National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

PAN-DOMAIN OPERATIONS AND SPECTRUM CONVERGENCE

Major A. Dorothea Sheasby

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

PAN-DOMAIN OPERATIONS AND SPECTRUM CONVERGENCE

By Major A. Dorothea Sheasby

Word Count: 2,363

Nombre de mots : 2.363

PAN-DOMAIN OPERATIONS AND SPECTRUM CONVERGENCE

AIM

1. Vehicles, weapons systems, sensors, communications and navigation equipment, the majority of the Canadian Armed Forces (CAF) is connected through information communication technology where invisible packets of information move at lightning speed, internal and external to the operating environment. There is a convergence of information and activities within the information environment, and the CAF needs to seize this opportunity to coordinate and restructure resources to maximize effects. The aim of this service paper is to discuss the challenges associated to pan domain operations, particularly focused on the cyber domain and evaluate what is required to enhance operational effectiveness to achieve mission success. This paper will not explore the requirement for improved CAF resilience within the information and cyber domains, but it cannot be ignored that the threat is no longer isolated to deployed capabilities, and that the interconnectedness of systems presents increased vulnerabilities to members at home and abroad.

INTRODUCTION

Current Operating Environment

2. Although pan domain is not a new concept, the recent recognition of the cyber domain is a new addition, and with it come unique challenges such as network protection and data integrity.[1] Several countries, such as the United Kingdom and the United States, have been immersed within the cyber domain for well over a decade. In 2016, the North Atlantic Treaty Organization (NATO) officially recognized cyber as a domain of military

[1] Will Spears, "A Sailor's Take on Multi-Domain Operations," Accessed Jan 14, 2021, https://warontherocks.com/2019/05/a-sailors-take-on-multi-domain-operations/.

operations; this recognition is a significant statement to adversaries because action within the cyber domain can now be subject to the NATO collective defence clause, whereby 'an attack against one is an attack against all.'[2]

3. While Canada and its allies have been focused on Counter-insurgency Operations (COIN), adversaries have been advancing their skills and capabilities to influence and leverage information and cyber operations to shape and achieve effects below the threshold of conflict. This 'grey-zone' will continue to be exploited, and the enemy will continually seek to disrupt, deter, and deny friendly forces, use and dominance within the borderless cyber and information domain. The CAF must be prepared to continuously defend its capabilities while also seeking opportunities to influence the information environment for periods of time to achieve or enable decisive action. Creating windows of opportunity will allow Canada and its allies to maximize capabilities and dominate our near-peer enemy.[3] Integration and collaboration of capabilities are vital to achieving future pan domain mission success.[4]

4. This paper will describe the current pan domain operating environment, with a particular focus on the convergence of electronic warfare and cyber operations. It will present three significant challenges that impact operational effectiveness: the current CAF force structure; the resource competition, and occupation management. The paper

---

[2] Maj A.D. Sheasby, "Global Vortex Essay: Cyber Security," (Joint Command Staff Course Paper, Canadian Forces College, 2020) 7-8, and Laura Brent, "*NATO's Role in Cyberspace*", Accessed Oct 24, 2020, https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html

[3] Kevin M. Woods and Thomas C. Greenwood, "*Multidomain Battle: Time for a Campaign of Joint Experimentation*," *Joint Force Quarterly : JFQ* no. 88 (First, 2018), 16.

[4] Department of Defence, *Electromagnetic Spectrum Superiority Strategy, (*Department of Defence - United States of America, 2020), 4-5.

will conclude with recommendations for improvements and further considerations to achieve future mission success.

DISCUSSION

Convergence within the information environment

5. Technology has driven the change in the battlespace and operating environment. Battlefields are no longer linear or contained within a defined geographical space depicted on a map. The current operating environment is vast, complex and multifaceted. Great power competition has created a shift and states are leveraging all aspects of diplomatic, information, military and economic (DIME) power to execute their strategy.[5] Although cyber may be a relatively new endeavor for the CAF, arguably we have been operating within the information environment and electronic magnetic spectrum (EMS) for decades. The electromagnetic spectrum is not a domain of its own, but it connects the domains and has significant overlap and congestion due to technology advances.[6] The cyber domain is slightly different because it is focused on networked information systems. Cyber is often viewed as a subset of the information domain but focused on computer systems and the Internet. The electromagnetic spectrum overlaps with cyber and the information domain – it is entangled. Where are the boundaries – and are they required?

6. Recent events in Ukraine have demonstrated adversarial capabilities to leverage multiple elements within the information environment, particularly the coordination of electronic warfare, information and cyber operations. US senior officials have recognized

---

[5] Department National Defence, *"DRAFT - Pan Domain Employment Concept,"* Ottawa, ON, 11.

