National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

THE INSTITUTIONAL CYBER GAP WITHIN THE CANADIAN ARMED FORCES

Maj R.F.J. Dias

JCSP 42

Service Paper

PCEMI 42

Étude militaire

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.

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.

© Her Majesty the Queen in Right of Canada, as represented by the Minister of National Defence, 2016.

© Sa Majesté la Reine du Chef du Canada, représentée par le ministre de la Défense nationale, 2016.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 42 – PCEMI 42
2015 – 2016

JCSP SERVICE PAPER – PCEMI ÉTUDE MILITAIRE

THE INSTITUTIONAL CYBER GAP WITHIN THE CANADIAN ARMED FORCES

Maj R.F.J. Dias

"This paper was written by a student 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."

Word Count: 2217

"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."

Compte de mots: 2217

THE INSTITUTIONAL CYBER GAP
WITHIN THE CANADIAN ARMED FORCES

AIM

1. The purpose of this service paper is to further explore the current capability gap within the Canadian Armed Forces (CAF) with regard to its cyberspace capabilities. Although CAF doctrine does not yet identify cyber as its own component, it is being recognized as its own unique domain which operates across all components and therefore applies to all three environmental elements. This paper will also propose a possible method to further enhance Canada's capabilities in the cyber domain through the creation of a cyber-component command. The intent of this paper is not to delve into the details of current cyber threats nor into the tactics, techniques and procedures (TTPs) to handle such threats, but more to focus on the need to institutionalize this emerging capability through a formalized Command Headquarters (HQ) construct.

INTRODUCTION

2. In the establishment and maintenance of an emerging capability such as a Command HQ, key aspects which should be considered are: development of strategic vision, establishment of an authority, whether it's operational or technical, and the resources to implement the vision. To that end, this paper will address these points as they relate to the current CAF cyber capability.

3. In 2010, the Government of Canada through the Public Safety Minister, the Honourable Vic Toews issued a national strategy regarding the future of Canada's Cyber Security posture.[1] This strategy mentions the CAF along with other government partners such as Public Safety Canada, the Royal Canadian Mounted Police (RCMP), the Canadian Security Intelligence

[1] Government of Canada. *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada*. Ottawa, 2010.

Service (CSIS), and the Communications Security Establishment Canada (CSEC) as playing a vital role in securing of our national cyber infrastructure. The national strategy was based on a whole of government (WoG) approach to handle this challenge including partnering with the private sector and critical infrastructure sectors.[2] This strategy would continue to build upon previously established initiatives such as the Canadian Cyber Incident Response Centre (CIRC) charged with monitoring and provision of technical advice and the coordination of a national response to cyber threats.[3]

4. In September of that same year, the CAF created an ad hoc Cyber Task Force (Cyber TF) to identify its cyber requirements and with the mandate to "optimize current cyber-related capabilities while setting the conditions for the force development, force generation and force employment of future cyber capabilities".[4] Since then, some things have moved forward. However, the challenges are compounded by the fact that most of these operating capabilities reside under different branches led by different Assistant Deputy Ministers (ADMs). The CAF seemed to have lost the momentum which had been created by the national cyber strategy. Additionally, the Chief of the Defence Staff (CDS) issued guidance in 2013, which stated "[he would] place particular focus on aggressively developing and integrating those essential joint capabilities [including cyber], to bring integrated effects where needed".[5] The CDS would further specify his intent to have a cyber-force capable of conducting operations in the cyber

[2] Government of Canada. *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada*. Ottawa, 2010, 12.

[3] *Ibid*., 3.

[4] Parliament of Canada. "The Standing Senate Committee on National Security and Defence, Ottawa, 05 November 2012". Last accessed 04 Feb 2016 http://www.parl.gc.ca/content/sen/committee/411%5CSECD/49784-e.HTM

[5] Canadian Armed Forces. *Chief of the Defence Staff Guidance to the Canadian Armed Forces.* Ottawa, 07 June 2013, 12.

domain, just as the CAF conducts operations in the land, sea, air, and space domains.[6] In spite of the CDS guidance, there lacks the cohesive, unifying vision necessary to handle cyber, and despite the best efforts of the small numbered team, the CAF Cyber TF is not capable to have great effect in this matter.

