operation," *Canadian Global Affairs Institute Policy Paper* (May 2018): 12.

[20] Jack Corrigan, "*Cyber Threats Are Emerging Faster Than DHS Can Identify and Confront Them*," Defense One, 21 March 2019, last accessed 20 May 2019. https://www.defenseone.com/threats/2019/03/cyber-threats-are-emerging-faster-dhs-can-address-them-secretary-says/155719/

If NORAD is given the lead for cyber warning and coordination with Canadian and U.S. entities in response to cyber events, this task would act to strengthen defences and to create the conditions for enhanced deterrence based on the power of partnering against cyber aggression. As previously stated, NORAD once progressed from being single-domain centered to include maritime warning, which enhanced the characterization of threats to North America. Similarly, in light of the proliferation of cyber threats, NORAD needs to once again evolve to accommodate for this new domain. The addition of cyber warning will heighten NORAD's relevancy in the face of adversary action and will create the conditions to provide efficient multidomain warnings.

CONCLUSION

NORAD has been providing North American defence through an enduring and unique binational relationship for over six decades. The events of 9/11 caused NORAD to develop and forced the interaction with the private and public sectors. Once again, it is time to amend the NORAD Agreement in order to counter 21st century threats. Adversary activity in the cyber domain has left a gap in the NORAD mission set which can only be filled by a huge commitment from both nations. In a statement, Prime Minister Trudeau commented about NORAD, saying that the "key to NORAD's success has been its ability to evolve and meet new challenges, and to take advantage of new opportunities. We can trust in its ability to continue to adapt as needed to meet the needs of the future."[21] This statement emphasizes Canada's commitment to maintaining and improving NORAD.

[21] Justin Trudeau, "Statement by the Prime Minister on the 60th anniversary of NORAD," 12 May 2018, last accessed 20 May 2019. https://pm.gc.ca/eng/news/2018/05/12/statement-prime-minister-60th-anniversary-norad

The ideas put forth in this paper suggest that binational cyber cooperation is required as the next step for NORAD in order to meet the latest challenges in the defence of North American. As noted, the largest gap in the defence of our continent is not found in the physical domains, but rather in the cyber domain where freedom within our military, economic, and political institutions are under constant attack. Due to its experience and makeup, NORAD is well postured to fill the gap in assessing the impact of cyber events that affect our nations. Despite its proud history of evolving based on the threat, it is feared that if NORAD does not take strides towards a cyber warning mission, its relevance may be put into question. A cyber warning mission that characterizes threats to North America would significantly assist both countries in defending and deterring emerging threats.

Bibliography

Canada, Department of National Defence, “Canadian Defence Policy, Strong Secure and Engaged,” 2017.

Canada, Prime Minister Justin Trudeau, “Statement by the Prime Minister on the 60th anniversary of NORAD,” 12 May 2018, last accessed 20 May 2019. https://pm.gc.ca/eng/news/2018/05/12/statement-prime-minister-60th-anniversary-norad

Canada, The Canadian Association of Defence and Security Industries “From Bullets to Bytes, Industry’s Role in Preparing Canada for the Future of Cyber Defence,” 2019 Annual Report.

Charron, Andrea and James Fergusson, “From NORAD to NOR[A]D: The Future Evolution of North American Defence Co-operation,” *Canadian Global Affairs Institute Policy Paper* (May 2018).

Charron, Andrea and James Fergusson, NORAD in Perpetuity? Challenges and Opportunities for Canada, Centre for Defence and Security Studies, University of Manitoba, 31 March 2014.

Corrigan, Jack, “Cyber Threats Are Emerging Faster Than DHS Can Identify and Confront Them,” Defense One, 21 March 2019, last accessed 20 May 2019. https://www.defenseone.com/threats/2019/03/cyber-threats-are-emerging-faster-dhs-can-address-them-secretary-says/155719/

Defence Security Technology, “Do we need a Cyber NORAD, Vanguard, 29 April 2015, last accessed 20 May 2019. https://vanguardcanada.com/2015/04/29/do-we-need-cyber-norad/

DeGering, Randall,“What is NORAD’s Role in Military Cyber Attack Warning?.” Homeland Security Affairs 12, Essay 5 (May 2016). https://www.hsaj.org/articles/10648

Herd, Alex, The Canadian Encyclopedia, s.v. "Canada and the Cold War", last modified March 22, 2019, https://www.thecanadianencyclopedia.ca/en/article/cold-war

North American Aerospace Defense Command, “The Need to Evolve North American Defense,” EvoNAD Point Paper 2017.

North American Aerospace Defense Command, “Terms of Reference,” 28 April 2016.

North American Aerospace Defense Command, “NORAD History,” last accessed 20 May 2019. https://www.norad.mil/About-NORAD/NORAD-History/

United States, Department of Defense, “Summary of DoD Cyber Strategy,” 2018

United States, President of the United States, “The National Cyber Strategy of the United States of America,” September 2018.