National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

CANADIAN CYBER FORCE:
A DISTINCT ENVIRONMENTAL COMMAND FOR THE CAF'S CYBER DOMAIN

Major Jessica F. Bélanger

JCSP 50

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 n° 50

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.

CANADIAN FORCES COLLEGE - COLLÈGE DES FORCES CANADIENNES

JCSP 50 - PCEMI n° 50
2023 - 2024

Service Paper – Étude militaire

CANADIAN CYBER FORCE: A DISTINCT ENVIRONMENTAL COMMAND FOR THE CANADIAN ARMED FORCES CYBER DOMAIN

Major Jessica F. Bélanger

CANADIAN CYBER FORCE: A DISTINCT ENVIRONMENTAL COMMAND FOR THE CANADIAN ARMED FORCES CYBER DOMAIN

AIM

1. In 2017, the latest defence policy*, Strong, Secure, Engaged – Canada's Defence Policy (SSE),* recognized cyber as a domain and "critical for the conduct of military operations."[1] Six years later, the *Pan-Domain Force Employment Concept– Prevailing in a Dangerous World (PFEC)* recognizes the importance of the five domains, such as maritime, land, air, space and cyber equally.[2] Despite the recognition of the cyber and space domains by SSE and the PFEC, the Canadian Armed Forces (CAF) currently has only environmental commands for three domains: maritime, land and air.[34] This service paper proposes creating an environmental command[5] for the cyber domain in the CAF named the Canadian Cyber Force (CCF).[6]

INTRODUCTION

Current Problems with the CAF Cyber Force

2. The CAF recognizes five following domains: maritime, land, air, space, and cyber, which shape the conduct of military operations due to their physical attributes.[7] This service paper has identified the following issues that justify the establishment of an additional environmental command in the CAF.

3. The first problem is that the CAF Cyber Force[8] is not administrated, managed, and commanded like the other existing domains. Environmental Chief of Staff (ECS), such as the Royal Canadian Navy (RCN), Canadian Army (CA) and the Royal Canadian Air

[1] National Defence, *Strong Secure Engaged - Canada's Defence Policy* (Her Majesty the Queen in Right of Canada, as represented by the Minister of National Defence, 2017), 72.

[2] Minister of National Defence, *Pan-Domain Force Employment Concept - Prevailing in a Dangerous World* (His Majesty the King in Right of Canada, as represented by the Minister of National Defence, 2023), 15.

[3] Canadian Forces Experimentation Centre, *Canadian Forces Joint Publication - CFJP 01 Canadian Military Doctrine - B-GJ-005-000/FP-001* (Her Majesty the Queen in Right of Canada, as represented by the Minister of National Defence, 2011), 4-2.

[4] See Annex B for more details about the DND and the CAF organizational structure.

[5] "National Defence Act (R.S.C., 1985, C. N-5) - Loi Sur La Défense Nationale (L.R.C., 1985, Ch. N-5)," last modified January 23, accessed Feb 18, 2024, https://laws-lois.justice.gc.ca/eng/acts/N-5/FullText.html#h-374706.

[6] This name does not exist. The Canadian Cyber Force (CFF) is the proposed name for the CAF Cyber Forces environmental command.

[7] Minister of National Defence, *Pan-Domain Force Employment Concept - Prevailing in a Dangerous World*, 15

[8] The current CAF Cyber Force includes "military and civilians personnel that force generate, employ and develop cyber operations, network operations and the Cyber Mission Assurance (CMA)." Source: DG Evaluation ADM(RS), *Evaluation of the Cyber Forces 1258-3-031-AMD(RS)*, 2021), 5.

Force (RCAF) report to the Chief of Defence Staff (CDS).[9] These environmental commands are under the operational chain of command and have command authority. Nevertheless, the chain of command of the CAF Cyber Force is different. Currently, the Chief of Staff Information Management (COS (IM)), Cyber Force Commander (CFC) and Chief of Cyberspace Staff are the same person.[10] Like other ECSs, the Cyber Force Commander (CFC) does report to the CDS; however, as the COS (IM), it reports to the Defence Chief Information Officer.[11]

4. This C2 is not ideal because it doesn't give the CFC a peer seat at the same table as other environmental command commanders: the CFC is a major general, and the ECSs are lieutenant generals. Also, ADM(IM) does not have command authority since it operates outside the operational chain of command.[12] Moreover, this C2 can hardly favour a pan-domain integration proposed by the PFEC, which requires the CAF "to act with synergy across the entirety of the operating environment."[13] Integrating the cyber domain into operations is difficult when there is no distinct environmental command for the cyber to act as a champion for CAF Cyber Force at the same level as other environmental commands.

5. The second problem is related to the Force Generation (FG) for CAF Cyber Force. The *Evaluation of the Cyber Force* mentioned that career development and opportunities for members are limited.[14] Currently, the availability of cyber military occupations is limited to one military occupation, Cyber Operator, and it is only available for non-commissioned members (NCM).[15] There is no military occupation dedicated to cyber officers. This is a problem because no proper career management exists for officers working within the CAF Cyber Force. Furthermore, the absence of officer military occupation for cyber does not allow adequate development of the CAF Cyber Force.[16]

6. This service paper will propose an ambitious and mature vision of what the CAF Cyber Force should be: a distinct environmental command. The first part of this service paper will present arguments to justify the establishment of an environmental command for the CAF Cyber Force. The second and third parts demonstrate that the CCF can achieve the F5 Model Framework and apply the five operation functions at the same level as other environmental commands.