[6] Department of Defence, *Electromagnetic Spectrum Superiority Strategy, (*Department of Defence - United States of America, 2020), 4.

the significance of the electromagnetic spectrum and identified it as a "tactical priority" since the enemy is "likely to achieve an asymmetric advantage that challenges the notion of US technological supremacy on the battlefield."[7]

Challenge: Force Structure

7. In recognition of the changing multi-domain operating environment the defence policy, *Strong Secure Engaged (SSE)*, has prioritized the investment in joint capabilities to improve "the development of military-specific information operations and offensive cyber operations capabilities able to target, exploit, influence, and attack in support of military operations."[8] However, the CAF's current approach to information and cyber operations is scattered and divided across numerous organizations within the CAF. To properly invest in capabilities, an integrated and comprehensive approach is required to facilitate interoperability and ensure that opportunities and vulnerabilities are completely considered.[9] There are several similarities between cyber operations and aspects of information operations, such as electronic warfare, which could enable or complement cyber effects, especially as the operating environment becomes increasingly interconnected.

8. The Canadian Army (CA) has only one Electronic Warfare Regiment, 21 EW Regt, which is now part of the Canadian Combat Support Brigade (CCSB).[10] The purpose

---

[7] "The New Battlefield: The Race to Integrate Cyber and Electronic Warfare," Accessed Jan 20, 2021, https://www.army-technology.com/features/new-battlefield-race-integrate-cyber-electronic-warfare/.

[8] Department of National Defence, *Strong, Secure, Engaged*, (Ottawa, ON: Department of National Defence, 2019), 41

[9] Department National Defence, *"DRAFT - Pan Domain Employment Concept,"* Ottawa, ON, 14, 21.

[10] Miranda Brumwell, *"Three Units Find a Home with Canadian Combat Support Brigade,"* Accessed Jan 28, 2021, https://www.cmfmag.ca/duty_calls/three-units-find-a-home-with-canadian-combat-support-brigade/.

of 21 EW Regt is to support the Canadian Mechanized Brigade Group (CMBG) in support of their line of operation tasks to the CA. The unit's role is exploiting the electromagnetic spectrum and denying the enemy the same ability while protecting friendly forces' ability to communicate and use the spectrum. The three main parts of electronic warfare are electronic protection (shield), electronic attack (act) and electronic support (sense).[11] Cyber operations also seek to exploit the electromagnetic spectrum by conducting offensive cyber operations (OCO) and defensive cyber operations (DCO) through computer networks and servers.[12] Electronic warfare and cyber operations seek to disrupt, degrade and disorient the adversary within the information environment to get inside their decision making cycle and influence their ability to act.

9. The Army's ground based electronic warfare entities can provide tactical level effects to support and enable a cyber operation. They can also deliver situational awareness to the commander by providing battle damage assessments (performance measures of effectiveness) and feedback on the operational effectiveness of the invisible effects delivered in the cyber domain. Cyberspace and electronic warfare are both a part of the information environment.[13]

10. The Canadian Forces Electronic Warfare Center (CFEWC) is another unit within the CAF that delivers capabilities within the electromagnetic spectrum. This unit is a part of the Canadian Forces Information Operations Group (CFIOG) within the Assistant Deputy Minister Information Management (ADM (IM)). The unit's role and function are

---

[11] John R. Hoehn and Catherine A. Theohary, "Convergence of Cyberspace Operations and Electronic Warfare," *Congressional Research Service* (August 13, 2019), https://crsreports.congress.gov/product/pdf/IF/IF11292.

[12] *Ibid.*, 3-2.

[13] Department of Defence, *Field Manual 3-38 - Cyber Electromagnetic Activities*, Washington, DC: Department of the Army, 2014, 1-6.

not linked to 21 EW Regt or connected to the Director General Cyber (DG Cyber) activities. There are numerous silos and a lack of coordination between the units focused on electronic warfare and this inhibits effectively operating within the information environment.

11. With the convergence of electronic warfare and cyber operations, similar desired effects can be achieved by employing tactical level electronic warfare assets (ground based or airborne) in the operating environment instead of utilizing strategic level cyber capabilities that require significant time to develop and strategic level authorizations. Electronic warfare support can search, intercept and locate signals within the EMS and produce assessed signals intelligence (SIGINT) which is used to support intelligence collection and analysis.[14]

12. The U.S. Army has recognized the importance of the converging capabilities and threats within the information environment, and they have established a field manual dedicated to Cyber Electromagnetic Activities (CEMA). CEMA is comprised of cyber operations (CO), electronic warfare (EW) and spectrum management operations (SMO).[15] The manual provides commanders and staff with direction on tactics and procedures to conduct and plan of these activities. The U.S. Army has been training small expeditionary cyber teams to defend and attack while employing EW to sense and conduct electronic attack and then have information operations experts link it together.[16]

---

[14] *Ibid.*,4-4.

[15] *Ibid.*,1-1.

