National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

An Organizational Vision for Cyber Mission Assurance in the RCAF

Major Robyn G. Scholes

JCSP 47

Master of Defence Studies

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

Maîtrise en études de la défense

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

MASTER OF DEFENCE STUDIES – MAÎTRISE EN ÉTUDES DE LA DÉFENSE

AN ORGANIZATIONAL VISION FOR CYBER MISSION ASSURANCE IN THE RCAF

By Major R.G. Scholes

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

Cyber threats pose a real risk to the Royal Canadian Air Force's (RCAF) ability to operate in a cyber-contested environment. Proactive risk management, through the Cyber Mission Assurance (CMA) Program, is necessary to ensure freedom of action, mission effectiveness and safety of aircraft and aerospace ground-based systems. While force development efforts progress on the RCAF CMA Program, this study proposes changes to the organizational structure to enable its steady-state implementation. It does so through the lens of RCAF command and control doctrine and the National Institute for Standards and Technology (NIST) Cyber Security Framework, assessing where cyber risk management capacity and expertise must exist at the tactical and operational level, as well as where authority and responsibility should be held. The theoretical assessment is used to develop analysis criteria for successful CMA-focused organizations, which are then applied to four proof-of-concept organizations: three in the RCAF and one in the Royal Canadian Navy. The results of the case studies provide constraints and lessons learned, informing the final recommendations for organizational structure change. The paper concludes that permanent tactical and operational level organizations for CMA are required for domestic and expeditionary operations. These organizations must be mission-focused with integral cyber and technical system expertise in order to successfully Protect, Detect, Respond and Recover from cyber threats.

CHAPTER 1 - INTRODUCTION

In a dimension of conflict without borders, we all live on the front line.

– Andy Greenberg, *Sandworm*

At 3:30 p.m. on 23 December 2015, the lights blinked out on 230 000 Ukrainians as Russian cyber actors attacked numerous power distribution centres, substations and backup power supplies. For up to 6 hours, ordinary citizens were left without electricity while utility company employees scrambled to manually override the virtually opened circuit breakers: it took months to fully recover.[1] This event marked the first coordinated attack against a civilian power grid, and illustrates that systems well beyond traditional information technology (IT), such as computers, networks and cell phones, are susceptible to cyber attack. It underscores that real world, physical consequences can emerge from actions taking place in cyberspace.

The threat in and through the cyber domain comes from a variety of sources possessing a diverse set of capabilities and intentions that may inflict a wide range of effects. The source of the cyber threat for military forces are principally nation-state actors; however, non-state actors such as criminals, terrorists, hacktivists, hackers and even insiders pose a risk. The actors' intentions, capabilities and opportunities to conduct cyber operations describes the level of threat that they pose, where intention is the most critical of these factors.[2] However, unlike the previously described example, most cyber operations fall short of causing physical destruction, injuries or death (Figure 1.1).[3] As the United States Cyber Command recognizes, "adversaries operate continuously below the threshold of the law of armed conflict (LOAC) to weaken

---

[1] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," (Mar 3, 2016). https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[2] Canada. Department of Defence, JDN 2017-02, *Joint Doctrinal Note on Cyber Operations* (Ottawa: DND Canada, 2017), 3-10 - 3-11.

[3] Chris Horner, "Cyber Operations 101 and Planning Considerations" Lecture, Canadian Forces College, Toronto, ON, 22 February 2021, with permission.

institutions and gain strategic advantages."[4] This means that militaries like the Canadian Armed Forces (CAF) are under constant threat, with effects occurring in either, or both, the cyber and physical domains.

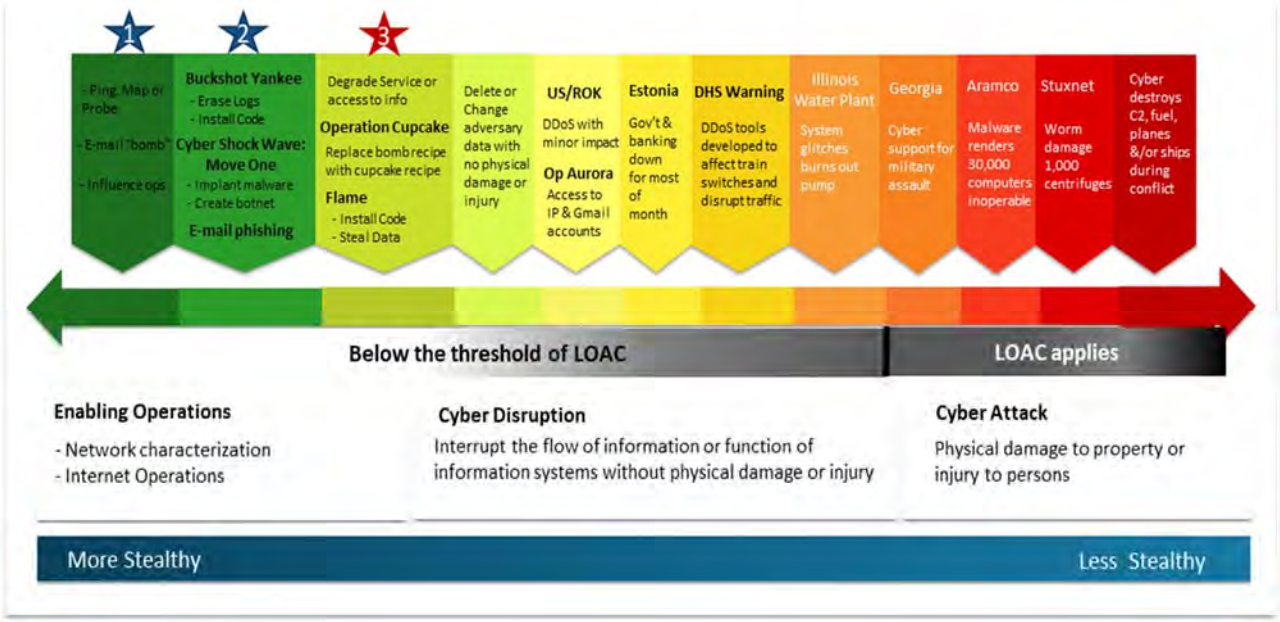

Figure 1.1 – Cyber Operations – Spectrum of Conflict
Source: Horner, *Cyber Operations 101 and Planning Considerations*, slide 8.

Cyber Resiliency & Cyber Mission Assurance

In this environment of persistent and constant threat, the CAF has recognized the exposure of its networks, computer systems, critical infrastructure, vehicles and weapons systems to the broad spectrum of cyber operations. Acknowledging the impossibility to protect or defend against every possible threat, the Pan-Domain Force Employment Concept (PFEC) advocates for comprehensive resilience across all systems, stating that the CAF must remain capable of completing its missions despite degradation or damage to its people, equipment,

[4] United States Cyber Command, *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command* (Fort Meade: US Cyber Command, [2018]), 3.

communication systems, and logistics chain.[5] It goes further to describe what resilience means in practice: "understand[ing] our critical vulnerabilities, reducing them where possible and protecting them where we can."[6] These three broad steps are effectively a deliberate risk management activity, which implies a need to prioritize systems and functions, describe their exposure to cyber threats, mitigate and shield against them, and finally monitor for effectiveness. The conduct of these mission-oriented, risk management activities has been formalized as the Cyber Mission Assurance (CMA) Program.[7]

The goal of the CMA Program is to "preserve CAF freedom of action in order to successfully accomplish all assigned mission sets in any cyber-contested domain."[8] As described in Figure 1.2, CMA focuses exclusively in the friendly (blue) zones of cyberspace, i.e. where the CAF/DND and allies exert control and defensive measures, and is oriented to physical systems, such as infrastructure, equipment, vehicles and weapon systems.[9] It excludes traditional IT systems such as computers, communication systems and enterprise networks, as the extant Network Operations (Net Ops) program encompasses risk management, security, and defence of these systems.

---

[5] Department of National Defence, *Pan-Domain Force Employment Concept* (Ottawa: DND Canada, [2020]), 30.

[6] Ibid., 30.

[7] Canada. Department of National Defence., *Cyber Mission Assurance Program Charter* (Ottawa: Vice Chief of Defence Staff, 2020a), iii.

[8] Ibid., iii.

[9] Chris Horner, "Cyber Operations 101 and Planning Considerations."

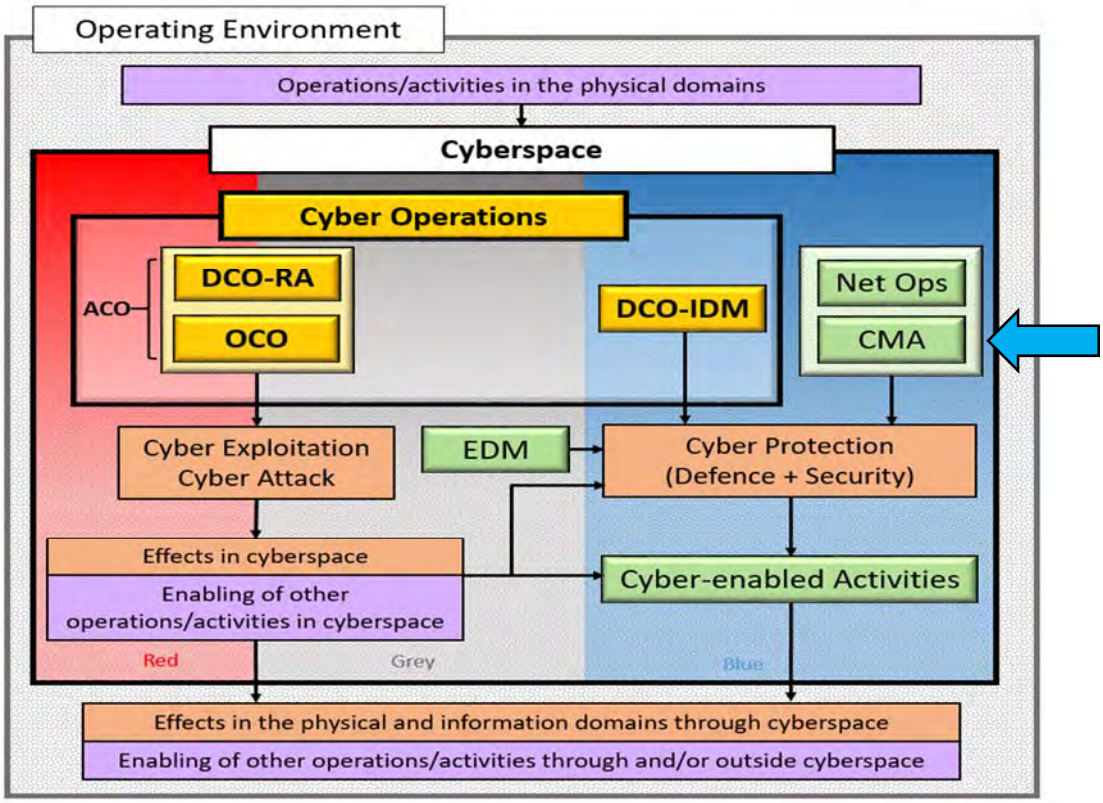

Figure 1.2 – Cyber Operations – Controls and Defensive Measures
Source: Horner, *Cyber Operations 101 and Planning Considerations*, slide 11.

The CMA Program explicitly states that the CAF is institutionally reliant on technology, and that people, processes and technology must all play a role in assuring mission success. This expansion of focus beyond the equipment itself, i.e., the technology, is an acknowledgement by the CAF that it requires the appropriate expertise and human resources, organized in such a manner that enables the force to prepare for and respond to cyber threats deliberately and consistently. The CMA Program provides a description of "what" needs to be done (a 5-step risk management process), but assigns the task tailoring of "who, where, when, and how" to the level 1 organizations, such as the Royal Canadian Air Force (RCAF).[10]

[10] Canada. Department of National Defence, *Cyber Mission Assurance Program Charter*.

The RCAF has been working towards the goal of cyber mission assurance, under various program titles, since 2013. As such, the RCAF CMA Program has progressed from the Conceive Pillar of Force Development into the early stages of Design Pillar. With this evolution, the RCAF Aerospace Warfare Centre (RAWC), Directorate of Aerospace Domain Development (DADD), 1 Canadian Air Division (1 CAD) Headquarters, Director General of Aerospace Equipment Management (DGAEPM), and Defence Research and Development Canada (DRDC) have collaborated on initial implementation steps for the program and have allocated some human resources to carrying out CMA tasks.[11] With this work already underway, and the Design Pillar still in progress, there is a need to identify what a mature and steady-state RCAF CMA Program would look like.

Drawing on the CMA Program charter's statement that people, processes and technology all have a role to play, this paper will focus explicitly on describing an organization that can draw upon and adapt existing processes and technology to provide mission assurance in a contested cyber environment. While some processes will be described, this is in the interest of identifying the roles and responsibilities of people involved in a proposed CMA organization. Technology, while a key contributor to enabling and conducting CMA activities, will not be discussed. Instead, the emphasis of this paper is on people and organizations, as processes and technology are entirely dependent on their creators and their users. The most rigorous processes are useless without understanding and application. Likewise, the most advanced technology is only as good as the humans who employ it. For these reasons, while CMA depends on the

[11] Simon Larocque (DTAES), telephone conversation with author, February 8, 2021.
LCol Janin Blanchet (DADD), email conservation with author, January 20, 2021.
Maj Jonathan Holsworth (DG Cyber), telephone and email conversation with author, February 2, 2021.

successful implementation of processes and technology, people underpin the program's ultimate effectiveness.

This paper will argue that the RCAF requires a permanent organizational structure at the tactical and operational level to effectively command, control and conduct cyber mission assurance. The recommendation for an RCAF CMA Program organizational structure is built through chapters two to five of this paper. In chapter two, CMA is set into the context of cyberspace and describes the activities required to achieve a steady-state implementation of CMA in the RCAF. Chapter three identifies where these activities should be carried out from the doctrinal command and control structures of the RCAF. Leveraging this doctrinal analysis, the fourth chapter compares four nascent organizations against the recommendations of the previous sections. Finally, in chapter five, recommendations and conclusions are drawn for how the RCAF should adapt its organization to facilitate continuous, integrated CMA in daily operations. The orientation of this paper towards people is reinforced by the literature, where much recent work has gone towards establishing a shared understanding of the cyber domain and people's role within it.

Literature Review

In relation to cyber warfighting, several key sources were drawn upon for a better understanding of the domain. Green provides a multidisciplinary assessment of cyber warfare, where the use of force and aggression in cyberspace is systematically addressed from various perspectives. The cyber domain is discussed in relation to its history, technical taxonomy, attribution challenges, international relations, strategy, legal and ethical considerations, providing a foundation for understanding the threats and evolution within this vast domain.[12]

[12] James A. Green, *Cyber Warfare: A Multidisciplinary Analysis*, ed. James A. Green, 1st ed. (Abingdon, Oxon; New York, NY: Routledge, 2015).

This feeds into the discussion of "cyber superiority," which Bryant describes as a necessary and important organizational construct for military planners and strategists. By assessing the extent to which the traditional maritime, land and air domains espouse local or universal superiority, and comparing this to conflicts in the cyber domain, he argues the importance of local superiority in cyberspace.[13] Bryant's concepts are reflected in the CAF's view of the cyber domain, as is evidenced by the division of cyberspace into red (adversary), grey (neutral/uncontrolled) and blue (friendly) zones (Figure 1.2).