[9] "Organizational Structure of the Department of National Defence and the Canadian Armed Forces," last modified September 21, accessed February 4, 2024, https://www.canada.ca/en/department-national-defence/corporate/organizational-structure.html#orgchart.

[10] National Defence DDFP2, *NDHQ Organization Change - C Cyber (Administered by ADM(IM))*, 2018), 1.

[11] Ibid.

[12] DG Evaluation ADM(RS), *Evaluation of the Cyber Forces 1258-3-031-AMD(RS)*, 14.

[13] Minister of National Defence, *Pan-Domain Force Employment Concept - Prevailing in a Dangerous World*, 7.

[14] DG Evaluation ADM(RS), *Evaluation of the Cyber Forces 1258-3-031-AMD(RS)*, 25.

[15] "Cyber Operator," accessed February 4, 2024, https://forces.ca/en/career/cyber-operator/.

[16] DG Evaluation ADM(RS), *Evaluation of the Cyber Forces 1258-3-031-AMD(RS)*, 26.

DISCUSSION

An Environmental Command for the CAF Cyber Force

7. This section will provide four arguments demonstrating that the CAF should create an environmental command for the cyber domain. The first argument concerns the arrival of Emerging and Disruptive Technologies. The second argument is about facilitating the application of the PFEC and integrating cyber operations within CAF's operations. The third argument is proposing a proper C2 for the CCF. The last argument discusses talent management.

Emerging and Disruptive Technologies (EDTs)

8. Warfare has always been shaped by technological innovation; however, EDTs[17], such as artificial intelligence (AI), robotization, or quantum computing, will change the nature of war at an unprecedented scale and speed.[18] Even if EDTs are already present in our daily lives, they are still at an early stage of development.[19] EDTs will be game changers by increasing interconnectivity between people and machines, contributing to global-scale economic, societal, war and conflict transformations.[20] Therefore, by changing the nature of conflicts, EDTs will bring many opportunities and risks for military forces.[21] CAF's adversaries are already in the race to leverage EDTs to gain a decisive advantage.[22]

9. Sustaining military preparedness is directly tied to the integration and operationalization[23] of EDTs.[24] The CAF has no choice but to operationalize some EDTs to remain relevant against future threats and near-competitor adversaries. As mentioned in the *NATO Advisory Group on EDT Annual Report 2021,* keeping change with EDTs will necessitate agile and rapid integration.[25] In addition to delivering effects with traditional cyber operations, the CCF could also become the responsible environmental command and the champion for integrating, operationalizing and defending EDTs leveraged by the CAF. In this manner, the CCF would provide an edge to the CAF in future conflicts over its adversaries and ensure Canada keeps pace with its allies.[26]

[17] See Annex B – Emerging and Disruptive Technologies for more details about definition and examples.
[18] Daniel Araya, *Artificial Intelligence for Defence and Security - Special Report* (Waterloo: Centre for International Governance Innovation, 2022), 1.
[19] NATO Advisory Group EDT, *NATO Advisory Group on Emerging and Disruptive Technologies - Annual Report 2021* (NATO Headquarters Brussels, Belgium: NATO Emerging Security Challenges Division,[2022]).
[20] Ibid.
[21] "Emerging and Disruptive Technologies," last modified June 22, accessed January 31, 2024, https://www.nato.int/cps/en/natohq/topics_184303.htm.
[22] Canadian Armed Forces, *Canadian Armed Forces Digital Campaign Plan* (His Majesty the King in Right of Canada, as represented by the Minister of Environment and Climate Change, 2022), 4.
[23] The operationalization of EDTs means leveraging the technology to deliver effects for military operations.
[24] Araya, *Artificial Intelligence for Defence and Security - Special Report*, 5.
[25] Ibid., 20.
[26] Canadian Armed Forces, *Canadian Armed Forces Digital Campaign Plan*, 4.

Pan-Domain Force Employment Concept (PFEC)

10. Having an environmental command for the cyber domain will facilitate the achievement of the PFEC's imperatives to counter current and future global threats.[27] The PFEC recognizes the importance of the five domains since their specific properties change how military operations are conducted. [28] The PFEC emphasizes that CAF's environmental commands must prioritize a pan-domain approach by focusing on what they can contribute to other domains and being ready to deliver effects in other domains.[29] Furthermore, it highlights the importance of developing expertise in all domains, which must be incorporated into operations.[30] It is also mentioned that CAF must "leverage operational experience to thoroughly understand each domain's unique characteristics and how effects from across domains come together."[31] Establishing the CCF will enhance CAF's ability to deliver effects through all domains and achieve the PFEC's imperatives.

Proposed C2 for the CCF

11. As mentioned in the introduction, the current C2 poses problems. First, the COS(IM) and the Director General Information Management Officer (DGIMO)[32] are triple-hatted and double-hatted, respectively. This causes conflicts of interest between being a service provider and a defender of DND and CAF information systems. Moreover, because Cyber Force Commander is a secondary and even a tierce function, it might be difficult for this person to fully focus on commanding the CAF Cyber Force. This might explain the absence of a champion for the cyber domain at the highest level of the organization and the lack of defined Accountability, Responsibility and Authority (ARA).[33] Creating a new environmental command would fix C2 issues and promulgate the CAF Cyber Force at the highest levels, where the CCF commander would have a seat at the same table beside their peers: the CA, RFAC and RCN commanders.