[16] Mark Pomerleau, "Here's how the US Army is Planning Tactical Cyber Operations," Accessed Jan 20, 2021, https://www.c4isrnet.com/cyber/2020/10/09/heres-how-the-us-army-is-planning-tactical-cyber-operations/.

The combined teams approach provides the commander with increased situational awareness and a variety of operational effects for a mission.[17]

Challenge: Resource Competition

13. Capabilities require people, processes, training and equipment to accomplish a mission. SSE tasks no. 76 and 90 respectively aspire to increase personnel within influence operations and use reservists with particular skillsets to fill cyber operator billets.[18] The CAF is in direct competition with other government departments, industry and private sector for these highly proficient cyber experts. There is currently a skills gap in Canada, and it is not expected to be filled in the near future due to the education and training requirements.[19] Additionally, the security classification level required to operate within the military cyber domain is typically Top Secret with compartments, which can take a significant portion of time to obtain, an average of one year and potentially longer depending on if the member is new to the military or if they have been severing for several years with an existing security clearance.[20]

14. SSE also stated, task no. 88, that the CAF would develop active cyber capabilities to use against adversaries in future missions.[21] The Communications Security Establishment (CSE) Act (Bill C-59) was approved in June 2017, which provides future

---

[17] *Ibid.*

[18] Government of Canada, *Strong, Secure, Engaged - Canada's Defence Policy*, Ottawa: Department of National Defence, 2017, 111.

[19] Rob Rashotte, "The Critical Shortage of Cybersecurity Expertise," Accessed Jan 19, 2021, https://policyoptions.irpp.org/magazines/july-2019/the-critical-shortage-of-cybersecurity-expertise/.

[20] Government of Canada. "TPD/BGTD Frequently Asked Questions," Accessed Jan 19, 2021, https://www.canada.ca/en/health-canada/services/drugs-health-products/drug-products/activities/enhanced-review-capacity-initiative/frequently-asked-questions.html.

[21] Government of Canada, *Strong, Secure, Engaged - Canada's Defence Policy* …, 111.

opportunity to provide technical and operational support the CAF.[22] This will be an opportunity for the CAF to leverage CSE's extensive experience and expertise within the cyber domain to develop specific skills and capabilities. Collaboration with CSE will be vital to maximizing resources. However, with these increased abilities, the government of Canada has also implemented new oversight and compliance mechanisms. The CAF's cyber domain endeavors will be under scrutiny and review by the National Security and Intelligence Committee of Parliamentarians (NSICOP). This will require dedicated resources to ensure all information requests are delivered to the NSICOP on a routine basis.

Challenge: Occupation Management

15. The evolution of the information environment and the rapid advances in technology require highly specialized leaders who possess technical expertise, an understanding of information technology and strong institutional skills such as operational planning in order to understand the strategic context of the operating environment. Leaders within this field must be able to advise, plan and direct a variety of specialties such as EW, SIGINT and cyber to commanders and senior government officials to ensure the proper coordination of desired operational effects are delivered to achieve mission success.

16. In 2017, the cyber operator trade standup initiated the growth of the CAF's cyber capability. The trade is composed of non-commissioned members (NCM) with niche technical computer network expertise. However, with the establishment of the cyber

[22] Josh Gold, "Canadian Cyberspace Governance — Or Lack Thereof?" Accessed Jan 27, 2021, https://thecic.org/canadian-cyberspace-governance-or-lack-thereof/.

operator occupation, which is part of the Communication and Electronics branch, there has been no identification of a dedicated officer trade or leadership capacity to understand and manage the new occupation. With the convergence of capabilities within the information environment, there is a requirement for knowledge of the electromagnetic spectrum, cyberspace and various information communication technologies. Currently, the communications and electronics (J6 staff) and the intelligence branch (J2 staff) are the main officer trades that interact and manage the cyber operators and electronic warfare operators and signals intelligence operators (these NCMs come predominately from the Communicator Researcher Operator trade).

CONCLUSION

17. Since the cyber domain is not visible to the human eye, we cannot think about it like a traditional battlefield where we would be aware of exactly who is operating in that space and roughly where they were located. There is a convergence within the information environment, particularly electronic warfare and cyber operations, that present an opportunity for the CAF to integrate capabilities to enhance operational effectiveness and to ensure effects are coordinated across the entire information environment to gain an advantage and achieve mission success. The CAF must adapt and adjust; it cannot afford to remain wedded to current organizational structures or equipment that fought the last war.