Building on the understanding of the cyber domain, LCol (ret'd) Martin provides three groupings of cyber warfare "schools of thought" in academia: Revolutionary Materialism, Liberal Materialism and Conservative. Martin argues that the CAF needs to incorporate a Liberal Materialistic perspective in the development of its cyber strategy, recognizing a balance between technology and humans as the drivers of change to cyber warfare. Importantly, this paradigm argues the need to "control the effects of cyber warfare through the power of social institutions."[14] It implies the necessity to structure and organize the military institution in consideration of the cyber domain, as well as generate norms for activities conducted in and through cyberspace.

The focus on human influence in the cyber domain extends into allied doctrine, where we see the domain divided into five (or six) interrelated layers. Summarized by the CAF Joint Doctrine Note, this includes the persona (and social), cyber persona, logical network, physical network, and geographic layers. The persona and social layer considers the importance of

[13] William D. Bryant, *International Conflict and Cyberspace Superiority : Theory and Practice* (Abingdon, Oxon: Routledge, 2016).

[14] P. E. C. Martin, "Cyber Warfare Schools of Thought: Bridging the Epistemological/Ontological Divide" Masters of Defence Studies Research Paper, Canadian Forces College, 2015).

individuals and groups "interpreting and exploiting the environment" and their responsibility of generating outcomes from the cyber domain.[15]

To enable defensive outcomes in the cyber domain, the National Institute for Standards and Technology (NIST) Cybersecurity Framework offers an approach to comprehensive risk management through "five concurrent and continuous Functions – Identify, Protect, Detect, Respond and Recover."[16] While developed as a standard for cybersecurity management of critical infrastructure across the US, the approach is in use internationally and is well suited to cyber-physical systems.[17] Leveraging the work by NIST, the CAF has adopted the Framework into its cyber doctrine, with the five functions underpinning both Defensive Cyber Operations and Cyber Mission Assurance activities. The Framework has established common terminology within the domain, and provides a robust means to organize the tasks, roles and responsibilities necessary for cyber risk management.

Conclusion

Following the NIST Framework, this paper seeks to explore how the activities of cyber mission assurance inform the organizational structure needed for their execution. It provides a new contribution to the field of cyber risk management by assessing, within the existing command and control doctrine of the RCAF, where capacity and expertise must exist at the tactical and operational level, as well as where authority and responsibility should be held. This work will thus inform the transition from implementation to steady-state of the RCAF CMA Program, and the organizational design change necessary for its success. As an initial step

[15] Canada. Department of Defence, JDN 2017-02, *Joint Doctrinal Note on Cyber Operations* (Ottawa: DND Canada, 2017), 2-4.

[16] National Institute for Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Gaithersburg: US Department of Commerce, [2018]), 3.

[17] Ibid., 1.

towards these recommendations, the next chapter provides an overview of cyberspace, the cyber domain and extant CMA policy and programs for the CAF.

CHAPTER 2 – CYBER MISSION ASSURANCE CONCEPTS

This chapter will provide foundational information and terminology related to the cyber environment and CMA. This is important to provide a common terminology and understanding, building upon the discussed literature, to anchor future chapters' discussions of activities and organizations. First, there is a description of the cyber domain with a definition of cyberspace and its inherent risks and threats. Then, it moves to define CMA, highlighting how it differs from Cyber Operations, and how it relates to the doctrinal operational functions. In the next section, the chapter shifts to CMA Programs at the strategic and operational level, before describing the extent that CMA has been initiated in the RCAF. In the final section, an analysis highlights the RCAF's progress against programmatic objectives, identifying recommendations for activities at the tactical and operational level in order to enable the shift from CMA implementation to CMA integration in day-to-day RCAF operations.

The Cyber Domain

The cyber domain is defined as representing "all factors that influence operations in cyberspace, to include people and infrastructure."[18] Therefore, cyberspace is the medium: an artificial, human made terrain where operations in this domain occur.[19] It extends beyond computers and networks to anything with a processor or circuit that can be manipulated, and is inclusive of the software and data resident within them. Cyberspace is omnipresent in the CAF as it is integrated into all levels of platforms, weapons, systems and networks that are dispersed across the maritime, land, air and space domains. This underscores its importance as "both a vital enabler and a significant vulnerability … [that] is critical to the delivery of many operational

[18] Canada. Department of Defence, JDN 2017-02, *Joint Doctrinal Note on Cyber Operations*, 2-2. A complete description of the cyber domain can be found in chapter 3 of the JDN 2017-02, *Joint Doctrinal Note on Cyber Operations.*

[19] See also Cyberspace definition in Appendix 1 - Glossary

effects."[20] While the cyber domain also represents a domain of opportunity, for the purpose of CMA, it is critical to understand the threats and risks that are present in cyberspace in order to maintain freedom of operation in this medium.

The Defence Terminology Bank (DTB) defines threats in the context of security, as "any potential event or act, deliberate or unintentional, or natural hazard that could result in a compromise."[21] This aligns with the Canadian Centre for Cyber Security's IT Security Guidance (ITSG) definition which states that threats in cyberspace can be accidental or deliberate with the effect of "compromising the confidentiality, integrity or availability of information systems."[22] Accidental threats are considered errors and, while these remain a hazard, they will not be explicitly discussed in this paper. Maintenance, quality management and other extant programs have matured sufficiently to deal with non-deliberate threats from a safety perspective.[23]

As defined, cyberspace threats have effects in the areas of confidentiality, integrity or information availability. Confidentiality refers to cyber intrusions that seek out intelligence, intellectual property, design and prototypes,[24] medical and personal information, academic research, company trade secrets,[25] and extends to data held in weapon systems. Information integrity speaks to both distortion and degradation data, with joint cyber doctrine going further to include system corruption and manipulation.[26] Effects could be considered as disinformation and

---

[20] Ibid., 1-1 - 1-2.

[21] "Defence Terminology Bank" (DTB), DND Canada , http://terminology.mil.ca, entry 695102

[22] Canada. Canadian Centre for Cyber Security, *IT Security Risk Management: A Lifecycle Approach. ITSG-33* (Ottawa: Communications Security Establishment, [2012]), 2.

[23] Quality Management Systems, such as the ISO 9000 family, have been adapted and entrenched in CAF safety and quality cultures. For example, the RCAF uses the AF9000+ program based on this international standard. Additional information can be found at: https://www.iso.org/iso-9001-quality-management.html

[24] Canada. Department of Defence, JDN 2017-02, *Joint Doctrinal Note on Cyber Operations*, 3-13.

[25] Canada. Canadian Centre for Cyber Security, *National Cyber Threat Assessment 2020* (Ottawa: Communications Security Establishment, [2020]), 11.

[26] Canada. Department of Defence, JDN 2017-02, *Joint Doctrinal Note on Cyber Operations*3-13

may have physical impacts, such as sending false messages to an aircraft engine.[27] Information availability addresses denying access, but may also mean data destruction, and often takes the form of ransomware[28] or denial of service attacks.[29] These are not an exhaustive list of cyber threats, but provide context for understanding the breadth of risks in cyberspace.

Technology Categories in Cyberspace

To better understand and address threats and risks in the cyber domain, DND/CAF has sub-divided cyberspace into three broad categories as depicted in Figure 2.1: Information Technology (IT), Operational Technology (OT) and Platform Technology (PT).[30] This division allows for attribution of expertise and responsibility along DND/CAF's existing organizational structure. Each of these areas will be described individually, and an example of a significant cyber event[31] will be used to put deliberate threats in each technology area into context. While this examination of each technology type is useful for a fundamental understanding, it must also be recognized that the categories have an interdependence when systems of systems[32] are considered.

---

[27] Evan Perez, "FBI: Hacker Claimed to have Taken Over Flight's Controls," *Cnn* (May 18, 2015). https://www.cnn.com/2015/05/17/us/fbi-hacker-flight-computer-systems/index.html.

[28] FireEye and Mandiant, *A Global Reset: Cyber Security Predictions 2021* (Milpitas: FireEye Inc,[2020]), 6.

[29] Damien McGuinness, "How a Cyber Attack Transformed Estonia," *BBC News* (Apr 27, 2017). https://www.bbc.com/news/39655415#:~:text=On%2026%20April%202007%20Tallinn,in%20some%20cases%20lasted%20weeks.&text=Such%20attacks%20are%20not%20specific%20to%20tensions%20between%20the%20West%20and%20Russia.

[30] "Defence Terminology Bank" (DTB), DND Canada, http://terminology.mil.ca

[31] A "significant cyber event" has an impact, or potential impact, on military operations. Differentiation among the four levels of cyber events are categorized by the intent and scale of effects. See glossary for the three additional terms: cyber security event, cyber security incident, and cyber attack.

[32] Purdue University defines systems of systems as the concept of large-scale integration of many independent, self-contained systems, which are highly interdependent. For further information, see https://engineering.purdue.edu/Engr/Research/Initiatives/Archive/SoS

Figure 2.1 – RCAF Examples of IT, OT and PT
Source: Canada, Cyber Mission Assurance Overview (1 CAD, Oct 2020), slide 5.

Information Technology (IT) is the classical technology domain composed of computers and networks. In this domain, cyber threats take a multitude of forms and make up near-daily major news stories. The Canadian Centre for Cyber Security's 2020 National Cyber Threat Assessment focuses on cybercrime, such as online fraud and "attempts to steal personal, financial and corporate information" as the most likely threat to Canadians.[33] Foreign influence, commercial espionage and intellectual property theft are identified as other persistent threats. It is best illustrated by the Ryuk ransomware which, working in tandem with two other pieces of malware, affected banking, municipal governments and health institutions internationally.[34] In one case of the Ryuk ransomware, United Health Services completely shut down its digital

[33] Canada. Canadian Centre for Cyber Security, *National Cyber Threat Assessment 2020*, 5.
[34] Canada, *Alert AL19-202: Ryuk Ransomware Campaign* (Ottawa: Canadian Centre for Cyber Security,[2019]).

health networks in the US, forcing some hospitals to return to paper and re-route patients from care.[35] As the CAF maintains a vast IT infrastructure, it too is susceptible to these threats. It is therefore no surprise that the CAF's IT systems are an identified target for state and non-state actors operating in cyberspace.

Operational Technology (OT) are those systems that monitor and control facilities, the energy sector, building infrastructure, etc. A prime example of the threat to OT is the 2010 Stuxnet worm which allegedly targeted Iranian nuclear enriching facilities by hijacking the industrial system that controlled centrifuge rotation speed.[36] However, the virus spread beyond its original intended targets and could have been used to take control of power plants, communication systems or even national power grids.[37] This area of cyberspace is a concern as the CAF has a significant holding of infrastructure, be it office buildings, steam plants, or aircraft hangars. Additionally, some of these facilities are dual-use, such as shared aerodromes and air traffic systems, implying that threats to military OT also represent a broader risk to the Canadian public.[38]

Platform Technology (PT) relates to weapon system platforms, vehicles (air, land, sea and space), and other defence systems. Numerous examples abound, ranging from the F-35 Joint Strike Fighter's vulnerabilities in its Autonomic Logistics Information System,[39] to credential

---

[35] Lily Hay Newman, "A Ransomware Attack has Struck a Major US Hospital Chain," *Wired* (Sep 20, 2020a). https://www.wired.com/story/universal-health-services-ransomware-attack/.

[36] Albright, Brannan and Walrond, *Did Stuxnet Take Out 1000 Centrifuges at the Natanz Enrichment Plant* (Washington: Institution for Science and International Security,[2010]). https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf.

[37] Nicolas Falliere, Liam O. Murchu and Eric Chien, *W32.Stuxnet Dossier* (Cupertino: Symantec,[2010]).

[38] "Airport Divestiture Status Report," Government of Canada, last modified Jan 12, accessed Apr 13, 2021, https://web.archive.org/web/20150930005553/http://www.tc.gc.ca/eng/programs/airports-status-menu-441.htm.

[39] Grant Turnbull, "Back Door for Hackers? F-35 Cyber Weaknesses in the Spotlight," *Global Defence Technology*, no. 97 (Mar, 2019). https://defence.nridigital.com/global_defence_technology_mar19/back_door_for_hackers_f-35_cyber_weaknesses_in_the_spotlight.

stealing in the US Predator and Reaper Drone fleets.[40] In another example relate to PT, the Israeli Defence Force's Operation Orchard leveraged airborne cyber techniques to "take control of the Syrian air defence network … subsequently activating a 'kill switch.'"[41] This enabled the Israeli Air Force to perform airstrikes on a Syrian nuclear reactor "without alerting the Syrians to their location or triggering any air defence capabilities."[42] It must be recognized that this integrated cyber and physical attack took place over 13 years ago, and that allied and adversary capacities have continued to evolve. Again, the example underscores the critical cyber threats that PT owned, operated and managed by the CAF are exposed to throughout their life cycle.

While examples were provided of threats within each technology type, their interrelation and dependencies must also be considered. This can be shown by looking at the example of an air traffic control tower at an RCAF Wing. IT is found in the Defence Wide Area Network (DWAN) computers which are used for email, shift scheduling, and holding records of controller currencies. OT is present in the electrical distribution, heating and cooling systems that ensure functionality of the DWAN computers (IT), as well as radios and communication systems (PT). Therefore, while each technology is considered separate, their function as a system of systems[43] is important when considering that overall mission accomplishment requires multiple technologies, or capabilities, functioning together.

Cyber Mission Assurance (CMA)

CMA speaks to the ability to accomplish a mission in a cyber-contested environment. As it is a relatively new and emergent domain within the CAF/DND enterprise, it is necessary to

---

[40] Noah Schactman, "Exclusive: Computer Virus Hits U.S. Drone Fleet," *Wired* (Oct 7, 2011). https://www.wired.com/2011/10/virus-hits-drone-fleet/.

[41] Martin, "Cyber Warfare Schools of Thought: Bridging the Epistemological/Ontological Divide," 49.

[42] Ibid., 49.

[43] A system of systems describes large-scale integration of many independent, self-contained systems. See https://engineering.purdue.edu/Engr/Research/Initiatives/Archive/SoS

provide a common foundation and language for all stakeholders. The following interrelated definitions have been promulgated through the DTB, and will be used throughout this paper. Additional key concepts and definitions can be found in Appendix 1 – Glossary.

- **Mission Assurance.**[44] The security and resilience of systems and capabilities for mission success.
- **Resilience**.[45] The ability to recover from adverse effects.
- **Cyberspace Resilience**.[46] The overall technical and procedural ability of systems, organizations and operations to withstand cyber incidents and, where harm is caused, recover from them with no or acceptable impact on mission assurance or continuity.
- **Cyber Mission Assurance**.[47] A sub-set of Mission Assurance that focuses on the ability of an organization, service, infrastructure, platform, weapon system, and/or equipment to operate and accomplish their mission in any cyber-contested domain.