DISCUSSION

5. While the CAF senior leadership recognize the cyber capability gap, they are pressed to define what the cyber environment is and how it will affect our future. Similar to the adoption and development of air power over the last one hundred years, a new domain in warfare is up us in the twenty-first century. In an attempt to find the answers to the cyber questions, the CAF established the Director General Cyberspace (DG Cyber) under the Vice Chief of the Defence Staff (VCDS) with the focus on development of policy, command and control, capability development and human resourcing. Despite the CAF Cyber TF reporting to DG Cyber, it cannot carry out cyber operations of any type because it lacks the personnel and structure to do so, and the command authority over those special units and branches across different ADMs with conflicting priorities. As the task force was created for a specific function, it follows that form and structure must be also created to achieve effectiveness and legitimacy needed for success.

6. In discussing the development of strategic vision, it must be noted that the last strategic guidance was issued in 2010, and in technological terms that is very much outdated. Therefore any strategic vision in relation to cyber will have to be re-evaluated given current and perceived cyber threats and trends. This will indeed create more future challenges as technological advances will outpace the ability for institutions to assess and react. This will require a strategic

[6] *Ibid*., 13.

entity to look beyond Horizon 1 timelines, while another organization develops the TTPs for the close fight.

7. It should also be mentioned, since the cyber domain transcends operating levels (strategic to tactical) and across operational functions (Command, Sense, Act, Shield, Sustain, Generate) and environmental domains (land, sea, air, space), there is a requirement for a holistic, partnered approach to defining the strategic vision.[7] Each Environmental Chief (EC) will undoubtedly want to ensure their organization's security concerns are addressed, and therefore relationship building and strategic messaging will be of great importance. This may be best served by having someone of similar rank or status (i.e.: Lieutenant- General or Commander of an L1 organization) or someone having been delegated authority to speak/act on behalf of someone who does. Having a clear mandate drawn from a comprehensive strategic vision will further the creation of cyber capabilities.

8. The establishment of command authority and clear chains of command is critical if cyber operations are to be effective. The mandate describes Canada's Cyber Security Strategy as a WoG endeavour.[8] With the multiple government partners and agencies involved, along with CAF specialty branches and units, the need to have clear delineation of operational command authority is paramount. The Cyber TF's inability to, plan, coordinate and execute cyber operations has to some degree, been due to not having direct command authority over the tactical elements. Those elements reside across other commands, ADM branches and government departments, creating additional challenges in the synchronization and coordination of effects.

[7] Melanie Bernier, and Joanne Treurniet. "Understanding Cyber Operations in a Canadian Strategic context: More than C4ISR, more than CNO." In *Conference on Cyber Conflict Proceedings*, 2010, 231.

[8] Government of Canada. *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada*. Ottawa, 2010, 9.

The continued compartmentalization of information, resources, and abilities continues to be a hindrance to effectively prosecute cyber activities.

9. A centralized unified command authority over all assets involved in the cyber operations is necessary if it is to be effective. The requirement also exists to ensure enough staff personnel are assigned across the varied staff functions and disciplines to create the synergy necessary to be an effective operational HQ. The staffs who currently work in DG Cyber and Cyber TF should be leveraged to establish the technical and strategic staff nucleus which would be necessary in a new cyber component command.

10. Planning and preparation happens in an operational headquarters, where strategic and political intent is translated into measureable effects. In cyber, those effects may have direct strategic consequences, such as a cyber-attack on an opponent's critical command and control network, or it may be less obtrusive such as cyber exploitation at a tactical level.[9] This necessitates a certain level of authority high enough for decision making and to accept risk in the conduct of sensitive cyber operations.[10]

11. In the realm of having the resources necessary to implement a strategic vision, Canada as a medium power, does not have the resources to invest as much into cyber as some of our allies do. However, lessons may still be learned from our allies as Canada develops its capabilities to meet the country's cyber needs. As Canada attempts to define the problem set, so too are our allies. US Cyber Command (USCYBERCOM) was stood up in 2010 and assumed

[9] Ian Dudgeon, Gary Waters, and Desmond Ball. *Australia and Cyber-warfare*. ANU Press, 2008, 127.