RECOMMENDATIONS

18. The convergence of cyber and electronic warfare activities necessitates the requirement for 21 EW Regt to be equipped with enhanced tactical level responsibilities and capabilities that can enable and support strategic level cyber activities. The CA

annual high readiness confirmation exercise MAPLE RESOLVE would be an opportunity to trial tactical cyber capabilities and scenarios. The initial planning conferences are typically held in the spring the year prior, and this would provide the opportunity to conduct preliminary discussions about incorporating cyber activities into the exercise. Coordination and training could be conducted this summer/fall 2021 between the 21 EW Regt and Director General Information Operations (DGIMO). DG Cyber should engage with Director Land Requirements (DLR) to consider future capabilities development, resourcing, and activities that land based electronic warfare platforms perform to deliver effects within the cyber domain and to protect against cyber threats (specifically the delivery and conduct of offensive cyber operations at the tactical level).

19. There is an immediate requirement to establish a sub-occupation or specialization within the Communications and Electronics (C&E) branch for an Information Warfare Officer (IWO). Recognizing the personnel shortages across the CAF, the creation of a new officer trade is not feasible. However, due to significant private and public sector demands for personnel with niche technical skills, serious consideration must be given to salary incentives and career/talent management for future IWOs and the current cyber operator occupation to improve recruitment and retention opportunities. A working group (WG) should be established with a six-month timeline to present a comprehensive option analysis to DGIMO.

20. The convergence between the cyber and information domain make it challenging to know exactly where one ends and the other begins due to the rapid tech advances. The cyber and EMS environment should be merged into a unified environment known as

"cyber-electromagnetic environment." Further study and review should be conducted of the various units and sections within the CAF involved in cyber, electronic warfare, or information operations and whether or not it is feasible to establish a joint CEMA construct for the CAF. There are too many silos within the institution, and consideration should be given to reviewing the current command and control relationships with a view to consolidating like entities. There are limited resources across the CAF, and the institution cannot afford to have duplication of effort or missed opportunities for collaboration due to separate and different chains of command. A WG should be made up of representatives from across the L1 organizations to present initial feedback to DGIMO by summer 2021. The WG should be prepared to propose various force structures that can best house and support a CEMA to deliver operational effectiveness for the CAF.

BIBLIOGRAPHY

Field Manual 3-38 - Cyber Electromagnetic Activities. Washington, DC: Department of the Army, 2014.

"The New Battlefield: The Race to Integrate Cyber and Electronic Warfare." Accessed Jan 20, 2021. https://www.army-technology.com/features/new-battlefield-race-integrate-cyber-electronic-warfare/.

Brumwell, Miranda. "Three Units Find a Home with Canadian Combat Support Brigade." Accessed Jan 28, 2021. https://www.cmfmag.ca/duty_calls/three-units-find-a-home-with-canadian-combat-support-brigade/.

Department National Defence. "Pan Domain Employment Concept." Ottawa, ON.

Department of Defence. *Department of Defence Electromagnetic Spectrum Superiority Strategy* : Department of Defence - United States of America, 2020.

Gold, Josh. "Canadian Cyberspace Governance — Or Lack Thereof?" Accessed Jan 27, 2021. https://thecic.org/canadian-cyberspace-governance-or-lack-thereof/.

Government of Canada. *Strong, Secure, Engaged - Canada's Defence Policy*. Ottawa: Department of National Defence, 2017.

———. "TPD/BGTD Frequently Asked Questions." Accessed Jan 19, 2021. https://www.canada.ca/en/health-canada/services/drugs-health-products/drug-products/activities/enhanced-review-capacity-initiative/frequently-asked-questions.html.

Hoehn, John R. and Catherine A. Theohary. "Convergence of Cyberspace Operations and Electronic Warfare." *Congressional Research Service* (August 13, 2019). https://crsreports.congress.gov/product/pdf/IF/IF11292.

Woods, Kevin M. and Thomas C. Greenwood. "Multidomain Battle: Time for a Campaign of Joint Experimentation." *Joint Force Quarterly : JFQ* no. 88 (First, 2018): 14-21. https://search-proquest-com.cfc.idm.oclc.org/trade-

journals/multidomain-battle-time-campaign-joint/docview/2040739033/se-2?accountid=9867.

Pomerleau, Mark. "Here's how the US Army is Planning Tactical Cyber Operations." Accessed Jan 20, 2021. https://www.c4isrnet.com/cyber/2020/10/09/heres-how-the-us-army-is-planning-tactical-cyber-operations/.

Public Safety Canada. *The Future Security Environment 2013-2040*. Ottawa, ON: Chief of Force Development.

Rashotte, Rob. "The Critical Shortage of Cybersecurity Expertise." Accessed Jan 19, 2021. https://policyoptions.irpp.org/magazines/july-2019/the-critical-shortage-of-cybersecurity-expertise/.

Sheasby, A. D. Maj. "Global Vortex Essay: Cyber Security." Canadian Forces College, 2020.

Spears, Will. "A Sailor's Take on Multi-Domain Operations." Accessed Jan 14, 2021. https://warontherocks.com/2019/05/a-sailors-take-on-multi-domain-operations/.