From these definitions, several core constructs can be extracted. First, is the critical concept that mission assurance, and in turn, CMA is centred on the ability to successfully accomplish a mission. Consequently, activities in this realm must focus on outcomes. Secondly, when linked with the concept of cyberspace resiliency, it orients CMA to the consideration of impacts on said outcome, where the results must be acceptable: implying an assessment and acceptance of risk. Therefore, CMA is, at its heart, a risk management process that enables the accomplishment of a mission. Thirdly, while cyberspace is considered its own domain by

[44] DTB 695221
[45] DTB 695250
[46] DTB 695811
[47] DTB 695102

DND/CAF and NATO, CMA applies to the existing land, sea, air and space domains.[48] Similarly, CMA is equally applicable across the five joint doctrinal operational functions: command, sense, act, shield and sustain.[49]

Operational Functions

At its origin, cyber was considered exclusively under the shield function, and centred on IT. This perspective has evolved in CMA conceptualization to a recognition that "cyber capabilities observed today are capable of delivering cyber-physical effects,"[50] and that OT and PT possess "critical dependencies on cyber technology to deliver effects in the air, space, [maritime and land] domains."[51] However, legacy doctrine, such as the 2006 CAF joint force protection doctrine and 2011 RCAF shield doctrine, have not kept up with this changing understanding of CMA. Nevertheless, RCAF operational directives such as the 2019 *RCAF Vectors* and Campaign Plan clearly state that "it is essential to integrate cyberspace operations capabilities into all aspects of RCAF operations."[52] These RCAF strategic guidance documents go further to state that a "passive defensive cyber posture is not sufficient,"[53] and affirm that active CMA is required. The deduction from these two assertions is that CMA risk management applies to all capabilities, and as the operational functions are used to develop and employ capabilities,[54] CMA risk management applies to all RCAF functions.

---

[48] "NATO's Role in Cyberspace," NATO, last modified Feb 12, accessed Apr 13, 2021, https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html. Canada. Department of Defence, JDN 2017-02, *Joint Doctrinal Note on Cyber Operations*, 4-7.

[49] Canada. Department of National Defence, *CFJP 3.0 Operations. B-GJ-005-300/FP-001* (Ottawa: DND Canada,[2011])., 1-5.

[50] Canada. Royal Canadian Air Force, *RCAF Concept Proposal: RCAF Cyber Mission Assurance V2.4* (Trenton: DND Canada,[2018])., 1.

[51] Ibid.

[52] Canada. Royal Canadian Air Force, *RCAF Campaign Plan* (Ottawa: DND Canada,[2019]).

[53] Ibid., 45.

[54] Canada. Department of National Defence, B-A-400-000/FP-001, *Royal Canadian Air Force Doctrine* (Ottawa: DND Canada, 2015)., 4-1.

CMA versus Cyber Operations

CMA and Cyber Operations are differentiated by the fact that CMA is a risk management activity that occurs in all domains, while Cyber Operations are operations conducted in or through the cyber domain.[55] Cyber Operations are broken into three types: Offensive, Defensive, and Support.[56] Offensive Cyber Operations are clearly understood as separate from CMA due to their offensive nature, and Support Cyber Operations are enablers. However, Defensive Operations overlap and integrate with CMA. Defensive Cyber Operations (DCO) "detect, defeat and/or mitigate offensive and exploitive actions" and are inclusive of internal defence measures (DCO-IDM) and responsive actions (DCO-RA). DCO activities are mission-focused, prioritized and threat-specific, and require an understanding of vulnerabilities as they pertain to adversarial capability and intent.[57] CMA, as with its IT counterpart of network operations, is largely threat agnostic. In short, DCO should be thought of as complementary to CMA, and supports its conduct. DCO may uncover new threats that require risk management, and a CMA risk management plan may implement DCO activities as part of a mitigation plan. However, CMA may also include risk mitigation activities, here the difference being whether they are executed in cyberspace (DCO) or on the platform (CMA).

DCO and CMA tasks can be broadly mapped to the NIST Cybersecurity Framework.[58] The Identify function is relevant to both DCO and CMA as it provides the institutional guidance for people, processes and technology under each program. Protect as a CMA activity speaks to

[55] Effects "in" cyberspace refer to those effects that both occur and manifest in cyberspace, i.e. denial of access to networks or systems, corruption or manipulation that destroys or degrades a network, or espionage/theft of information. Effects "through" cyberspace have an intended effect in another domain, such as the example of STUXNET or hijacking of the Syrian Air Defence network.

[56] See the glossary for description of each of these terms and Ch.4 of JDN 2017-02.

[57] Canada. Department of Defence, JDN 2017-02, *Joint Doctrinal Note on Cyber Operations*, 4-7.

[58] National Institute of Standards in Technology, "The Five Functions," US Government, last modified Aug 10, 2018 https://www.nist.gov/cyberframework/online-learning/five-functions.

the implementation of safeguards and technical solutions to cyber threats, either preventively or reactively. CMA protection measures are differentiated from DCO as they are implemented on the platform, vice in cyberspace. Similarly, Detect is another key point of overlap for CMA and DCO, as detection activities are occurring in the cyber (DCO) and all other domains (CMA), and this phase initiates a response to a detected threat. This assessment of Protect and Detect stresses that there is little distinction between the CMA and DCO activities, and given the connectivity of most military PT, makes differentiating between CMA and DCO inconsequential for these two functions.

During the Respond function, CMA identifies the need to conduct risk management for a new vulnerability or threat; and, DCO activities may be occurring in parallel in cyberspace to defeat, mitigate and/or exploit the threat. In the final function of Recover, the risks identified are addressed (on platform - CMA, in cyberspace - DCO) or simply accepted (CMA) allowing operations to resume. As this assessment of CMA and DCO in the context of the NIST Framework shows, there is substantial overlap and similarities in the activities required, and comparable competencies, tools and expertise are required. Therefore, efficiencies may be gained through combining some CMA and DCO activities for PT.

Cyber Mission Assurance Programs

The Cyber Mission Assurance programs described in this section link directly to the Identify function from the NIST Framework. They describe the policies, processes, and organizational responsibilities that enable the conduct of continuous cyber risk management in the CAF.

Level 0 – Cyber Mission Assurance Program

The CMA Program, under functional authority of the Vice Chief of Defence Staff (VCDS), is the over-arching framework for comprehensive cyber resilience in DND and the CAF. The CMA Program exists as a governance and oversight mechanism to centralize and align all activities across the institution through guidance to the Level 1 (L1) advisors and commanders. Similarly, it ensures coherence with Government of Canada (GC) departments and agencies, drawing on their insight and experience as well as that from allies, industry and academia. The CMA Program Charter and the Functional Planning Guidance for 2021-22 were recently released by the VCDS in Sep 2020, and form the most recent policy guidance in this domain.[59]

As defined above, CMA is a risk management activity. Through this lens, the CMA Program "seeks to enhance a cyberspace resilience culture by better understanding our critical vulnerabilities, reducing them where possible and protecting them where we can."[60] This is accomplished by identifying, assessing and mitigating cyber-associated risks through the following risk management framework:

[59] Canada. Department of National Defence., *Cyber Mission Assurance Program Charter*
Canada. Department of National Defence., *Cyber Mission Assurance Program: Functional Planning Guidance 2021-22* (Ottawa: Vice Chief of Defence Staff, 2020b).

[60] Canada. Department of National Defence., *Cyber Mission Assurance Program Charter*, 4.

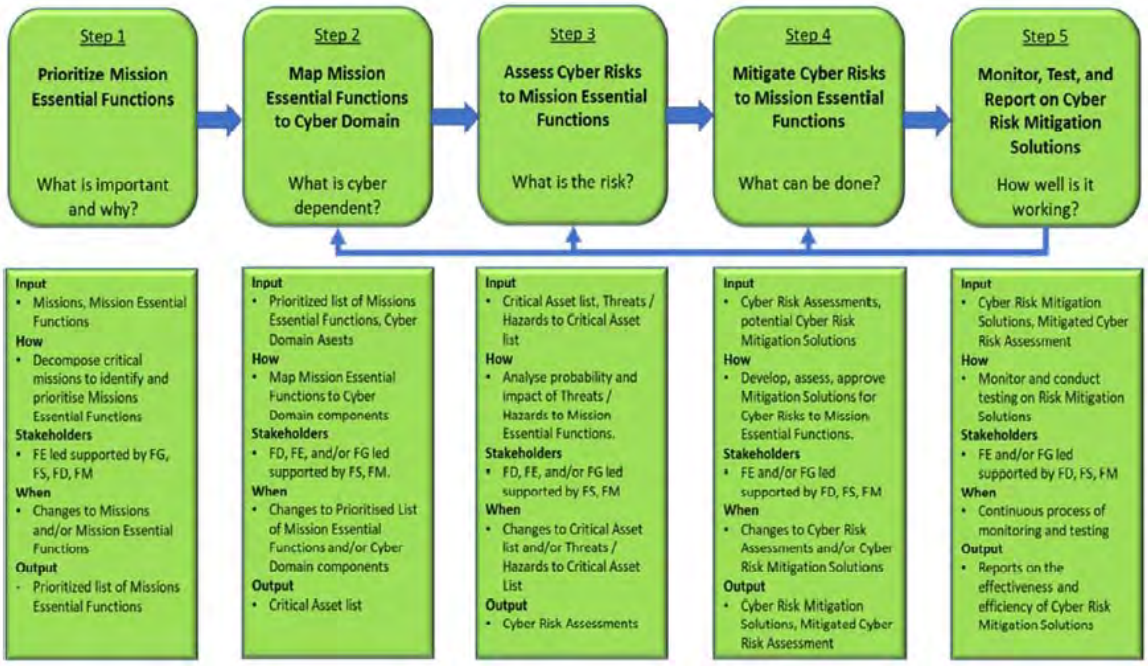

Figure 2.2 – Cyber Mission Assurance Risk Management Process
Source: Canada, *Cyber Mission Assurance Program Charter*, 8.

The core concept from the Figure 2.2 risk management framework is that risks are assessed based on a mission effect. To state this in other terms: a cyber threat must be mapped to an effect on a mission in order to determine a need to mitigate, or accept without mitigation, the risk. When a commander accepts the risk, and the mitigation is implemented, it can be considered that the initiation phase is complete (steps 1-4). The final step (step 5) is effectively in-service monitoring. Its objective is to determine when, or if, any of the initial risk management assumptions are invalidated, thereby requiring the risk management process to be iterated.

Level 1 – RCAF Cyber Mission Assurance

As an L1, the RCAF has a requirement to follow the CMA risk management framework, and adhere to the overarching policy guidelines for the CAF. Noting that the CMA Program and RCAF CMA Program were developed over the same timeframe and with close collaboration, program documentation works hand-in-hand. As is expected, the RCAF guidance narrows the

program scope considerably. While the highest operational level guidance document for the RCAF, *RCAF Vectors*, states that the program is inclusive of RCAF IT, OT and PT,[61] there is a recognition that "most RCAF mission critical cyberspace is built on non-traditional IT (OT & PT)"[62] and that these have "real-time and near-real time dependencies in the physical world that could have immediate impact on operations in the air and space domain."[63] Therefore, aligning with the L0 CMA Program, the emphasis is on risk management directly linked to negative effects on freedom of movement, or mission accomplishment, within the constraints of the RCAF's domains of air and space.

The RCAF CMA Concept Proposal highlights use of existing programs and processes to minimize overhead, and facilitate compliance. Key constructs include leveraging existing 1st, 2nd, and 3rd line maintenance support structures, integrating risk management into the current airworthiness and flights safety culture,[64] maximizing use of the operational risk assessment processes (applicable to PT) and the Security Authorization and Assessment (SA&S) processes (applicable to IT). Finally, it highlights the need to incorporate cyber planning into CAOC

[61] Canada. Director General Air Readiness, *RCAF Vectors* (Ottawa: DND Canada,[2019]), 32-33.
[62] Canada. Royal Canadian Air Force, *RCAF Concept Proposal: RCAF Cyber Mission Assurance V2.4*, 1.
[63] Ibid., 3.
[64] The RCAF culture of airworthiness, risk management and Flight Safety was borne out of a history of injury, death and loss of aircraft. These lessons, while learned in blood, took decades of incremental change and increasingly formalized policies, programs and education to reach their status. In particular, the five fundamental principles of Flight Safety are a defining feature of today's air force operations at home and abroad. For further reading on this evolution, costly mistakes, and today's Flight Safety Program see:
Erik Rozema-Seaton, "BOXTOP 22: The Cost of Focusing on an Operational Culture," *The Royal Canadian Air Force Journal* 8, no. 4 (Fall, 2019), 7-23. http://publications.gc.ca/collections/collection_2019/mdn-dnd/D12-16-8-4-eng.pdf;
"Flight Safety - Royal Canadian Air Force," DND Canada, last modified Oct 11, accessed Apr 13, 2021, http://www.rcaf-arc.forces.gc.ca/en/flight-safety/index.page;
Randall Wakelam, "The Air Force and Flight Safety: A Culture of Tolerated Disobedience," in *The Insubordinate and the Noncompliant: Case Studies of Canadian Mutiny and Disobedience, 1920 to Present*, ed. Howard G. Coombs (Kingston: The Dundurn Group and Canadian Defence Academy Press, 2007), 345-369.

operational level planning.[65] A key consideration behind the proposal is the necessity to develop knowledge in the cyber domain at all levels of the RCAF.

Given the nascence of the CMA program, efforts in the RCAF have been focused primarily on two key areas: conducting a Cyber Key Terrain Analysis (CKTA) and 3rd level materiel support activities. The CKTA prioritizes critical systems by analysis of the RCAF's functions/mission sets against the probability and severity of cyber threats; it is effectively the conduct of the CMA Program's steps 1-3, and one aspect of the NIST Framework's Identify function. The CKTA was initiated in 2015[66] and tasked to 1 Canadian Air Division (1 CAD) by Fragmentary Order (FragO) to the RCAF Campaign Plan.[67] In October 2020, 1 CAD Commander concurred with his staff's recommendation in the draft CMA Roadmap which documents final revision and publishing of CKTA 1.0 this fiscal year, and an ongoing update cycle directed by a 1 CAD Order (CADO).[68] An additional FragO is forthcoming in 2021.[69]

The Director General of Aerospace Equipment Program Management (DGAEPM), under the Assistant Deputy Minister for Materiel (ADM MAT), is tasked with 3rd line materiel support activities from acquisition through to disposal. Recognizing DGAEPM's inherent responsibility and scope for PT as the Technical Airworthiness Authority (TAA), DGAEPM is assigned Security Authority for PT which is further delegated internally to the Directorate of Technical

---

[65] Ibid., 4-6.

[66] Canada. 1 Canadian Air Division, *1 CAD Cyber Functional Integration Team (FIT) - Comd's Updated Guidance* (Winnipeg: DND Canada,[2015]), 4.
NOTE: CKTA was initiated in limited scope at 22 Wing under the original FIT Comd Guidance. The Updated Guidance transferred the responsibility to 1 CAD and grew the scope to all RCAF operations.

[67] Canada. Director of Air Domain Development, *Fragmentary Order (Frag O) 2018-011 to Campaign Plan - RCAF Cyber Mission Assurance Initiating Directive* (Ottawa: DND Canada,[2018]), 15.

[68] Canada. 1 Canadian Air Division, *1 CAD / CANR / JFACC Cyber Mission Assurance (CMA) Overview and Brief* (Winnipeg: DND Canada,[2020]), slides 14-15. Formal approval will be given through the next 1 CAD Campaign Plan (not yet released) which will incorporate the CMA Roadmap.

[69] Maj Kim Kieres (1 CAD), email discussion with author, 1 April 2021.

