National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

OPERATIONALIZATION OF CYBER DEFENCE: THE NEXT STEPS

Lieutenant-Colonel James Siebring

JCSP 47

Service Paper

Disclaimer

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

PCEMI 47

Étude militaire

Avertissement

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

Canada

CANADIAN FORCES COLLEGE - COLLÈGE DES FORCES CANADIENNES

JCSP 47 - PCEMI 47
2020 – 2021

SERVICE PAPER – ÉTUDE MILITAIRE

OPERATIONALIZATION OF CYBER DEFENCE: THE NEXT STEPS

By Lieutenant-Colonel James Siebring

Word Count: 2,400

Nombre de mots : 2.400

OPERATIONALIZATION OF CYBER DEFENCE: THE NEXT STEPS

AIM

1. The aim of this service paper is to provide considerations for the prioritization of defensive cyber capabilities. The Department of National Defense (DND) and the Canadian Armed Forces (CAF) have made significant advances in cyber organization, workforce and doctrine over the past seven years. In the next phase of developing an operational capability, the institution must consider prioritization of its limited available resources. The new roles of Defensive Cyber Operations (DCO) have been added to organizations already challenged with IT Security (IT Sec)[1] responsibilities. In this environment, small elements attempt to support a range of tasks exceeding their resources. Without focus, there is significant risk that DND/CAF's defensive resources will be fully engaged, but generate little measurable impact.

INTRODUCTION

2. In 2013, the CDS directed the CAF to develop and operationalize a cyber operations capability. [2] This direction resulted in annual increases in personnel invested into a range of positions from strategic to tactical. As staffs increased, organizational structures emerged, establishing a joint cyber organization within the Associate Deputy Minister for Information Management (ADM(IM)). The ADM(IM) Chief of Staff was double-hatted as the Cyber Force Commander (CFC) and became responsible for the entire range of force development through force management activities. Responsible to the CFC is DG Cyber and Director General Information Management (DGIMO). DGIMO is also the Commander Cyberspace Division (CCD) and the Joint Forces Cyber Component Commander (JFCCC). These senior leaders are responsive to a series of reporting relationships spanning the Chief of Defense Staff, Deputy Minister and the Commander of Canadian Joint Operations Command.[3]

3. Subordinate to DGIMO are two formations: 7 Communications Group, charged with a range of communications support tasks, and the Canadian Forces Information Operations Group (CFIOG), responsible for Signals Intelligence and Cyber Operations. In another illustration of the complexity of cyber force organization, CFIOG reports to both DGIMO and the Canadian Forces Intelligence Command (CFINTCOM).

4. As Cyber Operations structures and concepts continued to develop, the Canadian Forces Network Operations Center, originally created with an IT Sec mandate, became

[1] Language in this service paper is deliberately chosen to inform a broad audience. To that end, some phrasing and terminology may not align with current doctrine or norms within the Canadian Cyber Force. For example, IT Sec has been has been rebranded as Cyber Security. The term IT Sec is used in this paper as it more easily distinguishes concepts of security and defense.

[2] Deparment of National Defence, *Joint Doctrine Note Cyber Operations* (Ottawa: Canadian Forces Joint Warfare Center, 2017), 1-3.

[3] Department of National Defence, *CAF Cyber Operations Overview Brief (*Ottawa: Director General Information Management Operations, 2020), 9.

the focal point for CAF DCO. Already under-resourced for the growing scope of their original mandate, they were charged with the new role of cyber operations. The unit faces significant challenges with the balance of their responsibilities.[4] While some overlap exists, IT Sec and DCO represent vastly different approaches and are enabled by different cultures, tactics, specialties and authorities.[5]

DISCUSSION

5. Defensive cyber capabilities are high demand, low density assets. While cyber operations doctrine has been developed, direction on how it will be applied has not been established within the CAF. The organization has yet to articulate how the range of IT Sec and DCO responsibilities will be separated across the organization and where the priorities will rest.[6] In the ongoing operationalization of the CAF cyber program, the next phase must consider how the limited available resources will be focused.