Talent Management

12. The *Evaluation of the Cyber Forces* compiled by ADM (Review Services) in April 2021 has identified issues in FG for the CAF Cyber Force, such as the cyber military professional development and the difficulties in filling cyber positions.[34] Creating an environmental command for the CAF Cyber Force is believed to reduce the current problems with FG. Currently, career managers from all environmental commands identify NCMs and officers with skills in cyber to be posted in CAF Cyber Force's

[27] Minister of National Defence, *Pan-Domain Force Employment Concept - Prevailing in a Dangerous World*, 19-20.

[28] Ibid., 15.

[29] Ibid., 20.

[30] Ibid.

[31] Ibid.

[32] The DGIMO is also fulfilling the Joint Force Cyber Component Command function.

[33] DG Evaluation ADM(RS), *Evaluation of the Cyber Forces 1258-3-031-AMD(RS)*, 15.

[34] DG Evaluation ADM(RS), *Evaluation of the Cyber Forces 1258-3-031-AMD(RS)*, 2021), 24.

positions.[35] After a few years in the position, they are most likely being posted out of CAF Cyber Force. This negatively impacts the Force Development (FD) and FG since skills in cyber fade rapidly.[36]

13. As is true in the traditional warfighting domains, the cyber domain requires people with very specialized and diverse skills.[37] By creating an environmental command for the cyber domain, it will be necessary to review current military occupations and assess future needs. The Cyber Operator military occupation for NCMs was created a few years ago, and their main task is to conduct defensive and offensive cyber operations.[38] However, as of now, there is no military occupation for officers dedicated to cyber operations. The creation of an environmental command for the cyber domain would require the establishment of a military occupation for the cyber officer.[39] These officers would specialize in cyber warfare the same way pilots, Naval Warfare Officers, or infantry officers specialize in their domain warfare.

14. In the near future, the CCF might have to create additional military occupations beyond the "traditional" cyber operations. New military occupations for NCMs and officers must be created to facilitate the integration and operationalization of EDTs. For instance, the operationalization of AI and robotics will require new military occupations; see Annex B for more details. Offering additional military occupations equivalent to what can be found in the industry will facilitate recruiting people with specific skills and expertise.

15. A distinct environmental command for the cyber domain will positively impact people. First, being associated with a distinct organization will increase the sense of belonging and unity of effort, the same way combat arms troops have a sense of belonging to the Canadian Army. Second, it will favour a clear pathway for NCMs' and officers' professional advancement. It is recommended to assess future needs for additional military occupations. Creating new specialized and highly technical military occupations will help attract talent. Finally, it will also facilitate knowledge sharing, which is essential to maintain the speed of progress.

CCF F5 Model Framework

16. The F5 Model Framework describes the entire spectrum of military activities necessary for armed forces to achieve operational effects.[40] The *Evaluation of the Cyber Forces* recommends identifying proper ARAs for each role from the F5 model for CAF

[35] Ibid., 26.

[36] Ibid., 26.

[37] National Defence, *Department of National Defence and Canadian Armed Forces 2023-24 - Departmental Plan* (His Majesty the King in Right of Canada, as represented by the Minister of National Defence, 2023a), 37.

[38] "Cyber Operator."

[39] DG Evaluation ADM(RS), *Evaluation of the Cyber Forces 1258-3-031-AMD(RS)*, 26.

[40] "Report on Transformation 2011," last modified August 8, accessed January 22, 2024, https://www.canada.ca/en/department-national-defence/corporate/reports-publications/report-on-transformation-2011.html#a6-1.

Cyber Force.[41] A more detailed description of the F5 Model Framework for the CCF is provided in Table 1 in Annex D. First, the Force Employment (FE) would remain the same organizations as other environmental commands, which are the Canadian Joint Operations Command, the Canadian Special Operations Forces and the North American Aerospace Defence Command (NORAD. Second, CCF's main function would be being a Force Generator at the same level as other environmental commands. To achieve efficient FG and Force Support, the CCF would need its environmental logistics, communications, intelligence and military police NCMs and officers.[42] Additionally, the CCF should establish a centre of excellence for its Force Development (FD). Finally, the CCF's Force Management (FM) would be achieved by creating cyber environmental human resources and financial control positions within its headquarters.

Operational Functions

17. Command, Sense, Act, Shield, and Sustain are the five operational functions, which are functional capabilities to deploy and employ forces optimally.[43] This section describes each operational function and considerations for the CCF to accomplish them. The purpose is to validate how the CAF Cyber Force embedded under an environmental command could achieve the five operational functions.

Command

18. The Command is central since it integrates all other operational functions.[44] This function provides the establishment of an effective C2 under a Joint Task Force commander for the employment of military power that enables unity of purpose and effort.[45] With the appointment of a Joint Force Cyber Component Commander, the CCF would enable a component command like other ECSs. For the cyber domain, the command function will require significant coordination and cooperation with civilian authorities, governmental organizations such as the Communications Security Establishment or Shared Services Canada, academic institutions, and the industry.[46]

Sense

19. The Sense function is fundamental for operations within the cyber domain since it is the function that provides knowledge to the commander.[47] This function includes all activities that collect and process data.[48] Moreover, cyber operations require the ability to

[41] DG Evaluation ADM(RS), *Evaluation of the Cyber Forces 1258-3-031-AMD(RS)*, 30.
[42] See Annex C for more details.
[43] Canadian Forces Warfare Centre, *Canadian Forces Joint Publication - CFJP 3.0 Operations - B-GJ-005-300/FP-001* (Her Majesty the Queen in Right of Canada, as represented by the Minister of National Defence, 2011), 1-5.
[44] Ibid.
[45] Ibid.
[46] Canadian Forces Warfare Centre, *Canadian Forces Joint Publication - CFJP 3.0 Operations - B-GJ-005-300/FP-001*, 1-5.
[47] Ibid.
[48] Ibid.

sense within and outside CAF networks.[49] Future conflicts and wars are expected to leverage the cyber domain, and therefore, CAF must augment its intelligence capabilities in this environment.[50]

20. Defensive and offensive cyber operations require significant intelligence to be conducted efficiently.[51] The CCF should have cyber environmental intelligence officers and NCMs who will be specialists in cyberspace and EDTs. Furthermore, leveraging EDTs, such as AI, to augment intelligence capabilities will be key to collecting and processing data.