Airworthiness and Engineering Support (DTAES).[70] Similarly, an assignment as the Security Authority for OT resides within ADM Infrastructure and Environment (ADM IE), and IT remains under ADM Information Management (ADM IM). Applicable CMA processes for DGAEPM have been developed, and implementation is growing in maturity in with specialist support from DTAES to the fleets' Weapon Systems Managers (WSMs). The RCAF's responsibility for all aspects of mission assurance related to RCAF PT, supported by DGAEPM's dedicated Platform Protection Program, form the heart of the RCAF CMA program.

DGAEPM and CMA Processes

As a key pillar in DGAEPM's Platform Protection Program, Defence Research and Development Canada (DRDC) has adapted and combined key risk management processes relevant to cyber security, airworthiness and airborne systems, mission dependency modeling and systems engineering in order to develop a CAF-specific framework related to military system mission assurance.[71] The Risk-based Cyber Mission Assurance Process (RCMAP) is "a series of activities on the cyber risk management of military platforms and systems throughout their whole life cycle in order to achieve cyber mission assurance."[72] Aligning with the CMA Program, the RCMAP is concerned with assessing a mission impact based on its associated functions and the technological assets (systems) that fulfill those functions.

---

[70] Andre Pelchat and Luc Beaudoin, ""Security Authority" Recognition between DIM SECUR and DTAES. RDIMS# 2018892" DND Canada, Ottawa, 2020).

[71] A complete list of the applicable references is found in the DRDC RCMAP source documents, but three core processes make up the backbone: ITSG-33, NIST Cybersecurity Framework and DO-326A Cyber Security and Safety for Aircraft and Aircraft Systems.

[72] F. Rheaume and F. Painchaud, *Risk-Based Cyber Mission Assurance Process: Mission Criticality Analysis and Asset Valuation. DRDC-RDDC-2018-R0000* (Valcartier: Defence Research and Development Canada,[2018c]), i.

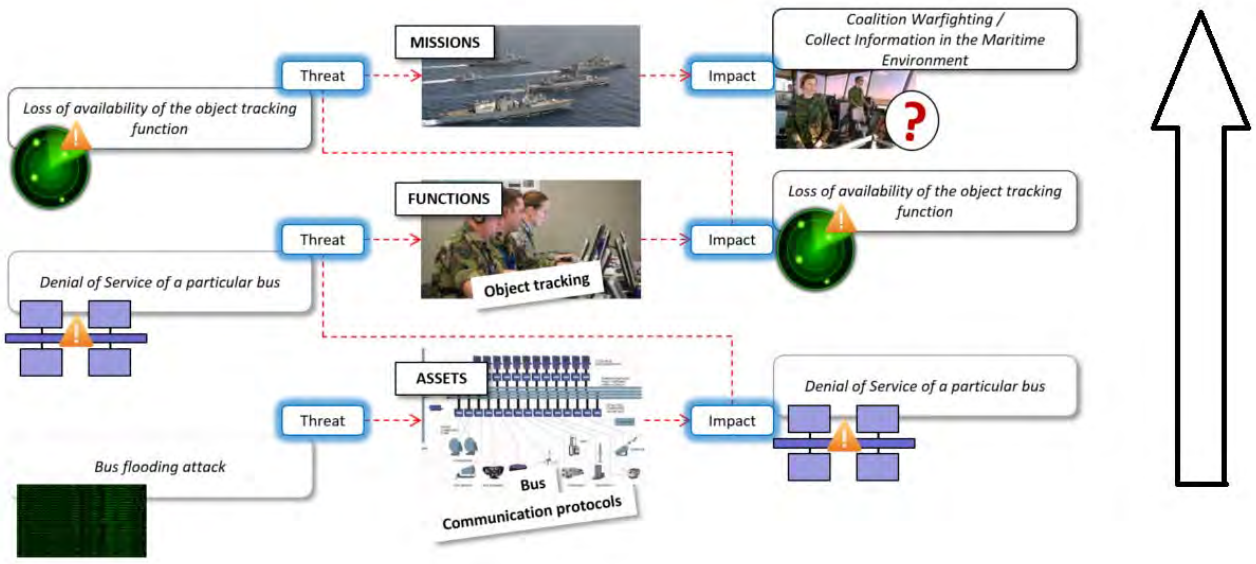

Figure 2.3 – Sample Case of the Risk-based Mission Assurance Process (RCMAP)
Source: DRDC, *Risk-based Mission Assurance Process: Example-driven Overview*, slide 15.

The RCMAP is comprised of three main activities: mission criticality analysis and asset valuation (MCAAV), risk assessment, and security development. These align to different phases of ADM MAT's Material Acquisition and Support (MA&S) process and the DND Project Approval Directive (PAD). Similarly, they tie to the NIST Cybersecurity Framework's functions: Identify, Protect, Detect, Respond and Recover. MCAAV and risk assessment activities are an Identify function. Security development relates to Protect, and may also facilitate Detection. Activities from the Respond and Recover functions are not specifically addressed by the RCMAP model.[73]

[73] F. Rheaume and F. Painchaud, *Risk-Based Cyber Mission Assurance Process (RCMAP): Example-Driven Overview* (Valcartier: Defence Research and Development Canada,[2018a]).

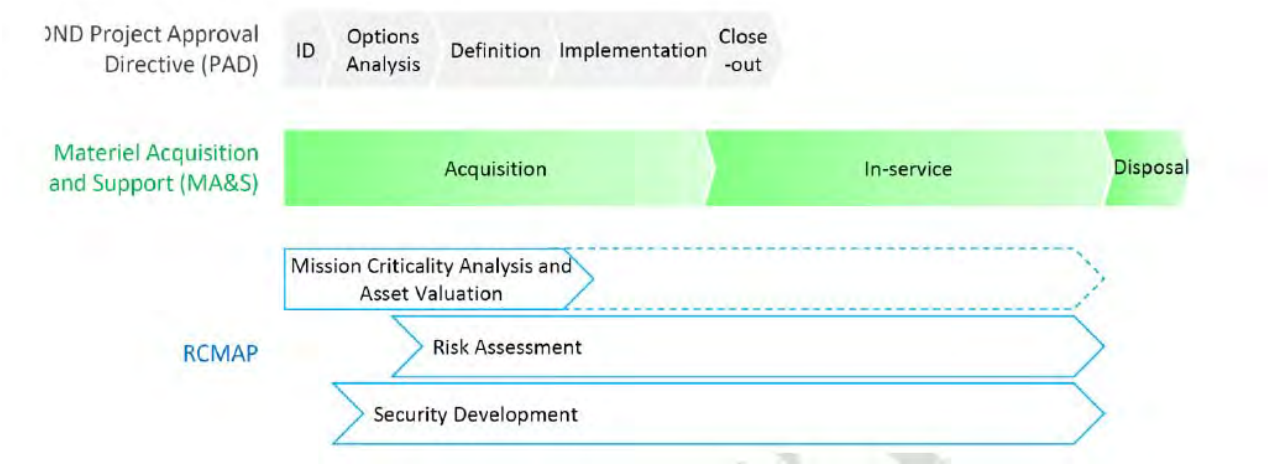

Figure 2.4 – Activities of the RCMAP in the PAD and MA&S Phases
Source: DRDC, *Risk-based Mission Assurance Process: Mission Criticality Analysis and Asset Valuation*, 8.

As evidenced by Figure 2.4 and the RCMAP reports, the activities focus primarily on acquisition and materiel support by ADM MAT organizations. In the in-service phase the Risk Assessment and Security Development phases are identified to require re-initiation when "assets are modified and new threats arise."[74] Related to aeronautical system modification, the release of the Technical Airworthiness Authority Advisory 2019-03[75] describes the need to assess cyber vulnerabilities for regulatory compliance. This is clearly laid out and support from DTAES is available for these assessments. Other than modifications, iterations of the in-service RCMAP activities would be triggered by a cyber incident, or if intelligence or vulnerability scanning/penetration testing identified that a new threat needs to be addressed. For in-service, DTAES envisages this occurring as an update to the MCAAV. However, while the activities and theory of RCMAP are well documented for these cases, its use in practice has been limited to date. The first full application of RCMAP from start-to-finish is underway for the Griffon Life

[74] F. Rheaume and F. Painchaud, *Risk-Based Cyber Mission Assurance Process (RCMAP): Risk Assessment. DRDC-RDDC-2018-R0002* (Valcartier: Defence Research and Development Canada,[2018b]), 4-5.
[75] DTAES Canada, *Technical Airworthiness Authority Advisory 2019-03* (Ottawa: DND Canada,[2019]).

Extension project, and refinement of the process is occurring in lock step with this practical implementation.[76] By extension, materiel support to CMA activities across the Protect, Detect, Respond and Recover functions is immature.

Gaps at Steady-state

RCAF efforts to date have focused on the initiation of the CMA program. With the first iteration of the CKTA soon to be published, and 3rd line materiel support processes in their first iteration, program implementation is underway. Therefore, the next area of focus should be to understand what core activities will need to be accomplished to transition to steady-state and then to conduct routine in-service activities. Aligning to the CAF CMA program's distribution across existing organizational responsibilities, gaps to achieve and operate at steady-state will be assessed at the tactical and operational level. The tactical level is inclusive of RCAF Wings, Squadrons and DGAEPM materiel support, while the operational level assessment focuses on 1 CAD headquarters.

[76] Simon Larocque (DTAES contractor), telephone conversation with author, 8 February 2021.

Operational Level

To transition to steady-state, the CKTA will require iterative updates as new capabilities are removed, added or modified, and as the threat environment changes. This has been captured in the CMA Roadmap, and will be incorporated into the next iteration of the 1 CAD Campaign Plan. CKTA activities have made up a significant portion of 1 CAD CMA efforts to date, and are nearing completion of the first run-through. While personnel experience and competency in the cyber realm are a necessity to continue these efforts, CKTA is not identified as a gap to achieve and operate in steady-state.

Operational level involvement with CMA will principally focus on the Identify, Respond and Recover functions, following existing operational risk management process.[77] Leveraging this construct, typically a threat is **detected** at a tactical level and assessed by a subject-matter expert, typically the platform's Technical Authority (TA) in DGAEPM, before the risk is reported to the operational level. This risk assessment is the **response** to the threat, and is prepared with support by the related Operational Authority (OA) in 1 CAD, who then supports and/or accepts the risk as the Operational Command Risk Acceptance Authority (OCRAA) enabling **recovery**, and continued operations. Risk mitigation activities[78] as agreed upon by the TA, OA and OCRAA may be implemented in parallel to the Response or Recovery: these are largely thought of as part of the Protect function. The use of this process for CMA requires supporting documentation, practical exercise and a build-up of expertise in TA and OA organizations. This should be a core focus of the operational level, noting the implication to 3rd line/DGAEPM support for risk management and iterations of **protection**, to enable successful

[77] Canada. Royal Canadian Air Force, *RCAF Concept Proposal: RCAF Cyber Mission Assurance V2.4*, 5.

[78] Risk mitigation may be inclusive of both CMA and DCO activities, see "CMA versus Cyber Operations" in this chapter.

transition and execution in steady-state. These activities form part of the Identify function, as they establish processes and responsibilities for the institution.[79]

Cyber operational level planning considerations were identified as a necessity for force employers in the CMA initiating directive, which implies a responsibility for the Joint Forces Air Component Commander (JFACC) in 1 CAD. A cyber annex was incorporated as an output to the Operational Planning Process, with a focus on opportunities for cyber operations.[80] While the threat level may change while on operations, CMA should be thought of as a routine activity that is integrated into the day-to-day. Therefore, much like Flight Safety or airworthiness, considerations for CMA will be equally important at home and abroad. In general, if this mindset is achieved with CMA, an increased level of vigilance documented by operational level planners is sufficient for PT. This implies two things: a core of subject matter expert(s) must reside in 1 CAD for planning considerations relevant to RCAF CMA. Second, and more importantly, a CMA-aware and capable culture must exist at both the operational and tactical level in order to Detect, Respond and Recover from cyber incidents. Both of these activities fall into the Identify function, forming the backbone of the people and processes in the CMA program.

Tactical Level

At the Wings and Squadrons (1st and 2nd line), with few exceptions,[81] CMA is presently not integrated into daily operations. Given that implementation activities have been focused on program development and high-level risk management activities, principally the Identify and Protect functions, it is unsurprising that there is minimal visibility and implementation in tactical level units. Given that this is new terrain, the core focus here will be to: understand and

---

[79] "The Five Functions"

[80] Canada. Director of Air Domain Development, *Fragmentary Order (Frag O) 2018-011 to Campaign Plan - RCAF Cyber Mission Assurance Initiating Directive*.

[81] Both 14 Wing and 22 Wing have stood up a Mission Defence Team to support CMA. See Chapter 4.

document accountability, roles and responsibilities, and to identify the requirements for training and competency development in the relevant roles.

In order to assess the role and associated training/competency required at the tactical level, the phases of the CAF CMA Program can be used. Wings and Squadrons activities are limited to phase 5 of the CAF CMA Program: monitor, test and report. This ties specifically to the Detect function and may have a limited role in the follow-on stages of Respond and Recover. The ability to **detect** implies that there are trained personnel responsible to recognize that a cyber incident has occurred and a reporting chain (process and personnel) to initiate the risk management Response and Recovery actions. Given system familiarity and experience, operators and maintainers of PT are expected to be the best suited to carry out this activity. Therefore, aircrew, air maintenance branch and communications and electronics branch personnel are all expected to have responsibilities and roles related to **detection**. This underlines the need for occupational specific training for these branches of technicians, engineers and operators, which begins at the outset of occupational training through to specialist qualifications. A training needs analysis for this purpose is required, and would need to incorporate gap training for personnel who are in operational units and wings. Creating a foundation of cyber understanding at the tactical level is an enabler to more detailed knowledge and expertise for those employed in materiel support and operational level positions. Following training, the challenge will be to emphasize the CMA-awareness and build a cyber capable culture, as mentioned in the operational level assessment.[82]

At 3rd line, materiel support in DGAEPM has already been discussed at length. The responsibilities of TAs, both in the air maintenance and communications and electronics

[82] Canada. Royal Canadian Air Force, *RCAF Concept Proposal: RCAF Cyber Mission Assurance V2.4*, 4.

branches, for air and ground systems respectively, have already been identified and accepted within DGAEPM.[83] The next stage is for cyber expertise to be integrated in these key roles, in addition to extant DTAES support, in order to enable risk management activities. A Training Needs Analysis has already been conducted, so this area is already advancing towards implementation.[84] It is therefore not assessed as a core focus for transition and execution at steady-state.

Common: Operational and Tactical Level

Achievement of a CMA-aware and capable culture is tied to force generation and readiness. The requirement for operational and tactical level training and competency development has been described to enable the transition to steady-state CMA operations. The next step is establishment of standards and a verification process to ensure that the trained cyber capabilities can be executed in real-world situations. Standards and evaluations are a well-understood concept in the RCAF, with Standards and Evaluations Teams (SET) incorporated at the fleet and operational level to ensure operator and technician currency and capabilities, particularly for those capacities that are not normally required during peacetime operations.[85] To ensure force readiness in a cyber-contested environment, the activities of Detect, Respond and Recover need to be exercised and confirmed to meet an established standard. To a smaller extent, verification of the Protect function will also be covered by this activity.