[10] Jeffrey L. Caton, *Army Support of Military Cyberspace Operations: Joint Contexts and Global Escalation Implications*. Army War College Strategic Studies Institute, 2015, 54.

responsibilities of previous network operations commands across their Department of Defense.[11] This also included their Combatant Commands' cyber capabilities falling under USCYBERCOM, thus leveraging technological advancements that had been previously isolated within their own respective elements (Army, Navy, Air Force, Marines).[12] In fact, during the establishment of USCYBERCOM, guidance was sought from the US Special Operations Command (USSOCOM) on how they stood up and absorbed the different elemental SF in a joint operational command environment.[13]

12. The same could be accomplished under a new CAF Cyber Command where the Army Network Operations Centre (ANOC) and the Royal Canadian Air Force Network Operations Centre (AFNOC) would allow for the Canadian Forces Network Operations Centre (CFNOC) to maintain network awareness across the strategic network infrastructure and ability to react to cyber incidents. For this to be effective, authority needs to be granted to the appropriate levels and a desire by all participants to want to participate. There have been times where competing personalities have not cooperated creating a divide amongst the network operations community. Once again, having all the cyber elements under one central unified command with the operational command authority to direct, synchronize and coordinate cyber activities would resolve the cross-element debate.

13. The very nature of this specialized multi-disciplinary field of cyber requires those who engage in it to be well versed in the technical and tactical level as well as understanding the strategic ramifications of their task. This grouping of future "cyber warriors" is very much akin

[11] Jeffrey L. Caton, *Army Support of Military Cyberspace Operations: Joint Contexts and Global Escalation Implications*. Army War College Strategic Studies Institute, 2015, 10.

[12] *Ibid*., 11.

[13] Christopher Paul, Isaac R. Porche III, and Elliot Axelband. *The other quiet professionals: lessons for future cyber forces from the evolution of special forces*. Rand Corporation, 2014.

to many Special Forces (SF) around the world. Just as our own Canadian Special Operations Force Command (CANSOFCOM) has elements which operate across the land, sea, and air domains in highly coordinated fashion, so will future cyber forces as it continues to define the cyber domain and its own battlespace as per the CDS guidance. Parallels can be drawn between how CANSOFCOM or USSOCOM matured as an entity and where CAF Cyber TF is today. For purposes of comparison, this paper will use examples from USSOCOM literature. Despite the scale and scope, CANSOFCOM would have similar observations.[14] Key areas of consideration are in personnel, development of doctrine, organizational structure, developmental strategy, training, sustainment and competence as a capability.[15]

14. On the issue of personnel, it can be argued that both SF and cyber forces are at their core, "small teams of highly skilled specialists" who's communities place great value on the human component above all else.[16] An additional burden on the issue of personnel is the retention of skilled *warriors.* Whether its lack of advancement opportunities due to the special nature of the work, or the skill fade due to the need to rotate back into conventional force units for career progression, the cycle creates a "lack of career continuity".[17]

15. Doctrine often lags behind operational imperatives, as military organizations cope with the ever evolving situation - cyber is no exception.[18] Developing doctrine takes time and often requires ability to review and validate. The time sensitive nature and fluidity of both irregular warfare and cyber warfare at times requires for doctrine to be written after the fact. The creation

[14] As observed by the author throughout briefings from the Commanding Officer of Joint Task Force 2, in Ottawa, Ontario and members of the Canadian Special Operations Regiment, Petawawa, Ontario.

[15] Christopher Paul, Isaac R. Porche III, and Elliot Axelband. *The other quiet professionals: lessons for future cyber forces from the evolution of special forces*. Rand Corporation, 2014, 31.

[16] *Ibid.*

[17] *Ibid.*, 32.

[18] Christopher Paul, Isaac R. Porche III, and Elliot Axelband. *The other quiet professionals: lessons for future cyber forces from the evolution of special forces*. Rand Corporation, 2014, 32.

of an operational command would not resolve this issue but it may be able to temper it with staff dedicated to lessons learned and the development of TTPs for future operations, the nation's centres of excellence (CoE) are developed.