Act

21. The combination of firepower, manoeuvre, and information operations to deliver desired effects are activities of the Act's function.[52] The latest integrates, synchronizes and harmonizes joint fires and activities of influence through the operational environment.[53] The CCF will become specialized in the conduct of cyber operations. In addition to these "traditional operations," it will have to adapt and develop new types of operations and new ways of delivering effects that will be enabled by EDTs, such as AI and robotization.

Shield

22. This operational function protects the force, its capabilities and freedom of manoeuvre in the environment.[54] Shield provide a defence against conventional and non-conventional threats and self-protection measures.[55] The CCF will have two main tasks under the Shield operational function. The first task will be the defence of all CAF cyber capabilities, such as networks and information systems. The second task will be defending EDTs operationalized by the CAF, such as AI models.

Sustain

23. The operational function Sustain regenerates and maintains capabilities during operation.[56] The sustainment of the CCF's operation requires access to cutting-edge technologies, equipment, software and hardware. It is recommended to create a cyber environmental logistic officer and NCM military occupations; see Annex B. Since the

[49] D Cyber FD, *Canadian Armed Forces Joint Doctrine Note - 2017-02 - Cyber Operations* (Her Majesty the Queen as represented by the Minister of National Defence, 2107), 5-18 - 5-20.
[50] Araya, *Artificial Intelligence for Defence and Security - Special Report*, 12.
[51] D Cyber FD, *Canadian Armed Forces Joint Doctrine Note - 2017-02 - Cyber Operations*, 5-18 - 5-20.
[52] Canadian Forces Warfare Centre, *Canadian Forces Joint Publication - CFJP 3.0 Operations - B-GJ-005-300/FP-001*, 1-5.
[53] Ibid.
[54] Ibid.
[55] Ibid.
[56] Canadian Forces Warfare Centre, *Canadian Forces Joint Publication - CFJP 3.0 Operations - B-GJ-005-300/FP-001*, 1-5.

evolution of technologies is extremely rapid, the CCF will need experts in procurement and logistic for the cyber domain.

CONCLUSION

24. This service paper intends to demonstrate the requirement to create an environmental command for the cyber domain in the CAF. Two main problems were identified regarding the current CAF Cyber Force: problematic C2 and talent management.

25. The establishment of the CCF would address these issues. The CCF will generate military forces to conduct cyber operations and operationalize EDTs, providing the CAF with an edge in future conflicts and remaining a reliable partner. Moreover, the establishment of the CCF will facilitate pan-domain FE. Furthermore, a distinct environmental command will improve talent management by establishing a sense of belonging to an element, cohesion and unity of effort among its members. New military occupations must be created to attract people with specialized expertise and to provide them with a proper career pathway for their professional advancement. Lastly, this service paper's second and third parts explain how the CCF would achieve the F5 framework model and apply the five operational functions, which describe the desired end state of a mature environmental command for the cyber domain.

RECOMMENDATION

26. The DND and the CAF can choose between different approaches for integrating the CAF Cyber Force: keeping the status quo[57], integrating within the current environmental commands, establishing a non-environmental command or creating an environmental command. This service paper recommends establishing a distinct environmental command for the CAF Cyber Force, which could be named the Canadian Cyber Force.

27. All possible approaches presented above should be assessed. Several factors could influence the decision, especially the financial cost of revamping the CAF Cyber Force and creating additional military occupations. The second option, integrating within current services, might facilitate the pan-domain approach proposed by the PFED since ECSs would be responsible for their cyber operations. However, it might create discrepancies in the cyber forces' maturity and fragment initiatives between environmental commands, as is currently the case for AI.[58] Therefore, having one commander and integrating the CAF Cyber Force under a distinct environmental command would be recommended to avoid duplicating efforts and discrepancies between environments. From a short-term perspective, the CCF option might be the costliest; however, it might have the best return on investment for the CAF. Besides, the CAF should adopt a long-term vision for their CAF Cyber Force. It would be recommended to

[57] The current situation for the CAF Cyber Force.

[58] Minister of National Defence, *The Department of National Defence and Canadian Armed Forces Artificial Intelligence Strategy*Her Majesty the Queen in Right of Canada as represented by the Minister of National Defence, 2022), 2.

envision what the CAF would need to operationalize its cyber domain for the next fifty to hundred years. The CCF would establish the foundations of that vision.

ANNEXES

A. Annex A – Organizational Structure of the Department of National Defence and the Canadian Armed Forces
B. Annex B – Emerging and Disruptive Technologies
C. Annex C – Proposed Military Occupations for the Cyber Domain
D. Annex D – F5 Framework Model

BIBLIOGRAPHY

Canada. Department of National Defence. "Director General Information Capabilities Force Development (DGICFD)." . Accessed February 8, 2024. http://admim-smagi.mil.ca/im_intranet/about/organization/dgicfd.page.