6. IT Sec is a broad and more general discipline when compared to DCO. It is threat agnostic, leveraging best practices and established standards to assure a network through a focus on policy compliance. [7] For an IT Sec practitioner, the overarching priority is the maintenance of the best possible security posture for a network environment. DCO by comparison, is mission and adversary focused. The purpose is to generate effects in or through cyberspace.[8] DCO activities are focused actions that occur across a range of environments including networks, weapons platforms and industrial control systems.[9] DCO can be employed to enable conventional operations, to generate independent effects, or contribute to a full-spectrum cyber operation.

7. The broad emphasis and network focus of IT Sec can be easily exploited by a sophisticated adversary. However, IT Sec provides a foundation for DCO.[10] Without a strong security posture, an environment is not defensible. DND/CAF requires both IT Sec and DCO capabilities, and thus the challenge is not which should be selected, but how should the priorities be balanced, and what is the optimal organizational structure for these separate disciplines.

Defensive Cyber Operations

8. Internal to DCO, there are a range of potential options for how capabilities may be focused. These options most often fall into one of two categories: Operations or Intelligence:

[4] Travis Jardine, Report on CFNOC Growth 2014-2019 (Canadian Forces Network Operations Center: Briefing Note, 7 Jan 2020), 3.

[5] An example of the differences between IT Sec and DCO is witnessed in how compromises are managed. IT Sec practitioners tend to immediately remediate a compromise to avoid risks to service provisioning. A DCO practitioner is more likely to observe adversary activity to gain information and enable follow-on activities, potentially including offensive cyber operations.

[6] Discussion of separation of responsibilities between specific units is outside the scope of this paper.

[7] Joint Doctrine Note Cyber Operations, 1-2,1-3.

[8] *Ibid*, 4-3.

[9] *Ibid*, 1-2,,1-3.

[10] *Joint Doctrine Note Cyber Operations*, 1-2,1-3,1-4.

a. Operational Focus. An operational focus starts with CAF named operations and places the Canadian Joint Operations Command (CJOC) as the focus for support. The approach requires a detailed understanding of individual operations. Planners must understand the missions, their critical tasks and how they are enabled by the range of weapons platforms, communications systems and networks.[11] Combining this analysis with insights into adversary intent and capability, an understanding of how an adversary could target an operation is developed. This planning enables the generation of the right specialist capabilities, positioned in the right locations with the right authorities.[12] An operational focus requires significant planning and intelligence capability coupled with specialist technical skills.

b. Intelligence Focus. An intelligence focus is centered on the adversary. Its organizing principle is to operate where the adversary is, or is most likely to be. Planners leverage intelligence to determine intent and capability and activities are focused to act pre-emptively, posturing capabilities when and where required to deny the adversary their objectives. Where there are intelligence gaps, deliberate DCO missions can be developed to collect information on adversary activity,[13] informing follow-on efforts including offensive cyber operations.[14] This approach would inevitably overlap with an operational focus, but cyber defence capabilities are prioritized based on a broader analysis spanning the entirety of DND/CAF Cyberspace.

9. Despite operations being the foundational purpose of the CAF, not all are created equal. Many are likely to be conducted in a benign cyberspace environment, thus the commitment of limited density assets would be ill advised. Operations that approach the higher end of the spectrum of conflict are those that will be increasingly be challenged in cyberspace. In this environment, adversaries are more likely to expend advanced capabilities targeting mission systems and platforms. This contested cyber environment would witness a barrage of simultaneous assaults across the entirety of a mission's cyber enabled systems. Effects will specifically target platform systems such as those that degraded the functioning of U.S. Stryker armoured vehicles, or spoofed maritime GPS locations.[15]

10. In the current environment of global competition below the threshold of war, adversaries are more likely to conduct shaping and intelligence activities rather than overt

[11] Canadian Forces Network Operations Center, *Functional Mission Analysis Cyber Guide* (Ottawa: Canadian Forces Information Operations Group, 2019), 5.

[12] Examples of mission platforms range widely. Examples include: armored vehicles, ships, aircraft and command support systems like the RCAF's Battle Control System-Fixed (BCSF).

[13] Often the best information on an adversary can be established by observing activity at the perimeter of, or within one's own systems and networks.

[14] Currently DND/CAF uses the term Active Cyber Operations (ACO) to describe offensive operations.