16. Just as doctrine lagged behind operational tempo, so too did the necessary training for the development of the tradecraft. Both SF and cyber forces have been affected by this reality and have been forced to find their own solutions to the training deficiencies, thus risking non-standard practices or the creation of their own schoolhouses, such as the Canadian Special Operations Training Centre which falls under command of CANSOFCOM.[19] With the establishment of a command providing a force development capability, the identification of a training shortfall may be the impetus to create a new CoE for cyber in Canada. A CoE may include participants from not just CAF cyber units, but also those from our WoG partners to include middle and upper management for advanced planning and strategy development.

CONCLUSION

17. Although the DG Cyber and CAF Cyber TF have been mandated to focus on development of policy, force development, force generation and force employment of future cyber capabilities, they have fallen short of their mandate over the last five years. The absence of strategic vision, an established authority, and resources have all contributed to the delay, and the inability to institutionalize this capability. Failure to have a unified command structure to harness all the discrete capabilities that exist across the CAF, has contributed to not achieving the CDS's intent. The different cyber branches and units demonstrate a fractured capability, at times

[19] As observed by the author throughout briefings from the Commanding Officer of Joint Task Force 2, in Ottawa, Ontario.

working at cross purposes, demonstrating the need for a unified approach with unity of purpose and unity of command in line with an authoritative strategic vision.

18. The ultimate goal is to identify a command level organization (L1 organization) which will apply a holistic approach to cyber. It would have under command current existing cyber assets and capacity to develop future capabilities with a view to having an established cyber domain within the CAF capable of conducting the full spectrum of cyber activities. To address many of the noted concerns regarding the current state of cyber in the CAF, senior leadership must continue to be educated on how to apply cyber as another capability in achieving strategic effect. DG Cyber under the VCDS is currently best situated to continue to champion for the requirement of a cyber-component command.

BIBLIOGRAPHY

Bernier, Melanie, and Joanne Treurniet. "Understanding Cyber Operations in a Canadian Forces College Strategic context: More than C4ISR, more than CNO." In *Conference on Cyber Conflict Proceedings*, 2010. pp. 227-243.

Betz, David, and Tim Stevens. *Cyberspace and the State: Toward a Strategy for Cyber-power*. The International Institute for Strategic Studies, 2011.

Canadian Armed Forces. *Chief of the Defence Staff Guidance to the Canadian Armed Forces.* Ottawa, 07 June 2013.

Caton, Jeffrey L. *Army Support of Military Cyberspace Operations: Joint Contexts and Global Escalation Implications*. Army War College Strategic Studies Institute, 2015.

Caulkins, Bruce D. *Proactive self defense in cyberspace*. Army War College Strategic Studies Institute, 2009.

Da Silva, Joseph, Hugh Liebert, and Isaiah Wilson III. *American Grand Strategy and the Future of US Landpower*. Army War College Strategic Studies Institute, 2014.

Dudgeon, Ian, Gary Waters, and Desmond Ball. *Australia and Cyber-warfare*. ANU Press, 2008.

Gray, Colin S. *Making Strategic Sense of Cyber Power: Why The Sky is Not Falling*. Army War College Strategic Studies Institute, 2013.

Gansler, Jacques S. *Democracy's arsenal: Creating a twenty-first-century defense industry*. MIT Press, 2011.

Government of Canada. *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada*. Ottawa, 2010.

Mazanec, Brian M., and Bradley A. Thayer. *Deterring Cyber Warfare: Bolstering Strategic Stability in Cyberspace*. Palgrave Macmillan, 2014.

Parliament of Canada. “The Standing Senate Committee on National Security and Defence, Ottawa, 05 November 2012”. Last accessed 04 Feb 2016. http://www.parl.gc.ca/content/sen/committee/411%5CSECD/49784-e.HTM

Paul, Christopher, Isaac R. Porche III, and Elliot Axelband. *The other quiet professionals: lessons for future cyber forces from the evolution of special forces*. Rand Corporation, 2014.