Araya, Daniel. *Artificial Intelligence for Defence and Security - Special Report*. Waterloo: Centre for International Governance Innovation, 2022.

Bojanova, Irena, Ric Kuhn, and Jeffrey Voas. "Emerging Disruptive Technologies." 56, no. 12 (December, 2023): 27-30. doi:10.1109/MC.2023.3314933. https://ieeexplore.ieee.org/document/10319846.

Canada. Department of National Defence. *Canadian Armed Forces Digital Campaign Plan.* 2022.

Canada. Department of National Defence. *Canadian Forces Joint Publication - CFJP 01 Canadian Military Doctrine - B-GJ-005-000/FP-001.* 2011.

Canada. Department of National Defence. *Canadian Forces Joint Publication - CFJP 3.0 Operations - B-GJ-005-300/FP-001.* 2011.

Canada. Department of National Defence. *Canadian Armed Forces Joint Doctrine Note - 2017-02 - Cyber Operations.* D Cyber FD, 2107.

Canada. Department of National Defence. *NDHQ Organization Change - C Cyber (Administered by ADM(IM)).* 2018.

Canada. Department of National Defence. *Evaluation of the Cyber Forces 1258-3-031-AMD(RS)* 2021.

Canada. Department of National Defence. "The Canadian Armed Forces Browse Careers." Accessed February 8, 2024. https://forces.ca/en/careers.

Canada. Department of National Defence. "Cyber Operator." Accessed February 4, 2024. https://forces.ca/en/career/cyber-operator/.

Gupta, Sakshi. "10 Awesome & High-Paying AI Careers to Pursue in 2024." Accessed February 4, 2024. https://www.springboard.com/blog/data-science/careers-in-ai/.

Lele, Ajey. *Disruptive Technologies for the Military Security* Springer Nature Singapore, 2018.

Canada. Minister of Justice. "National Defence Act (R.S.C., 1985, C. N-5) - Loi Sur La Défense Nationale (L.R.C., 1985, Ch. N-5)." Accessed Feb 18, 2024. https://laws-lois.justice.gc.ca/eng/acts/N-5/FullText.html#h-374706.

Canada. Department of National Defence. *Canadian Forces Joint Publication - CFJP 01 Military Doctrine.* 2011.

Canada. Department of National Defence. *The Department of National Defence and Canadian Armed Forces Artificial Intelligence Strategy.* 2022.

Canada. Department of National Defence. *Pan-Domain Force Employment Concept - Prevailing in a Dangerous World.* 2023.

Canada. Department of National Defence. "Assistant Deputy Minister (Information Management)." Accessed February 4, 2024. https://www.canada.ca/en/department-national-defence/corporate/organizational-structure/assistant-deputy-minister-information-management.html.

Canada. Department of National Defence. *Beyond the Horizon - A Strategy for Canada's Special Operations Forces in an Evolving Security Environment.* 2020a.

Canada. Department of National Defence. *The Department of National Defence and Canadian Armed Forces - Data Strategy*. 2019.

Canada. Department of National Defence. *Department of National Defence and Canadian Armed Forces 2023-24 - Departmental Plan.* 2023a.

Canada. Department of National Defence. "Organizational Structure of the Department of National Defence and the Canadian Armed Forces." Accessed February 4, 2024. https://www.canada.ca/en/department-national-defence/corporate/organizational-structure.html#orgchart.

Canada. Department of National Defence. "Report on Transformation 2011." Accessed January 22, 2024. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/report-on-transformation-2011.html#a6-1.

Canada. Department of National Defence. *Strong Secure Engaged - Canada's Defence Policy.* 2017.

NATO. "Emerging and Disruptive Technologies." Accessed January 31, 2024. https://www.nato.int/cps/en/natohq/topics_184303.htm.

NATO Advisory Group EDT. *NATO Advisory Group on Emerging and Disruptive Technologies - Annual Report 2021*. NATO Headquarters Brussels, Belgium: NATO Emerging Security Challenges Division, 2022.

NATO Allied Command Transformation. "Fact Sheet - Military Uses of Artificial Intelligence, Automation, and Robotics (MUAAR)." Accessed February 14, 2024. https://www.act.nato.int/wp-content/uploads/2023/05/2019_MCDC_MUAAR-2.pdf.

Reding, D. F. and J. Eaton. *Science & Technology Trends 2020-2040 - Exploring the S&T Edge NATO Science & Technology Organization*. Brussels: NATO Science & Technology Organization, 2020.