---

[83] Canada. Department of National Defence, *Technical Airworthiness Manual (TAM). C-05-005-001/AG-001* (Ottawa: DND Canada,[2019b]).

[84] Maj Kim Kieres (1 CAD), telephone conversation with author, 27 October 2020.

[85] Evaluated exercises, particularly those conducted by the NORAD evaluation teams within CANR and NORAD HQ, assess the readiness to respond to events such as an intercept of a foreign military aircraft, an unidentified civilian aircraft, or posturing at a forward deployed location as a deterrence measure. For example, Exercise AMALGAM DART 2021. "NORAD Conducts Arctic Air Defense Exercise AMALGAM DART," NORAD, last modified Mar 17, 2021, accessed Apr 29, 2021, https://www.norad.mil/Newsroom/Article/2538728/norad-conducts-arctic-air-defense-exercise-amalgam-dart/

Conclusion

To enable the shift from CMA implementation to CMA integration in day-to-day RCAF operations, the focus needs to be on enabling CMA activities. Assuming that activities already underway with the initiation phase will continue, this leaves several activities to be conducted at the operational and tactical level. The operational level needs to be the subject-matter expert on CMA in air force planning, and to incorporate CMA considerations into the existing operational risk management process. This is matched by competency development at 1st, 2nd and 3rd line, and an increased awareness and training in order to develop a CMA-aware and capable culture, which could be seen as a culture parallel to Flight Safety. Finally, verification of force readiness at the operational and tactical level is required through standards and evaluation.

This chapter has focused on recommendations related to the activities inherent in CMA. Using the NIST Framework, gaps for operational level is principally related to Identify, while both the operational and tactical level have gaps in Detect, Respond and Recover. Similarly, 3rd line materiel support for the Protect function is needed. While discrete actions can be taken to enable these activities, achievement of lasting competency and capacity can only be accomplished through tailoring the organizational structure of the RCAF. This means identifying roles and responsibilities for these functions, and embedding them in permanent organizational structures and positions that hold accountabilities, responsibilities and authorities (ARAs) related to CMA.

CHAPTER 3 – COMMAND AND CONTROL CONSIDERATIONS

Introduction

This chapter examines the existing doctrine and organizational structures for command and control (C2) of the RCAF and the Joint Forces Cyber Component Commander (JFCCC). As CMA policy emphasizes that existing processes and structures will be used to their maximum extent possible, understanding current doctrine and C2 is necessary before assessing whether there are adjustments required to enable a steady-state conduct of CMA in the RCAF. The applicable doctrine will be studied in relation to the activity-based gaps identified in chapter 2, which principally relate to the functions of Identify, Detect, Respond and Recover. In the final section of this chapter, the organizational structure of Contingency Operation Plan (CONPLAN) LADON, a defensive cyber operation conducted in response to a threat or event in the cyber domain, will be described in relation to CMA and the Detect, Respond and Recover activities.

RCAF command and control (C2) doctrine has evolved substantially in the last decade. Indeed, there has been a concerted focus to develop, document, and teach how the RCAF generates and employs air power effectively in today's context. With the release of the second version of the RCAF Command and Control Doctrine Manual[86] in 2018, associated supporting articles from the RCAF Aerospace Warfare Centre (RAWC) and achievement of steady-state delivery of officer professional development programs, it can be posited that this doctrine is now mature and integrated into the RCAF culture.[87] Therefore, key concepts will be extracted from

[86] Canada. Department of National Defence, *RCAF Doctrine: Command and Control. B-GA-402-001/FP-001* (Trenton: Canadian Forces Aerospace Warfare Centre, 2018).

[87] In the author's opinion, while the culture change surrounding the air expeditionary construct was not easily accomplished, there are four reasons to state that maturity and integration has been achieved. 1. Formalization and release of the doctrine. 2. Comd 1 CAD direction to use a common organization and naming convention for Wings and ATFs (i.e. Mission Support Squadron/Element and Operational Support Squadron/Element), 3. Continuous, routine delivery of the RCAF's Professional Military Education courses on command, control and expeditionary ops, 4. Over six years of ongoing operations under the ATF construct.

the aforementioned articles and doctrine in order to identify organizational considerations for the CMA program in both Force Generation (FG) and Force Employment (FE) operations.

Air Power and Joint Operations

RCAF doctrine states that command and control must be considered separately in order to execute the primary air power tenet of centralized control, decentralized execution. As LCol Pux Barnes indicates, this tenet enables "the most efficient use of limited air assets, [permits] air power activities to be refocused quickly … respond to changing demands and priorities … and to be concentrated at the critical place and time."[88] It is paralleled by the concept that mission command, or "decentralized command" is used extensively by the RCAF with command authority assigned at the tactical level. In this construct, people and equipment are assigned to a tactical commander to allow flexibility and agility in order to execute the assigned mission.[89] The conclusion drawn from this principle is that the organizational structure needs either a minimum level of integral CMA capability in the smallest practicable unit for which tactical command (TACOM) is assigned, or in its immediate supporting infrastructure, such as the Operational Support Squadron at the Wing. For the RCAF, this is at the level of a Squadron/Wing for FG or an Air Task Force for FE. Therefore, assigned roles and responsibilities related to detecting and reporting incidents, and associated competency development, needs to be integral to these organizations.

Since 2011, the RCAF has developed and implemented the Air Task Force (ATF) concept to formalized the deployment of air forces in contingency and deliberate lines of operation. This "flexible C2 solution" enables operational or tactical command of assigned air

---

[88] Pux Barnes, *Command Or Control? Considerations for the Employment of Air Power in Joint Operations* (Trenton: Canadian Forces Aerospace Warfare Centre,[2014a]).

[89] Pux Barnes, *Mission Command and the RCAF: Considerations for the Employment of Air Power in Joint Operations* (Trenton: Canadian Forces Aerospace Warfare Centre,[2014c]).

forces both at home and abroad. [90] Two relevant particularities of the ATF doctrine are the requirement for the ATF Commander (ATF Comd) to monitor RCAF residual authorities and to implement and monitor operational risk management processes.[91] Operational risk management refers to the use of the approved Mission Acceptance Launch Authority (MALA) matrix and, when necessary, applying the Operational Risk Assessment Tool (ORAT).[92] In a similar vein, the five residual authorities exist to "protect personnel and equipment from unnecessary risk."[93] They are authorities which are retained by the FG Commander and do not transfer to the FE chain of command.

Of particular importance to CMA are the residual authorities of Technical Airworthiness and Operational Airworthiness. Organizational structure and risk management processes under the operational risk management framework, encompassing Technical and Operational Airworthiness in addition to operational risk, equally apply to FG and FE activities. Given that the RCAF CMA program intends to leverage this risk management framework, the existing organizational structure is broadly suitable to Respond to cyber incidents or threats: expertise and risk acceptance remain centralized and aligned with authorities at the operational level headquarters in 1 CAD and materiel support in DGAEPM.[94] However, minor additions to the existing organizational structure are necessary to incorporate technical expertise into operational and airworthiness-based risk assessments for CMA.

---

[90] Pux Barnes, *The RCAF Air Task Force: Considerations for the Employment of Air Power in Joint Operations* (Trenton: Canadian Forces Aerospace Warfare Centre,[2014d]).

[91] Canada. Department of National Defence, *RCAF Doctrine: Command and Control. B-GA-402-001/FP-001*, 42.

[92] Canada. Department of National Defence, *RCAF Flight Operations Manual* (Winnipeg: DND Canada,[2020b]), 2.2.2.4.

[93] Canada. Department of National Defence, *RCAF Doctrine: Command and Control. B-GA-402-001/FP-001*, 9.

[94] Canada. 1 Canadian Air Division, *1 CAD Orders, Volume 3, 3-310. Operational Risk Management for Air Operations* (Winnipeg: DND Canada,[2014]).

Operational Headquarters

At the operational level headquarters in 1 CAD, the Joint Forces Air Component Commander (JFACC) "integrates air effects into joint, combined operations."[95] Dual-hatted, the JFACC is assigned to the 1 CAD Comd by the Comd RCAF, and is supported by the standing Canadian Air Operations Centre (CAOC).[96] The 1 CAD Comd, as an air division commander, is the force generator and is responsible for RCAF readiness.[97] In contrast, the JFACC is the force employer of RCAF air power. Therefore, a single individual acts on behalf of the RCAF Comd for C2 of FG and FE air operations, supported by the air staff (A Staff). Further, as the sole air component commander for the CAF, the JFACC fills three roles: JFACC to Comd CJOC, JFACC to Regional Joint Task Force (RJTF)/JTF Comd, and Canadian NORAD Region (CANR) Comd, in addition to responsibility for regional search and rescue.[98] Broadly, the JFACC has the responsibility to "recommend proper employment and C2,"[99] "provide air-power *support*,"[100] and in respect to NORAD "exercising C2 of all air forces assigned, attached and made-available to the NORAD mission in CANR."[101]

The JFACC and the CAOC's role in planning, directing, controlling and coordinating air forces at the operational level, domestically and abroad, implies that there is a need for embedded expertise in the CAOC staff on CMA such that Respond and Recover activities can be

---

[95] Pux Barnes, "The JFACC and the CAOC-Centric RCAF: Considerations for the Employment of Air Power in Joint Operations," *RCAF Journal* 3, no. 3 (Summer, 2014b), 12-20. http://www.rcaf-arc.forces.gc.ca/en/cf-aerospace-warfare-centre/elibrary/journal/2014-vol3-iss3-04-the-jfacc-and-the-caoc-centric-rcaf.page.

[96] Support is also exercised at the Wing level in order to supplement CAOC staff; however, as the Wing is at the Tactical level it is excluded from this discussion on Operational Headquarters.

[97] Canada. Department of National Defence, *RCAF Doctrine: Command and Control. B-GA-402-001/FP-001*, 24.

[98] Ibid., 31.

[99] Barnes, "The JFACC and the CAOC-Centric RCAF: Considerations for the Employment of Air Power in Joint Operations," 12-20

[100] Barnes, "The JFACC and the CAOC-Centric RCAF: Considerations for the Employment of Air Power in Joint Operations," 12-20. Emphasis by Barnes.

[101] Barnes, "The JFACC and the CAOC-Centric RCAF: Considerations for the Employment of Air Power in Joint Operations," 12-20.

conducted. Embedded Air Component Coordination Elements (ACCE) representing the JFACC at CJOC and the RJTFs, have a similar responsibility, but given the relatively small size of these elements and their responsiveness to the CAOC, CMA support could be sufficiently accomplished through reach-back, like many other specialist A Staff positions, i.e., A4 Construction Engineer, A4 Maintenance, A6, etc.[102]

Respecting this construct, a proposal for the 1 CAD Cyber Team is currently in development. The Cyber Team's primary objective would be to support Operations and Readiness, leveraging cyber expertise from four occupational areas: air operations, air maintenance (AERE), communications and electronics (CELE), and intelligence (INT). Some of the positions are planned to be part time, given estimated workload.[103] The inclusion of additional specialties in the cyber team acknowledges that PT and operations integration requires knowledge and experience from various stakeholders, and is expected to help broaden the ability to conduct planning, risk management activities, and operations control. This is particularly relevant in relation to airworthiness considerations for cyber risk management, and is discussed further below. Finally, although approval for this organizational change is pending, and it is intended as an interim step, it will be used as the baseline of the 1 CAD HQ's cyber C2 structure.

[102] While it is acknowledged that the CAOC staff is small, and not fully staffed, the creation of additional positions elsewhere is thought to only exacerbate this situation and further disperse the limited amount of existing expertise.

[103] Canada. 1 Canadian Air Division, *1 CAD / CANR / JFACC Cyber Mission Assurance (CMA) Overview and Brief* (Winnipeg: DND Canada,[2020]).

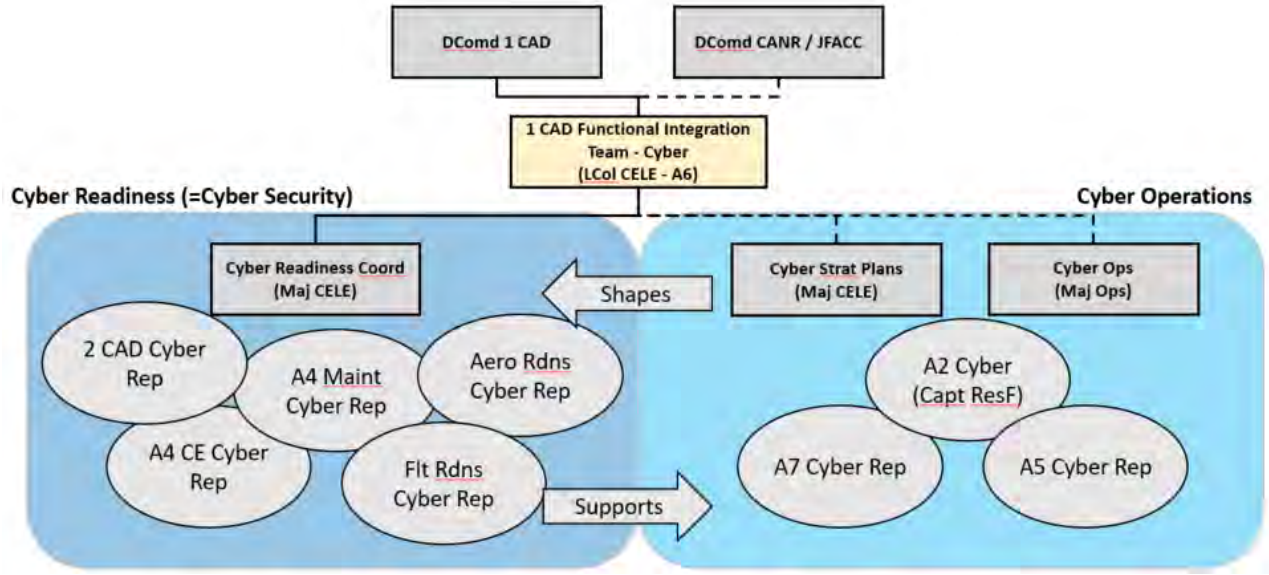

Figure 3.1 – 1 CAD/JFACC/CANR Cyber Team (Interim) v5
Source: Maj Kieres, Email conversation with author, 7 April 2021

Standards and Evaluation Teams

Standards and Evaluation Teams (SETs) are detached sections of 1 and 2 CAD, and are responsible to the Operational Airworthiness Authority (OAA) through the 1 CAD Deputy Comd FG or 2 CAD Comd. The SETs exist to ensure standardization across 1 and 2 CAD Wings, in addition to ensuring operational airworthiness oversight. The full list of SETs is described at CADO 5-508, with SETs assigned to monitor aircrew readiness on each fleet of aircraft, aerospace control operators, maintenance personnel, and 1 and 2 CAD HQ operations staff. Air Force Standards is the coordinating element that provides RCAF wide standardization across all communities. Air Force Standards also has the responsibility to "identify, research and address issues" in addition to "maintaining an ongoing awareness of aviation best practices."[104]

Operational Standards Visits (OSV) are conducted each 12-24 months at operational units to monitor compliance with "CAD Orders, Manuals of Operation and Standard Operating

[104] Canada. 1 Canadian Air Division, *1 CAD Orders, Volume 5, 5-508. Standardization and Evaluation Teams* (Winnipeg: DND Canada,[2019]).