[15] The War Zone, "The U.S. Army's New Up-Gunned Stryker Armored Vehicles Have Been Hacked," accessed 16 February 2021, https://www.thedrive.com/the-war-zone/26458/the-u-s-armys-new-up-gunned-stryker-armored-vehicles-have-been-hacked; Canadian Naval Review, "Cyber defence – How vulnerable is the Canadian Navy?" last accessed 20 January 2021, https://www.navalreview.ca/2020/12/cyber-defence-how-vulnerable-is-the-canadian-navy/.

attacks on CAF operation. These activities make a wider range of DND/CAF organizations potential targets. Gaining insights into personnel, procurement efforts or research is likely to be of greater interest in the current environment. The compromises of Defense Research and Development Canada (DRDC) and the Royal Military College lend credence to this theory.[16] A challenge in the intelligence focus is the sheer scope of DND/CAF Cyberspace. Accurate intelligence is essential.

11. An operational focus risks committing capabilities to prepare for an adversary that may never manifest, and an intelligence focus may chase an invisible foe. Once again the challenge in the prioritization of DND/CAF defensive cyber capabilities is achieving the right balance of the approaches. As DND/CAF weighs the balance of priorities a range of options, organization must be considered.

Organization

12. The location of a capability within a broader organization has significant impact. The culture, policies, processes and mandate of a parent organization impact priorities and resourcing. This challenge of organization of defensive capabilities is not unique to the Canadian Armed Forces. Businesses have been grappling with this challenge of managing risk to their networks and systems for years.

13. Given the importance of technology to business function, the Chief Information Officer (CIO), equivalent to ADM(IM) within DND/CAF, has grown to be a key element of any large corporation. Commonly reporting directly to the CEO, they are vital to the integration and operation of Information Technology (IT) resources.[17] Initially, they were also responsible for the security of these services. As threats and risks increased, and companies encountered multi-million dollar losses, the environment shifted.[18] A new position has emerged to assist companies to operate in this environment of increased risk: the Chief Information Security Officer (CISO).

14. The CISO's responsibilities for security, and the CIO's role to integrate and operate IT services are naturally in competition. Given the requirement to balance these perspectives, how an organization structures these roles is indicative of their priorities. In industry, the scale is tipping toward security. Increasingly, the CISO does not report to the CIO. More commonly the CISO reports through operational channels or directly to the CEO. [19] In industry the decisions weighing the service provision versus security risks

[16] Colin Freeze, "What a cyber attack looks like – from the target's point of view," Globe and Mail, 26 May 2014, https://www.theglobeandmail.com/news/politics/globe-politics-insider/what-a-cyber-attack-looks-like-from-inside-the-government/article18853435/; Alexandra Mazur and Jennifer Basa, "Student information, financial info published in suspected RMC data leak after cyber attack," Global News, 20 Aug 2020, https://globalnews.ca/news/7283754/student-financial-rmc-data-leak-cyber-attack/.

[17] Erastus Karanja and Mark A. Rosso, "The Chief Information Security Officer: An Exploratory Study," Journal of International Technology and Information Management 26, no. 2 (2017), 32.

[18] Karanja and Rosso, 25.

[19] Karanja and Rosso, 28-29.

is increasingly occurring outside the office of the CIO. Their security and defensive capabilities are increasingly distinct from IT service provision.

15. This trend is not unique to industry. The US military demonstrated a similar evolution. Commencing in 1998, The US established Joint Task Force-Computer Network Defense. This organization was created within the Defense Information Services Agency, an organization similar to that of a CIO or in DND/CAF structure, ADM(IM). Between 1998 to 2017 the organization iteratively expanded, ultimately becoming a functional Combatant Command. US Cyber Command started as an IT Sec task force and as they evolved, their security roles were divested and they became an independent organization with a mandate to conduct full spectrum cyber operations. [20]

CONCLUSION

16. DND/CAF requires defensive cyber capabilities that are broad and concentrated, specialized and generalized and both adversary and operationally focused. The institution must ensure a baseline of security for enterprise networks, while being prepared to enable CAF operations in a contested cyber environment. Demands are vast and resources are limited. Focus and prioritization is required to optimize a limited capability and ensure that training and capability investments generate a relevant capability.