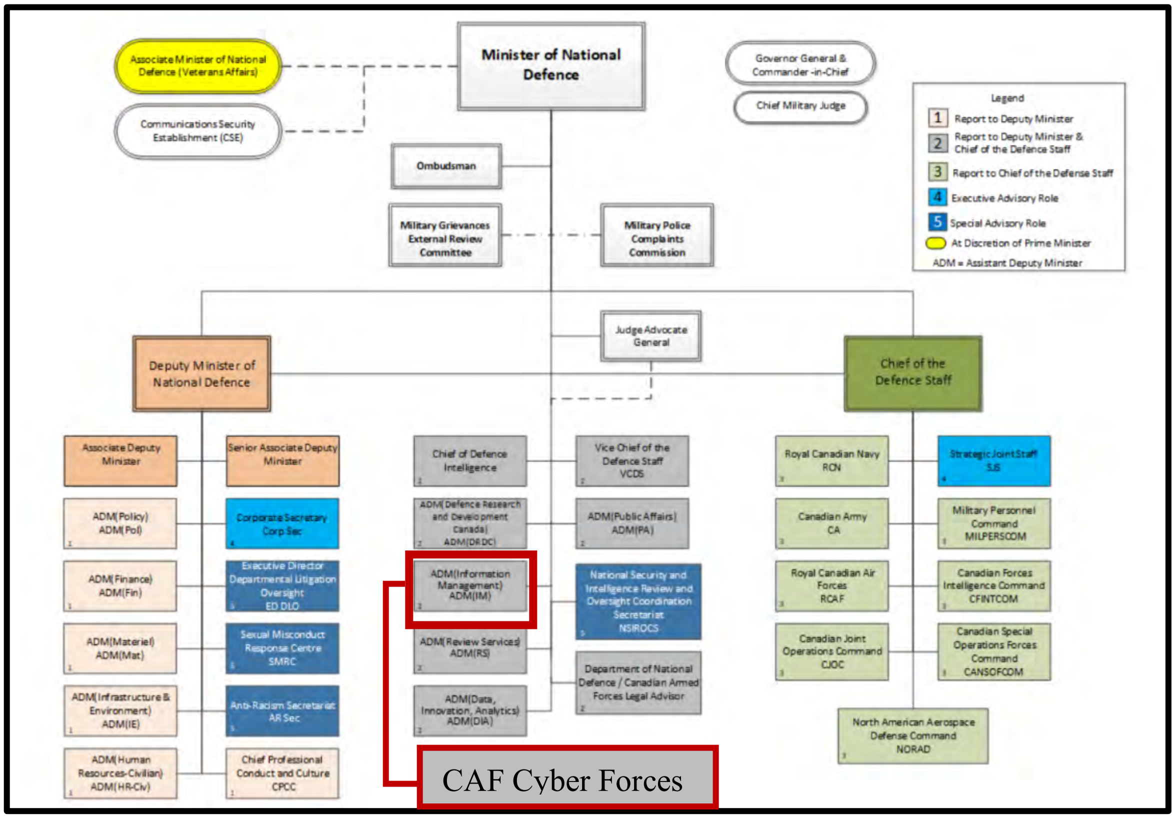
Canada. Department of National Defence. "Royal Canadian Air Force Aerospace Warfare Centre." Accessed February 4, 2024. https://www.canada.ca/en/air-force/corporate/royal-canadian-air-force-aerospace-warfare-centre.html.

Smeets, Max. *No Shortcuts - Why States Struggle to Develop a Military Cyber-Force.* Oxford University Press, 2022.

This page intentionally left blank.

ANNEX A – ORGANIZATIONAL STRUCTURE OF THE DEPARTMENT OF NATIONAL DEFENCE AND THE CANADIAN ARMED FORCES

1. The figure below is the current organizational structure of the DND and the CAF.



Associate Minister of National Defence (Veterans Affairs)
Communications Security Establishment (CSE)
Minister of National Defence
Governor General & Commander -in-Chief
Chief Military Judge
Legend
1 Report to Deputy Minister
2 Report to Deputy Minister & Chief of the Defence Staff
3 Report to Chief of the Defense Staff
4 Executive Advisory Role
5 Special Advisory Role
At Discretion of Prime Minister
ADM = Assistant Deputy Minister
Ombudsman
Military Grievances External Review Committee
Military Police Complaints Commission
Judge Advocate General
Deputy Minister of National Defence
Chief of the Defence Staff
Associate Deputy Minister
Senior Associate Deputy Minister
ADM(Policy) ADM(Pol)
Corporate Secretary Corp Sec
ADM(Finance) ADM(Fin)
Executive Director Departmental Litigation Oversight ED DLO
ADM(Materiel) ADM(Mat)
Sexual Misconduct Response Centre SMRC
ADM(Infrastructure & Environment) ADM(IE)
Anti-Racism Secretariat AR Sec
ADM(Human Resources-Civilian) ADM(HR-Civ)
Chief Professional Conduct and Culture CPCC
Chief of Defence Intelligence
Vice Chief of the Defence Staff VCDS
ADM(Defence Research and Development Canada) ADM(DRDC)
ADM(Public Affairs) ADM(PA)
ADM(Information Management) ADM(IM)
National Security and Intelligence Review and Oversight Coordination Secretariat NSIROCS
ADM(Review Services) ADM(RS)
Department of National Defence / Canadian Armed Forces Legal Advisor
ADM(Data, Innovation, Analytics) ADM(DIA)
CAF Cyber Forces
Royal Canadian Navy RCN
Strategic Joint Staff SJS
Canadian Army CA
Military Personnel Command MILPERSCOM
Royal Canadian Air Forces RCAF
Canadian Forces Intelligence Command CFINTCOM
Canadian Joint Operations Command CJOC
Canadian Special Operations Forces Command CANSOFCOM
North American Aerospace Defense Command NORAD

Figure 1 - Organizational Structure of the DND and the CAF

Source: "Organizational Structure of the Department of National Defence and the Canadian Armed Forces," last modified September 21, accessed February 4, 2024, https://www.canada.ca/en/department-national-defence/corporate/organizational-structure.html#orgchart.

2. The figure shows in green the three environmental commands reporting directly to the Chief of Defence Staff: Royal Canadian Navy (RCN), Canadian Army (CA) and Royal Canadian Air Forces (RCAF). The CAF Cyber Forces is embedded under ADM(IM) and the Defence CIO reports to the Deputy Minister of National Defence.