Procedures."[105] These visits are documented by a report to a delegate of the OAA on administration of standards, training and operational procedures (mission planning, basic and advanced procedures, emergencies, etc.) in order to confirm that operations are being safely and effectively conducted. Currently, there is no responsibility for any of the SET organizations to report on the ability of a units to conduct operations in a cyber-contested environment. By extension, OSVs do not verify a unit, supporting element, or operator's ability to Detect, Respond and/or Recover from a cyber event.

Materiel Group Support

The Assistance Deputy Minister for Materiel (ADM(MAT)) reports to the Deputy Minister of National Defence, as the "central service provider and functional authority for all defence materiel and equipment programs."[106] The organizations under ADM(MAT) thus manage military equipment throughout its entire life cycle, from conception to disposal. Reporting to ADM(MAT), the Director General of Aerospace Equipment Management (DGAEPM) is responsible for material support for aerospace equipment. DGAEPM is principally organized along capability lines, such as fighters and trainers, tactical aviation, and Radar and Communication Systems (R&CS), supported by specialist expertise in the Directorate of Technical Airworthiness and Engineering Support (DTAES). Positions in DGAEPM, including DTAES, are principally filled by Aerospace Engineers (AERE), senior air maintenance technicians, or their public servant equivalents. In comparison, positions in the R&CS directorate are filled by Communications and Electrical Engineers (CELE) and communication branch technicians.[107]

---

[105] Ibid.

[106] "Materiel Group Home: About Us," DND Canada, accessed Jan 20, 2021, DWAN intranet: http://Materiel.mil.ca/about-us/index.page.

[107] Author's experience from four years of employment in DGAEPM Fighters and Trainers Directorate.

While there are no formal reporting lines between DGAEPM and the RCAF, there is coordination and support provided by DGAEPM to the RCAF for materiel management of its assets. These lines of support and coordination occur typically between 1 CAD staff officers of the associated fleet or equipment, and also with direct engineering support provided to units operating or maintaining aircraft and equipment. The purpose of this coordination is to ensure operational effectiveness throughout the life cycle of the equipment, in addition to conducting risk management, and maintaining airworthiness. [108] These lines of communication are essential to support the Detect function, and risk management and mitigation activities in Respond and Recover.

Risk Management Authorities

The activity and various processes surrounding risk management have already been discussed at length in their relation to CMA. However, the authorities, responsibilities and accountability chain merits further discussion. Three separate authorities will be discussed: Technical Airworthiness Authority (TAA), Operational Airworthiness Authority (OAA), and Operational Command Risk Acceptance Authority (OCRAA). The TAA and OAA have powers and responsibilities granted in accordance with the *Aeronautics Act* for the airworthiness program. The TAA is responsible for "all standards of safety for aeronautical products relating to product design, manufacture, maintenance and materiel support." While the OAA is responsible for "all standards of safety for air operations and aeronautical products relating to flying operations."[109]

---

[108] Canada. Department of National Defence, *Technical Airworthiness Manual (TAM). C-05-005-001/AG-001* (Ottawa: DND Canada,[2019]).

[109] Canada. Department of National Defence, *Operational Airworthiness Manual (OAM). B-GA-104-000/FP-001* (Winnipeg: DND Canada,[2017]).

Canada. Department of National Defence, *Technical Airworthiness Manual (TAM). C-05-005-001/AG-001*

The airworthiness program is concerned with achieving an acceptable level of safety for military aeronautical products based on four principles: airworthiness related activities are completed to accepted standards, by authorized individuals, accomplished within acceptable organizations using approved procedures.[110] When the acceptable level of safety cannot be maintained, an airworthiness risk is identified: "danger or threat to safety of flight caused by a failure related to operational or technical standards related to the design, manufacture, operation or maintenance of an aeronautical product."[111] When this occurs, the Risk Assessment Risk Management (RARM) process is conducted jointly by the TAA and OAA to describe the risk, propose a plan for mitigation, and seek OCRAA endorsement. As the name implies, the OCRAA accepts command responsibility for operating with the identified risk and approves the risk management plan. In the context of airworthiness risk, OCRAAs are assigned by the OAA to accept increasing levels of risk and may be assigned outside of the regular chain of command.[112]

The OCRAA has a similar role in the operational risk management process. However, differentiating itself from the airworthiness program, operational risk "is concerned with threats … due to the specific conditions that exist that may impact the successful conduct of any operation, mission or task."[113] It is inclusive of conditions impacting force generation, interoperability challenges, the operating environment, and enemy presence or capabilities; it excludes any type of accidental loss. While the airworthiness program is a regulatory compliance mechanism to Canadian law, operational risk management exists to facilitate mission

---

[110] Canada. Department of National Defence, *Technical Airworthiness Manual (TAM). C-05-005-001/AG-001*

[111] Canada. Department of National Defence, *Operational Airworthiness Manual (OAM). B-GA-104-000/FP-001*, 5-1.

[112] Ibid.

[113] Ibid.

achievement and is governed by a 1 CAD Order (CADO).[114] Despite the different objectives behind airworthiness and operational risk, the OCRAA's role remains as the operational commander with the authority to accept the identified operational risk, with or without mitigating actions. The Operational Risk Assessment Tool (ORAT) follows a similar format to the airworthiness program's RARM, documenting the risk, mitigation plan, and its acceptance and approval. Subject matter experts and stakeholders are used as necessary to complete the ORAT, but no specific authorities or roles are pre-assigned. Similarly, the OCRAA for operational risks is not clearly designated by an overarching order. An ORAT is approved by the "appropriate Commander responsible for implementing the operation at risk" and "the onus [is] on each Commander … to determine if they have the authority to proceed."[115] The accountability chain of the operational commander aligns with the existing chain of command for either FG or FE.

Also under the umbrella of operational risk is the Mission Acceptance Launch Authority (MALA), which "enables risk management of flight operations at the tactical level."[116] Different from both the RARM and the ORAT, the MALA "identifies the accumulation of risks and hazards."[117] As described in the Flight Operations Manual, the authority and initial approval for domestic and deployed operations is by Comd 1 CAD, or delegate, and effectively provides OCRAA by pre-approving the delegation of the risk acceptance authority to the tactical level. Here, the Flight Authorization Officer is assigned by the resulting risk level from applying the MALA matrix and has the responsibility to confirm that Mission Acceptance has been given at the appropriate level and authorizes launch authority.[118]

---

[114] Canada. 1 Canadian Air Division, *1 CAD Orders, Volume 3, 3-310. Operational Risk Management for Air Operations*

[115] Ibid.

[116] Canada. Department of National Defence, *RCAF Flight Operations Manual*, 2.2.2.4.

[117] Ibid.

[118] Ibid.

CMA can apply to both airworthiness and operational risk, depending on the threat's effect on safety of flight or mission effectiveness. Given the described roles and responsibilities of the OA, TA and OCRAA, there is an existing and suitable chain of accountabilities that may be leveraged for the use of the RARM, ORAT and MALA processes. In relation to the RARM and ORAT, changes have been proposed to better align these processes to the CMA program.[119] Similarly, there is a requirement for Director of Fleet Readiness to update MALAs for operating fleets to incorporate CMA risk considerations. The changes to the MALA will enable the Detect function at operational units, while updates to the RARM and ORAT will enable Protect, Detect, Respond and Recover functions to occur. Common to these risk management tools is the ability of the RCAF Commander to control risk to air assets in air and joint operations, and their use for CMA is a logical extension of this command responsibility for risk acceptance.

Joint Forces Cyber Component Commander

The Joint Forces Cyber Component Commander (JFCCC) also serves as the Director General Information Management Operation (DGIMO). The DGIMO force generates "cyberspace capabilities on behalf of the Cyber Force Commander (CFC)," and provides "service delivery and cyber protection of assigned IM/IT on behalf of ADM(IM)."[120] The JFCCC is charged with "FE of cyberspace capabilities on behalf of a Designated Supported Commander (DSC)."[121] This implies that the JFCCC has a responsibility to contribute to joint planning and employment of cyber assets, inclusive of crisis response, as well as joint exercises and coordination with other cyber-related partners (ADM(IM), CSE, OGDs, NORAD, Five Eyes

[119] R.G. Scholes, "The RARM and ORAT for RCAF Cyber Mission Assurance" (Joint Command and Staff Program Service Paper, Canadian Forces College, Toronto, 2021).

[120] Canada. Department of National Defence, *Roles and Responsibilities - Joint Force Cyber Component Commander* (Ottawa: DND Canada,[n.d.]).

[121] Ibid.

partners, NATO, etc.). In the FE role, the JFCCC "is responsible for making recommendations to the DSC on the proper employment of cyberspace assets and on [their] C2."[122] Therefore, CANR Comd, as a DSC, has a touch point with the JFCCC in support of cyber FE for the NORAD mission.

In support of Comd CJOC, the JFCCC has a standing Cyber Component Coordination Element (CCCE) integrated into CJOC for the purpose of operational-level coordination and planning. The CCCE integrates into the operational planning process, advising on cyber operations and coordinating with J3, J5 and J6 staff as necessary. Further, the CCCE is responsible to maintain situational awareness of cyber assets deployed on operations including feedback on support and sustainment.[123] Similar CCCE structures could be used in support of CANSOFCOM, NORAD or JTF HQs when identified as a DSC, but have not been employed as either temporary or permanent organizations.

Another component of the forces under the authority of the JFCCC is the Canadian Forces Cyber Group, which includes the Canadian Forces Network Operations Centre (CFNOC) and their Cyber Protection Teams (CPT). As the CFNOC Concept of Operations observes, "CFNOC's essential task is the conduct of defensive cyber operations – internal defensive measures (DCO-IDM)" with a focus "on the continuity of military operations (Mission Assurance)."[124] While DCO-IDM as a deliberate operation is the highest priority effort at CFNOC, they may also deploy mission tailored teams in response to an anticipated cyber incident, or one that has occurred, i.e. incident response. Priority of effort is further refined by

---

[122] Ibid.
[123] Ibid.
[124] Canada. Canadian Forces Network Operations Centre, *Canadian Forces Network Operations Centre (CFNOC) Concept of Operations* (Ottawa: DND Canada,[2019]), 3.

operational and intelligence priorities.[125] While the mandate of the CFNOC Concept of Operations implies that they are responsible to "ensure the CAF has freedom of action within the CAF cyberspace"[126] various other sections of the same document refine their area of responsibility to the DND/CAF network. There is therefore ambiguity on whether CFNOC is solely responsible for IT systems, or whether they have a role to play in PT, recognizing that current CFNOC capabilities remain IT focused.

In all cases, the JFCCC and subordinate organizational elements are focused on cyber operations. While DCO enables CMA in the detection phase, and is a fundamental risk mitigation activity for Response and Recovery, these are separate functions with different responsibility chains. Additionally, JFCCC responsibility is scoped to providing cyber expertise and support to force employers, and has traditionally focused on IT systems. These combined factors clearly indicate a limited ability to leverage JFCCC assets in support of the RCAF CMA program and reaffirms that an integral cyber capacity is required. However, best practices can be shared and a consideration not to duplicate structures must remain central to proposed organizational changes. For example, development of a 1 CAD Cyber planning cell should consider CCCE structure and expertise. Similarly, PT incident response teams should leverage lessons learned from CFNOC CPT in addition to minimizing overlap in capabilities. In the event of a significant cyber event, dedicated incident response teams would be required. CONPLAN LADON templates how this response would occur.

CONPLAN LADON

CONPLAN LADON is a pan-CAF contingency plan that responds to a cyber event, or imminent threat, which would affect the ability to deploy, employ, sustain, command and control

[125] Ibid., 6.
[126] Ibid., 2.

FE operations.[127] The CONPLAN can be activated, with CDS consent, by three CAF force employers (Comd CJOC, Commander Canadian Special Operations Forces Command [CANSOFCOM] and Comd NORAD) when assigned forces are insufficient to deal with the cyber event. The CONPLAN is a DCO-IDM operation, and therefore conducts "activities … within [CAF's] own cyberspace to ensure freedom of action."[128] Direction and execution of the CONPLAN is delegated to the JFCCC, and the FE Comd is designated as the supported commander. While the CONPLAN executes activities in or through the cyber domain, it is done with the intention to enable unimpeded operation of IT, OT and PT in an operational theatre.

Phase 0 of CONPLAN LADON is indications and warnings, and is continuously in effect through normal day-to-day cyber security actions and monitoring by the existing cyber authorities and C2 structure. The transition from Phase 0 to Phase 1 can be described as the completion of a detect activity. This escalation and activation of further CONPLAN phases occurs in conjunction with a risk assessment, which the CONPLAN describes as uniquely IT centric and reported in accordance with IMS 6003-1-1.[129] However, in the larger context of PT and OT, this is a CMA process that should leverage the most suitable cyber-specific risk management process for the affected systems. Acceptance of the risk, either as proposed through CMA or as prescribed by IMS 6003-1-1, limits or authorizes operations during the respond activity, i.e., CONPLAN LADON Phases 1 and 2 where the adversary is contained and expelled from CAF (blue) cyberspace.

---

[127] Canada. Chief of the Defence Staff, *CONTINGENCY OPERATION PLAN (CONPLAN) LADON - Defensive Cyber Operations - Internal Defensive Measures* (Ottawa: DND Canada,[2019]).

[128] DTB 694341

[129] ADM(IM) Canada., *IMS 6003-1-1, Information Technology Security Incident Management* (Ottawa: DND Canada,[2018]).

CONPLAN LADON is a one-time effort under a named operation, where additionally attributed forces are apportioned to the FE Comd, but retained under the command of the JFCCC, to conduct DCO-IDM. Like all other CONPLANs, activation of LADON is in exceptional circumstances; further it focuses on the DCO portion of the activities of Respond and Recover, and employs CFNOC CPTs which are currently equipped and trained for enterprise IT systems, not PT. Additionally, the reporting mechanism through the ADM(IM) chain does not sufficiently address airworthiness and operational risks as required by extant RCAF policies. Finally, LADON specifies that it is only activated when local resources are exhausted or insufficient to respond to the cyber threat.

In short, CONPLAN LADON does not respond to the day-to-day requirements of RCAF CMA activities. This implies that the existing RCAF organization, both in FE and FG, must have expertise and personnel able to Detect and Respond to routine cyber events and a surge capacity for incident response. For the Respond activity, this must include reporting to appropriate RCAF risk acceptance authorities (OCRAA). Similarly, the RCAF requires involvement in initiating or improving features related to the Protect function due to PT expertise and, potentially, airworthiness requirements. In the context of CMA, these factors support the recommendations for embedded cyber capacity in the smallest practicable unit for which tactical command (TACOM) is assigned (Squadron/Wing or ATF), in the CAOC, and supported by specialist technical support in ADM MAT/DGAEPM.

Conclusion

This chapter focused on the existing doctrine and C2 structures for RCAF FG and FE in order to inform a tailored organizational structure for CMA. Further, it looked at joint organizations and CONPLAN LADON to assess where non-RCAF elements could be

incorporated to minimize duplication of responsibilities. This assessment was considered in the context of steady-state RCAF CMA operations, for the activity gaps related to Detecting, Responding to, and Recovering from cyber threats or incidents.