17. This paper has provided considerations to broaden and advance ongoing discussion, however; it could not address the enormity of the challenge. It did not discuss the development of offensive capabilities, support to SOF or environmental mission assurance programs. These programs also drawing from the same limited resource pool. It did not discuss the impacts of Shared Service Canada, the Canadian Center for Cyber Security, the Communications Security Establishment. Finally, it did not address the host of authorities and policy challenges.

18. The CAF Cyber Force has made significant strides since 2013, but in order to truly operationalize cyberspace capabilities, the next phase of development must centre on the development of clear priorities for tactical elements. In an environment where demand exceeds resources, there is no right answer and only one wrong one: attempting to do it all.

RECOMMENDATION

19. Similar to any military endeavour, the right answer in prioritizing cyber defence capabilities is the hybrid course of action. The challenge lies in determining its composition. If the CAF approach of force generating for the most challenging mission is applied, then an operations focused DCO approach should be the priority. This approach requires the application of the most complex combination of authorities, planning, technical skill and intelligence. This prioritization will posture the CAF for operations in

[20] U.S. Cyber Command,"US Cyber Command History," accessed 8 February 2020, https://www.cybercom.mil/About/History/.

complex future operating environments, at the cost of a less than optimal posture for the current broad threat environment. Regardless of the balance of priorities established, their successful realization must consider organization.

20. Grouping cyber defence capabilities within ADM(IM), DND/CAF leveraged a similar approach witnessed within industry and the U.S. Military. As these organizations developed, they increasingly separated their workforces into more distinct structures. As DND/CAF moves forward, it too must determine the best organizational model to enable the intended effects. While grouping within ADM(IM) has significant synergies, its culture and priorities skew towards an enterprise security focus. The movement of CAF Cyber Capabilities to a different L1 such as CFINTCOM should be studied. Cyber capabilities have intelligence value that have yet to be fully realized and closer alignment supporting intelligence capabilities is an operational enabler. In the interim, DND/CAF must consider ADM(IM)'s organizational impact on the generation of the desired cyber defence capability and implement mitigations where required.

BIBLIOGRAPHY

Canada. Canadian Forces Network Operations Center. *Functional Mission Analysis Cyber Guide*. Ottawa: Canadian Forces Information Operations Group, 2019.

Canada. Department of National Defence. *CAF Cyber Operations Overview Brief*. Ottawa: Director General Information Management Operations, 2020.

Canada. Deparment of National Defence. *Joint Doctrine Note Cyber Operations*. Ottawa: Canadian Forces Joint Warfare Center, 2017.

Canadian Naval Review. "Cyber defence – How vulnerable is the Canadian Navy?" Last accessed 20 January 2021. https://www.navalreview.ca/2020/12/cyber-defence-how-vulnerable-is-the-canadian-navy/.

Freeze, Colin. "What a cyber attack looks like – from the target's point of view." Globe and Mail, 26 May 2014. https://www.theglobeandmail.com/news/politics/globe-politics-insider/what-a-cyber-attack-looks-like-from-inside-the-government/article18853435/.

Mazur, Alexandra and Basa, Jennifer. "Student information, financial info published in suspected RMC data leak after cyber attack." Global News, 20 Aug 2020, https://globalnews.ca/news/7283754/student-financial-rmc-data-leak-cyber-attack/.

Jardine, Travis. *Payment of Industry Certifications for Cyber Analysts.* Canadian Forces Network Operations Center: Briefing Note 17 June 2020.

Jardine, Travis. *Report on CFNOC Growth 2014-2019*. Canadian Forces Network Operations Center: Briefing Note, 7 Jan 2020.

Karanja, Erastus, and Mark A. Rosso. "The Chief Information Security Officer: An Exploratory Study." Journal of International Technology and Information Management 26, no. 2 (2017): 23-43. https://scholarworks.lib.csusb.edu/jitim/vol26/iss2/2/

U.S. Cyber Command."US Cyber Command History." Accessed 8 February 2020. https://www.cybercom.mil/About/History/.

The War Zone. "The U.S. Army's New Up-Gunned Stryker Armored Vehicles Have Been Hacked." Accessed 16 February 2021. https://www.thedrive.com/the-war-zone/26458/the-u-s-armys-new-up-gunned-stryker-armored-vehicles-have-been-hacked.