ANNEX B – EMERGING AND DISRUPTIVE TECHNOLOGIES

1. This annex will provide a definition of Emerging and Disruptive Technologies and examples.

Definition

2. Emerging and Disruptive Technologies (EDT) could be defined as "technical innovations that render existing technologies and social relations obsolete or radically altered."[59]

3. For a technology to be considered an EDT, the *Science & Technology Trends 2020-2040 - Exploring the S&T Edge NATO Science & Technology Organization* report established three conditions: emergent, disruptive and convergent.[60] A technology predicted to reach maturity between 2020 and 2040 is considered "emergent."[61] This same technology must be "disruptive," meaning a major revolutionary impact.[62] Finally, to be categorized as an EDT, the technology must be "convergent," which means that the technology must be emergent and disruptive at the same time.[63]

Examples

4. Here are some examples of EDTs[64]:

- Nanotechnology;
- Biotechnology;
- Genome Editing and Synthetic Biology;
- Artificial Intelligence;
- Neural Nets and Machine Learning;
- Quantum and Biological Computing and Molecular Communication;
- Robotics and Automation (Including Drones and Additive Manufacturing);
- Sensors and Internet of Things;
- Blockchains and Smart Contracts; or
- Geoengineering and Earth Systems Engineering.

6. NATO has identified nine EDTs considered as a priority[65]:

- Artificial Intelligence;

[59] Jim Thomas, "An Overview of Emerging Disruptive Technologies and Key Issues," *Development* 62, no. 1-4 (October 23, 2019), 5-6. doi:10.1057/s41301-019-00226-z. https://doi.org/10.1057/s41301-019-00226-z.

[60] D. F. Reding and J. Eaton, *Science & Technology Trends 2020-2040 - Exploring the S&T Edge NATO Science & Technology Organization* (Brussels: NATO Science & Technology Organization, 2020), 6.

[61] Ibid.

[62] Ibid.

[63] Ibid.

[64] Thomas, "An Overview of Emerging Disruptive Technologies and Key Issues," 5-6.

[65] "Emerging and Disruptive Technologies."

- Autonomy;
- Quantum;
- Biotechnologies and Human Enhancement;
- Hypersonic Systems;
- Space;
- Novel Material and Manufacturing;
- Energy and Propulsion; and
- Next-Generation Communications Networks.

ANNEX C – PROPOSED MILITARY OCCUPATIONS FOR THE CYBER DOMAIN

1. This annex aims to propose future military occupations for the Canadian Cyber Forces (CCF). Table 1 below divides military occupations between cyber, artificial intelligence, robotics and support. AI and robotics are two potential EDTs the CAF will most likely leverage in the coming years. First, as mentioned in *The DND and CAFAI Strategy*, "AI is a central priority of DND/CAF, and its allies and adversaries." This highlights AI's importance for the CAF. Second, robotics is another potential EDT that could become a priority for the CAF. NATO is currently investigating the use of robotics for military operations with the *Military Uses of Artificial Intelligence, Automation, and Robotics* initiative.[66] The CCF might have to create additional military occupations for further EDTs in the future.

2. Cyber Operator is the only military occupation that is currently available.[67] The proposed military occupation below Cyber Operator could be sub-occupations or distinctive military occupations. Table 1 also proposes military occupation for officers based on being specialized in the conduct of cyber operations, incident management or cloud management. The future development of technologies will dictate the need to establish additional military occupations for cyber officers. Yet, the Cyber Operation Officer should be created sooner rather than later. Interesting to note that the *Evaluation of the Cyber Forces* mentioned:

> 84% of survey respondents believe that DND/CAF would benefit from the creation of a Cyber Officer occupation. The majority of these respondents were at the tactical and operational levels. However, the majority of interviews with senior management disagreed. 66 percent of interviewees thought there was no need for a Cyber Officer position.[68]

3. Unfortunately, the report does not explain the discrepancies between both results. A possible reason is that officers at the tactical and operational levels might be suffering more from the absence of military occupation for officers in their career compared to those at the strategic level.

4. CCF would have similar military occupations for support that can be found in other environmental services. Depending on the CCF size, chaplains and military police could be added.

[66] "Fact Sheet - Military Uses of Artificial Intelligence, Automation, and Robotics (MUAAR)," last modified May, accessed February 14, 2024, https://www.act.nato.int/wp-content/uploads/2023/05/2019_MCDC_MUAAR-2.pdf.

[67] "Cyber Operator."

[68] DG Evaluation ADM(RS), *Evaluation of the Cyber Forces 1258-3-031-AMD(RS)*, 26

Table 1 – Military Occupations in the Canadian Cyber Forces

Cyber Operations	Artificial Intelligence	Robotics	Support
Military Occupations for Non-Commissioned Members			
Cyber Operator	Data Scientist	Electromechanical and Robotics Technician	Human Resources Administrator
Cyber Operator - Red Teamer	Data Analyst		Financial Services Administrator
Cyber Operator - Blue Teamer			Material Management Technician
Digital Forensics and Incident Response Specialist			Intelligence Operator
Industrial Control System Specialist			Military Police
Cloud Security Analyst			
Military Occupations for Officers			
Cyber Operation Officer	AI Engineer Officer	Robotics Engineer Officer	Legal Officer
Cloud Security Officer	Machine Learning Engineer Officer	Mechanical Engineer Officer	Intelligence Officer
Cyber Incident Management Officer	Natural Language Processing Engineer Officer	Design Engineer Officer	Logistic Officer
	Software Engineer Officer		Military Police Officer
	Big Data Engineer Officer		Personnel Selection Officer
			Training Development Officer
			Public Affairs Officer
			Chaplain

Sources: "10 Awesome & High-Paying AI Careers to Pursue in 2024," last modified January 3, accessed February 4, 2024, https://www.springboard.com/blog/data-science/careers-in-ai/.
"The Canadian Armed Forces Browse Careers," , accessed February 8, 2024, https://forces.ca/en/careers.