At the tactical level, CMA activity gaps were related to Detection, as well as initiating a Response and Recovery through a reporting chain. Therefore, given RCAF C2 doctrine, tactical level CMA capacity needs to be integral to the Squadron or Wing for FG, and in the ATF when deployed. At the operational level, the focus is on integration of CMA into planning and risk management in order to Respond and Recover. Inclusion of different occupations in the 1 CAD Cyber Team will broaden the scope of cyber considerations and the capacity to support operational planning. Related to planning joint operations, coordination already occurs with the CCCE; however, there may be opportunities to exploit their lessons learned.

For risk management, linking to Response and Recovery, the existing authorities and processes for the RARM, ORAT and MALA are assessed as suitable for CMA, with the caveat that subject matter experts must be involved in their preparation. However, tailoring the risk management processes for CMA is recommended as a pre-cursor to the transition to in-service CMA activities. Finally, common to both tactical and operational level is the need for standards and evaluation on CMA Detect, Respond and Recover activities, and it is proposed that this leverages the existing SET framework. These four recommendations: integral CMA capacity for FG and FE, occupational breadth, cyber expertise in risk management, as well as standards and evaluations, form the framework for assessment of emergent CMA-focused organizations in the next chapter.

CHAPTER 4 - CASE STUDIES

Introduction

In this chapter, the CP140 Mission Defence Team – Cyber, Canadian Air Defence Sector Mission Defence Team, 1 CAD Cyber Team, and the Royal Canadian Navy's (RCN) Fleet Cyber Team (FCT) will be addressed as organizational case studies for CMA. Each of the case studies will be conducted in the same manner, and using the same analytical framework for consistency and rigour in the development of the resulting conclusions. While the focus of this assessment is for RCAF organizations, the RCN FCT is included as a case study due to similarities with RCAF safety culture, the program's similar level of maturity to RCAF equivalents, and the cyber force strategy's endorsement by the Commander of the RCN.

To conduct the assessment, first, the organization will be introduced and described in terms of its purpose, how the proposal was developed, and its level of maturity. This section will also describe the reference documentation used for the analysis. Then, the organization will be assessed against the four command and control factors which were developed in chapter three, taking into consideration their suitability to complete Detect, Respond and Recover, and specific to the Operational level, the relevant activities from Identify and Protect. A summary of the results will then be discussed to identify strengths, areas of improvement, and observations for the final recommendations of a CMA organizational structure for the RCAF.

The assessment of these organizations is pertinent to the development of this paper's recommendations because it represents several varied approaches to the same problem, all of which have been principally developed from the bottom-up by individuals with different experiences and backgrounds. It therefore provides multiple perspectives into the problem of adapting existing organizational structures to meet an emerging problem, considering the high

reliance on professional competencies, potential resistance to cultural change, and institutional shortages of personnel. By taking into consideration organizations which have been developed under these constraints, the "blue sky" solution proposed in this paper will be more grounded in the reality of the CAF. At current time, each of these organizations is in the very early implementation, and their reference documentation is principally in draft form. Further, the proposed organizations are largely seen as a first step towards dedicated cyber mission assurance teams: future iterations and evolution are expected. Therefore, the assessments drawn here may have immediate applicability, in addition to informing the proposal for a permanent organizational structure that enables steady-state CMA.

CP140 Mission Defence Team

The CP140 Aurora aircraft is a Canadian variant of the Lockheed P3. It was purchased in 1982 for the purposes of Maritime Patrol, and has undergone several incremental upgrade programs to maintain operational relevancy. While its current role is described as Long Range Patrol in the maritime environment, inclusive of Anti-Submarine Warfare, Above Surface Warfare, and Intelligence, Reconnaissance and Surveillance (ISR), it is also equipped for overland ISR missions such as those executed during OP IMPACT.[130] Supporting these diverse and highly technologically sophisticated roles is the latest aircraft upgrade through the Block IV program, which updates sensors, self-defence and communications systems.[131] The implementation of the Block IV upgrades introduce new vectors for cyber threats to both mission

[130] "Operation IMPACT," DND Canada, last modified Dec 15, accessed Mar 2, 2021, https://www.canada.ca/en/department-national-defence/services/operations/military-operations/current-operations/operation-impact.html. Bernie Thorne, "The Lockheed CP-140M Aurora, Canada's Current Long Range Patrol Fleet," *Canadian Military Journal* 21, no. 2 (Spring, 2021), 26-37. http://www.journal.forces.gc.ca/vol21/no2/PDF/CMJ212Ep26.pdf., 29-33.

[131] Bernie Thorne, "The Lockheed CP-140M Aurora, Canada's Current Long Range Patrol Fleet," *Canadian Military Journal* 21, no. 2 (Spring, 2021), 26-37. http://www.journal.forces.gc.ca/vol21/no2/PDF/CMJ212Ep26.pdf., 28-29, 33-35.

and airworthiness, as well as providing a means to execute cyber defence and mission assurance (Protect and Detect features).

The CP140 Mission Defence Team – Cyber (MDT-C) has been initiated as an integral component of the research phase of the Force Development process for RCAF CMA. The CP140 Aurora was selected for this DTAES led effort as, following the Block IV program upgrades, as the aircraft will have continuous internet connectivity while airborne and integrated cybersecurity design features.[132] The CP140 MDT-C is assigned as a flight in the 415 Long Range Patrol Force Development Squadron (415 Sqn), with a Service Level Agreement between 1 CAD and DGAEPM supporting the MDT-C's responsibilities for cybersecurity and defence. Its purpose is "to provide … an organic first and limited second line cybersecurity capability to manage and maintain the CMA and continuous airworthiness cybersecurity posture of the CP140," with a stated secondary objective to inform the CMA force development efforts.[133]

The importance of this organizational trial is that it deals directly with the complexity of integrating CMA into PT in the RCAF. It has the dual requirements of addressing safety of flight and operational risks from threats in and through cyberspace, and is therefore subject to both CMA and Airworthiness Program considerations. Further, given the RCAF human resources structure and airworthiness regulatory requirements, it necessitates reliance and integration with the air maintenance branch and operators: this is not an organization with an exclusive communications and electronics branch footprint. The Concept of Employment documentation for the MDT-C underscores the premise that "technical and engineering personnel involved in the day to day technical support … need to be at the forefront" of the CMA effort, as they best

---

[132] Government of Canada. Department of National Defence, *DRAFT v1D - CP140 Mission Defence Team - Cyber (MDT-C) Concept of Employment. RDIMS 1968517* (Ottawa: DND Canada,[2021b])., 1.
LCol Janine Blanchet (DADD), email conversation with author, 20 Jan 2021.

[133] Ibid.

understand the technology which is being protected and defended. It goes further to state, that there is a cultural and experiential gap related to the cyber domain which will necessitate training and close collaboration.[134]

As of late summer 2020, the CP140 MDT-C is staffed with one Captain Aerospace Engineer (AERE) as the flight leader. His primary emphasis, in close liaison with DTAES, has been the completion of the Concept of Employment, inclusive of the key tasks of the MDT-C, proposal for an organizational structure (rank, experience, training, occupation, etc.), and assignment of tasks, roles and responsibilities to the identified positions.[135] This work remains in development, with the Concept of Employment nearing a final draft. Options for a proposed organizational structure have been discussed, and a probable structure is included in Figure 4.1. As of February 2021, two reservist positions (1x Cyber Operator and 1x Any Trade – with a desire to staff with an Avionics Technician) are allocated to the MDT-C but are not filled.[136]

[134] Ibid, 2-3.
[135] Capt Alec Harlow (415 Sqn), telephone conversation with author, 12 February 2021.
[136] Capt Alec Harlow (415 Sqn), email conversation with author, 4 March 2021.

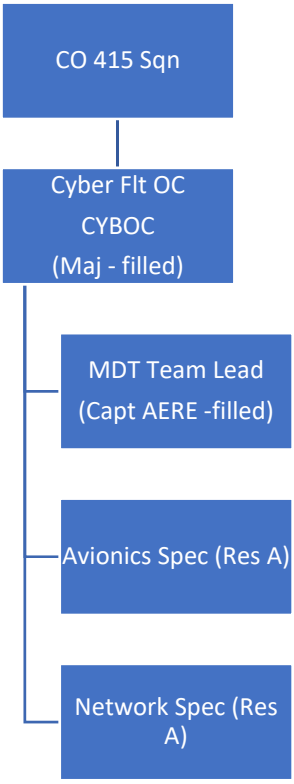

Figure 4.1 – CP140 MDT-C Proposed Organization
Source: Department of National Defence, *DRAFT CP140 Mission Defence Team - Cyber (MDT-C) Implied Tasks Breakdown*, 6.

Table 4.1 – CP140 MDT-C Assessment

Factor	Analysis
Integral CMA capacity for FG & FE	- A small team of one full time and two part-time members is proposed at 415 Sqn, which regularly provides software support to the operational squadrons. - Task list speaks principally to domestic operations (FG and FE), does not address deployed operations for FG or FE. - Balanced consideration of Detect, Respond, Recover activities. - Identifies linkages for Protect function with DGAEPM staff.
Occupational breadth	- MDT is mixture of maintenance and communications branch. - Leverages DTAES 8 embed in CFINTCOM for threat cueing.
Cyber expertise in risk management	- MDT Team Lead has responsibility to conduct initial risk assessments. - Clearly describes need for airworthiness reporting (initiate response activities such as RARM), and integration of cybersecurity in fleet-specific airworthiness policy (Engineering Process Manual Supplement). - Proposes to leverage Flight Safety reporting.

	- Describes necessity to report operational risks to operational authority in 1 CAD and support ORAT generation. - Proposes use of the MCAAV tool to assess new threats; unclear how this will tie directly into RARM or ORAT. - Inclusion of technical and operational authorities, and coordinating relationships. - Identifies JFCCC/DGIMO roles and responsibilities.
Standards and evaluation	- Describes cyber readiness, but principally related to technology verification. - Proposes conducting internal exercises and drills.

Source: Department of National Defence, *DRAFT v1D - CP140 Mission Defence Team - Cyber (MDT-C) Concept of Employment*, 1-14.

The results of the assessment at Table 4.1 show significant consideration for safety of flight and airworthiness regulations, and speaks to the necessity of engagement with operational and technical risk authorities. It describes use of the RARM and ORAT, stating that the MDT-C Team Lead is responsible for conducting initial risk assessments in these processes. It leverages the MCAAV tool for in-service risk management as a practical extension and operationalization of the RCMAP, thereby providing a consistent means of assessing cyber threats through acquisition, modification and operational use. While these are procedural observations, they indicate maturity in the development of tasks, roles and responsibilities of the MDT-C Team. The concept of employment also describes a coordinating relationship with DTAES, 1 CAD operational authorities, and the Weapon System Manager (WSM), although little detail is provided. Related to an integral CMA capacity, the flight's structure under 415 Sqn provides a wing-level cyber resource that matches the fleet's software engineering support model.[137] In summary, the strengths of this organizational structure include active engagement of cyber expertise in risk management and an integral CMA structure for domestic, east coast operations. However, it must be noted that this is a purely theoretical assessment based on a moderate level

[137] Government of Canada. Department of National Defence, "DRAFT v1D - CP140 Mission Defence Team - Cyber (MDT-C) Concept of Employment", 1-14.

of process and task description detail which stands to be proven when human resources are assigned and the model is able to be put into practice.

From the case study, two areas for improvement are identified. First, there is a necessity to support CP140 fleet assets on the west coast and in a deployed context. Secondly, there is a need for greater occupational depth and breadth.[138] In the current structure, there is no discussion of how the MDT-C will provide support to fleet assets which are away from Greenwood. Considerations should be made for how the force would adapt and expand to support FG deployments, expeditionary FE, and for fleet assets that operate out of CFB Comox, BC. This ties closely into the observation regarding occupational breadth and depth: the total number of personnel proposed for the proof-of-concept are anticipated to be insufficient for the currently described scope of tasks and responsibilities. Further, there is little discussion of the interface with operational squadrons, who are the prime units that the MDT-C supports, and it is certain that CP140 avionics expertise will be needed in order to adequately conduct CMA on the fleet.[139] Finally, in regards to observation related to evaluations and standards, the requirement for internal exercises and testing is a valid requirement. When higher headquarters or operational level guidance is issued regarding standards and evaluation, it is expected that a new task would be required to internally implement, train and monitor these standards.

In summary, the CP140 MDT-C clearly describes the overarching roles, responsibilities, tasks and processes that are necessary for CMA execution. The emphasis on deliberate risk management using existing tools is reflective of the influence from air maintenance branch

[138] A second proposal for a larger MDT-C organization was provided by Capt Alec Harlow to more adequately addresses the scope of tasks described by the concept of employment, but it has insufficient detail to be analyzed and there are no resources to staff such an organization at this time.

[139] The requirement for avionics expertise is known and well internalized by the MDT-C Team Lead, but is not formally identified in the reserve staffing requests for the two MDT-C positions in order to maximize the hiring pool. Capt Alec Harlow (415 Sqn), email conversation with author, 4 March 2021.

personnel who have driven and shaped this organization's development. This is expected to be a major strength going forward, and should assist in bringing credibility to CMA efforts as the operational community is familiar with these processes. It is expected that as the organization brings on additional human resources, it will be able to commence defining the standard operating procedures for data collection, baselining, incident response, and other activities inherent in its role to Detect, Respond and Recover. The challenge will be to prioritize these activities within the MDT-C's limited capacity, iterate through the first applications of an in-service MCAAV for a legacy fleet, and establish a strong relationship with the operational CP140 squadrons.

Canadian Air Defence Sector Mission Defence Team

The Canadian Air Defence Sector (CADS) surveils, identifies, warns and provides tactical command and control for aerospace defence forces in the Canadian NORAD Region (CANR).[140] It conducts this mission on behalf of Commander NORAD, reporting to the Comd CANR, using "a network of satellites, ground-based radar, airborne radar and fighters to detect, intercept and … engage any air-breathing threat."[141] As this statement implies, there is an existing heavy reliance on cyber-enabled systems with further connectivity planned through modernization, the Strategic Homeland Integrated Ecosystem for Layered Defense (SHIELD). Combining integrated systems with clear recognition of adversary capability and intention in the cyber domain, underlies the importance of CMA for NORAD.[142] For these reasons, CADS

[140] "22 Wing North Bay," DND Canada,

[141] "North American Aerospace Defense Command," US DoD, last modified n.d., accessed Mar 26, 2021, https://www.norad.mil/About-NORAD/.

[142] Terrence J. O'Shaughnessy and Peter M. Fesler, *Hardening the Shield: A Credible Deterrent & Capable Defense for North America* (Washington: Woodrow Wilson International Center for Scholars,[2020]).

Mission Defence Team (MDT) is the second proof-of-concept for the RCAF CMA force development effort.

The CADS MDT leverages the experience of 22 Wing as the original lead for the Cyber Functional Integration Team and draws on the responsibility and expertise of the Communications and Information Systems (CIS) Flight (communications and electronics branch) which maintains local NORAD PT (Battle Control System).[143] Further, it benefits from existing cyber program maturity in the NORAD headquarters, including routine cyber exercises. With a very different composition of occupations from flying squadrons across the RCAF, and the uniqueness of operating a critical, bi-national command and control node, the trial at CADS is important to inform the design of a permanent organizational change for the RCAF.