ANNEX D – F5 FRAMEWORK MODEL

The F5 Model Framework describes the entire spectrum of military activities necessary for armed forces to achieve operational effects.[69] The *Evaluation of the Cyber Forces* recommends identifying proper Accountability, Responsibility and Authority for each role in the F5 model for CAF Cyber Force.[70] The F5 Model Framework for the CCF is described in Table 2 below.

Table 2 – F5 Framework Model

Force Definition	Responsible Organization	Canadian Cyber Force
Force Employment: FE includes "activities and processes related to the command, control, and overall employment of military field forces in operational roles." [71]	Currently, there are three Force Employers in the CAF: • Canadian Joint Operations Command (CJOC) • Canadian Special Operations Forces (CANSOF) • North American Aerospace Defence Command (NORAD)	CJOC, CANSOF and NORAD would be the only FE for the CCF, the same as the other environmental commands.
Force Generation: FG could be resumed as preparing a military force to be deployed. FG starts with recruiting new military personnel.[72] Then, training, assembling, equipping, certifying and maintaining a defined state of readiness for the new military personnel are the following activities required for FG.[73]	Environmental Chief of Staff (ECS): This function is the main effort of the existing environmental commands and their subordinate organizations.[74]	The CCF would be a force generator at the same level as the other ECS[75], such as the Canadian Army, Canadian Royal Air Force and the Royal Canadian Navy. FG is also done by providing communications, intelligence, logistics, medical, and military

[69] "Report on Transformation 2011."
[70] DG Evaluation ADM(RS), *Evaluation of the Cyber Forces 1258-3-031-AMD(RS)*, 30.
[71] "Report on Transformation 2011."
[72] Ibid.
[73] "Report on Transformation 2011," last modified August 8, accessed January 22, 2024, https://www.canada.ca/en/department-national-defence/corporate/reports-publications/report-on-transformation-2011.html#a6-1.
[74] Ibid.
[75] Canadian Forces Experimentation Centre, *Canadian Forces Joint Publication - CFJP 01 Canadian Military Doctrine - B-GJ-005-000/FP-001*, 1-3

		police.[76] Therefore, the CCF will require its communications, intelligence, logistics, medical and military police NCMs and officers to facilitate the FG (see Annex B).
Force Support: FS is a fundamental activity for FG and FE. It assures sustainment for deployed and non-deployed troops, such as logistic support of personnel and infrastructures and movement, control, maintenance and repair of operational equipment and material.[77]	Several organizations involved, but no central oversight.[78]	FS would be necessary for the CCF to FG and FE cyber forces. Delivering effects in the cyber domain requires access to specialized equipment and infrastructures with the latest and most innovative technology. The CCF will require additional workspace with high-security zones to facilitate interoperability with Canadian partners and international allies.[79]
Force Development: FD is about improving military capabilities, driven by policy changes, security environment and lessons learned from past operations.[80] It includes all efforts to identify and gain approval for new military capabilities and to bring those capabilities to a sufficient level of maturity	CAF Chief of Force Development is responsible for Force Development; however, FD is significantly shaped by ECS and other organizations.[82]	CCF would influence the FD to develop cyber domain military capabilities, including developing and integrating EDTs. Currently, the Director General Information Capabilities Force Development (DGICFD) and, more specifically, the Director of Cyber Operations Force Development (DCOFD) are responsible for the

[76] Canadian Forces Experimentation Centre, *Canadian Forces Joint Publication - CFJP 01 Canadian Military Doctrine - B-GJ-005-000/FP-001* (Her Majesty the Queen in Right of Canada, as represented by the Minister of National Defence, 2011), 5-9.

[77] "Report on Transformation 2011."

[78] Ibid.

[79] National Defence, *Department of National Defence and Canadian Armed Forces 2023-24 - Departmental Plan*, 37.

[80] "Report on Transformation 2011."

[82] Ibid.

to be integrated into the normal FS, FE and FG.[81]		development of cyber domain doctrine and expertise.[83] The CCF could establish its centre of excellence. The same idea was proposed by *The DND and CAF AI Strategy* that highlights the necessity of creating a *Defence AI Centre* for the CAF that will serve as a hub of expertise to facilitate the integration of capabilities, develop a common repository of AI models and applications and provide access to common datasets.[84] The CCF Centre of Excellence would develop doctrines, best practices, and expertise and train CAF members about cyber operations, AI or others EDTs.
Force Management: It includes governance, developing policy, human resources, financial control, and mandated programs.[85]	Vice Chief of the Defence Staff.[86]	The CCF will need to create positions within its headquarters such as human resources, and financial control to provide a proper FM (see Annex B).

[81] "Report on Transformation 2011."

[83] "Director General Information Capabilities Force Development (DGICFD)," last modified October 25, accessed February 8, 2024, http://admim-smagi.mil.ca/im_intranet/about/organization/dgicfd.page.

[84] Minister of National Defence, *The Department of National Defence and Canadian Armed Forces Artificial Intelligence Strategy*, 15.

[85] "Report on Transformation 2011."

[86] Ibid.