The purpose of the CADS MDT is to "detect, deter and defend against cyber threats on the CADS mission systems."[144] This mission statement is a clear expansion beyond the role of CMA, and speaks to the previously discussed functional overlap of CMA with DCO-IDM and the near-to-medium term requirement to supplement CFNOC with mission system expertise. Resulting from this broader scope, the CADS MDT Concept of Operations (CONOPS) provides activities to be conducted in each of the five functions of NIST's Cybersecurity Framework (Identify, Protect, Detect, Respond and Recover).[145] Some of the tasks, particularly in the Identify and Protect phases, were previously assessed in chapter two as the responsibility of 1 CAD or DGAEPM, and may not be well suited to a small, embedded MDT within CADS. The inclusion of these tasks may be reflective of the role that CADS has played in implementing

---

[143] Canada. 1 Canadian Air Division, *1 Cdn Air Div Cyber Functional Integration Team (FIT) - Comd's Guidance* (Winnipeg: DND Canada,[2012]). Maj Rebecca Pietzsche, telephone conversation with author, 12 February 2021

[144] Government of Canada. Department of National Defence, *DRAFT - Canadian Air Defence Sector (CADS) Mission Defence Team (MDT) Concept of Operations*DND Canada,[2020a])., 6.

[145] Ibid., 6-8.

cyber mission assurance activities in the RCAF over the last decade, including critical implementation activities like the Cyber Key Terrain Analysis. Of note, however, the CONOPS later identifies the scope of the MDT's functions to more closely align with the expected activities of Detect, Respond and Recover.[146]

The development of the CADS MDT CONOPS was conducted by CIS Flight leadership, leveraging work by the RCN in their development of the draft FCT CONOPS, and tailoring these activities, roles and responsibilities to CADS. The CADS MDT CONOPS is thorough in its description of tasks, and has a clear understanding of the role it will play in CMA and DCO-IDM on PT. While the CONOPS remains a draft, it is the most mature of the RCAF organizations studied in this chapter. The proposed organizational structure of the MDT (Figure 4.2) leverages the existing CIS Flight in 22 Wing. As of February 2021, the MDT has been allocated two reservist positions (1x Aerospace Telecommunication and Information System (ATIS) Technician and 1x Cyber Operator) and is actively recruiting for a public servant to fill the MDT Operations Officer position.[147] While none of these three positions are presently filled, the allocation of positions and funding towards 60% of the proposed force structure is a significant step towards the necessary resources to conduct CMA.

[146] Ibid., 8.
[147] Maj Rebecca Peitzsche (22 Wg OC CIS Flt), email conversation with author, 20 Jan 2021.

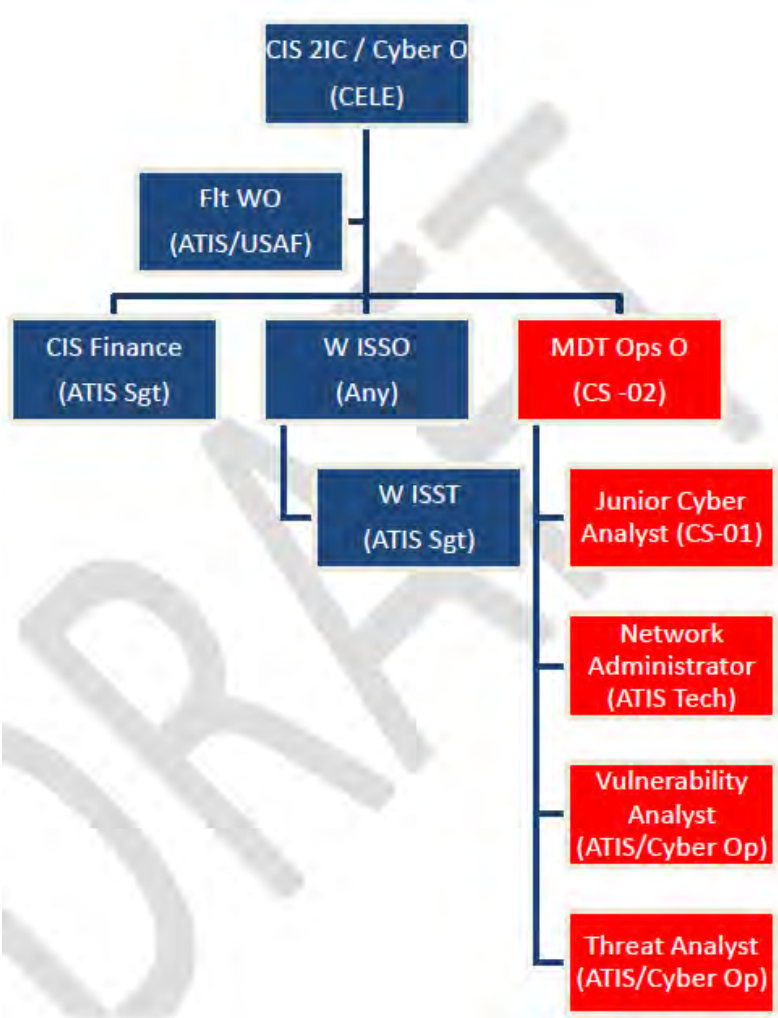

Figure 4.2 – CADS MDT Proposed Organization[148]
Source: Department of National Defence, *DRAFT - Canadian Air Defence Sector (CADS) Mission Defence Team (MDT) Concept of Operations*, 10.

Table 4.2 – CADS MDT Assessment

Factor	Analysis
Integral CMA capacity for FG & FE	- FG and FE are both conducted at CADS given the domestic NORAD mission, i.e. no expeditionary force. Therefore, proposed MDT structure inherently addresses both missions.
Occupational breadth	- MDT is communications branch focused - Detecting and reporting activities are described in context of MDT and Operator responsibilities, i.e., Operator would report "non-baseline" behavior as a detection activity - 22 Wg OSS Intelligence cell is identified as collaborator - Links to NORAD Command Cyber Protection Teams (US Cyber Operators)

[148] Blue positions are existing in the CIS Flight, and red positions are to be created.

Cyber expertise in risk management	- Unique reporting and incident response posture. Reports to NORAD/USNORTHCOM Cyber Domain Chief in addition to following CONPLAN LADON.[149] - MDT is responsible to recommend containment and mitigation of an incident - MDT responsible to maintain incident response procedures, but not explicit that this is to include deliberate risk management - No description of initiating of risk management activities to 1 CAD or NORAD operational authorities. - MDT Vulnerability Analyst position task includes "technical and nontechnical (evaluation of people and operations) risk and vulnerability assessments of relevant technology" and security controls to mitigate risk.
Standards and evaluation	- CONOPS does not mention establishment or maintenance of standards, or an evaluation process. - NORAD does perform routine evaluations and cyber exercises, but documentation is not available at unclassified level.

Source: Department of National Defence, *DRAFT - Canadian Air Defence Sector (CADS) Mission Defence Team (MDT) Concept of Operations*, 1-14.

The strengths assessed by the case study at Table 4.2 are the integral capacity of the CADS MDT to support FG and FE missions, occupational breadth, and standards and evaluation to a limited extent. Given that the CADS mission is non-expeditionary, the static force structure of the MDT is sufficient for FG and FE. While the MDT does not include any of the defence system operators, the ATIS technicians who already have a maintenance responsibility for these systems provide system expertise related to vulnerability and threat assessment. Operator training and responsibility in incident reporting further mitigate the lack of operator involvement; however, the risk in this approach is that CMA will be seen as the exclusive responsibility of the communications and electronics branch. Finally, NORAD exercises incorporate cyber considerations in order to ensure mission readiness. However, the extent to which this covers standards and evaluation for CMA has not been fully assessed.

[149] Maj Rebecca Peitzsche (22 Wg OC CIS Flt), email conversation with author, 19 March 2021

In order to improve on the strengths of the CADS MDT, there is a requirement to expand upon roles and responsibilities related to risk management. The CONOPS provides almost no information on incident response, reporting, and initiation of the risk management process which is central to CMA. While a flowchart depicting incident response was provided, the emphasis of these activities are on functional Response and Recovery, without description of command risk acceptance or involvement.[150] It is thought that this lack of emphasis may be an artefact of the authors of the document, given that risk management tools such as the RARM and ORAT are less frequently used in this occupational branch. Given that these processes will be defined at the operational level, the observation is that the MDT needs to identify who at the tactical level is responsible for conducting these assessments and clarifying the associated communication and reporting chains. In relation to this observation, given the maturity of cyber expertise in the NORAD Command, there may be existing processes or supports that could leveraged by the MDT related to risk management and incident reporting. Further, the CONOPS could be used to centralize these key references while the team is in development.

In summary, the CADS MDT Case Study analysis shows an organizational construct and CONOPS solidly grounded in cyber doctrine, and supported by existing expertise in the organization. There is clear consideration for the internal, tactical level responsibilities of the MDT, but expected outward facing activities and communication linkages are not described. The CONOPS depiction of both CMA and DCO-IDM activities highlights possible efficiencies that can be exploited at CADS and elsewhere, while ensuring coverage for CFNOC's current IT system focus.

[150] Maj Rebecca Peitzsche (22 Wg OC CIS Flt), email conversation with author, 25 March 2021

1 CAD Cyber Team

As previously introduced in chapter three, 1 CAD is the operational level headquarters for the RCAF. It is mandated to ensure RCAF readiness through FG, and also enables FE when Comd 1 CAD is acting as Comd CANR, the JFACC or the regional SAR commander. To effectively conduct these critical responsibilities, there is a need for 1 CAD to integrate CMA into planning, readiness, and execution of operations. Further, as a higher-level headquarters, 1 CAD is expected to establish policy and processes for tactical level implementation.

The proposal for a 1 CAD Cyber Team follows the multi-role construct of the 1 CAD staff, whereby the Cyber Team is organized along functional lines to enable and support the JFACC, Comd 1 CAD, and Comd CANR. The area of responsibility expands on the doctrinal definition of CMA to include mission assurance for IT, OT and PT through cyber security, cyber planning, and cyber operations.[151] The proposal deliberately identifies alignment of existing staff expertise to their associated systems for cyber security and risk management. For example, the A6 and Aerospace Readiness provide CMA support for the NORAD Battle Control System, Tactical Data Links, and other Radio Frequency communications typically associated with the communications and electronics branch. Similarly, the A4 Maint and Fleet Readiness provide CMA support to aircraft and onboard weapon systems, directly linking aircrew and maintenance branch personnel to their existing area of responsibility. Completing the triad, OT is addressed by A4 CE and A6 with support for such systems as physical security, utilities monitoring and supervisory control and data acquisition (SCADA). These system experts will also be relied upon for support to A2/A3/A5 staff's cyber operation planning and execution. While cyber operations

[151] Maj Kim Kieres (1 CAD), email conversation with author, 5 March 2021

are expected to grow, the majority of all cyber activities are expected to be related to readiness and CMA.[152]

At current time, this proposal is in the planning stages and, while an activity described by the 1 CAD CMA Roadmap, is not yet supported by a formal concept of operation, employment, or task list.[153] The plan is in development by personnel in the communications and electronics branch, and clearly identifies the need for operation and system expertise in the advancement of its development and implementation.[154] Further, it recommends that ultimate responsibility for the program must be with the operations; this reflects RCAF doctrine that a commander holds operational responsibility for all risk. The next step in the refinement of the program is Comd 1 CAD concurrence, and staffing the representative positions by the 1 CAD directorates for the needed cross-functional expertise.[155] The proposed organization is provided at Figure 4.3.

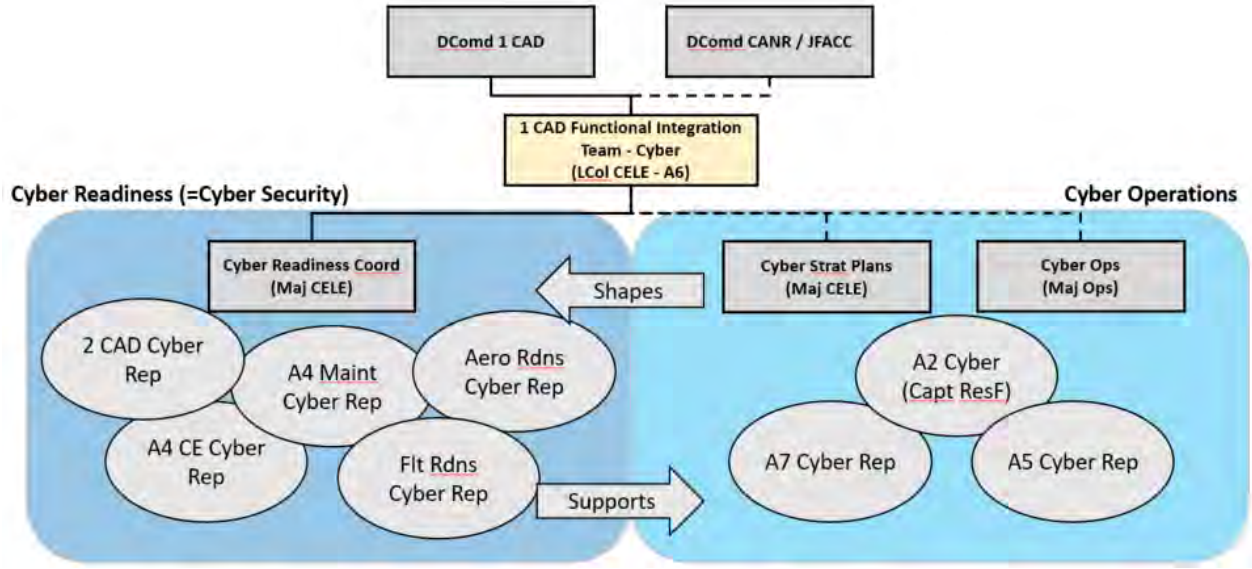

Figure 4.3 – 1 CAD/JFACC/CANR Cyber Team (Interim) v5
Source: Maj Kieres, Email conversation with author, 7 April 2021.

[152] Ibid.
[153] Canada. 1 Canadian Air Division, *1 CAD / CANR / JFACC Cyber Mission Assurance (CMA) Overview and Brief* (Winnipeg: DND Canada,[2020]).
[154] Maj Kim Kieres (1 CAD), email conversation with author, 5 March 2021
[155] This is expected to require additional personnel in the long term, i.e. not "PY neutral". Maj Kim Kieres (1 CAD), email conversation with author, 1 April 2021.

Table 4.3 – 1 CAD Cyber Team Assessment

Factor	Analysis
Integral CMA capacity for FG & FE	- Cross-functional team which relies on collaboration, vice reporting relationships - Unclear of what responsibilities and tasks will be assigned to cover NIST Framework functions. - Unclear if technical expertise will be available to assist in Respond and Recover activities.
Occupational breadth	- Clearly covers all areas of expertise for IT/OT/PT within 1 CAD responsibility.
Cyber expertise in risk management	- As the organization receiving tactical level incident reports, there is no information or description of authority, accountability and responsibility for risk management. - No information on RARM and ORAT use.
Standards and evaluation	- No integration of a standards and evaluation team as a stakeholder in "Cyber Readiness" portion of functional organization. - Cyber learning and training objectives for the 1 CAD HQ are ongoing to support readiness.

Source: Maj Kieres, Email conversation with author, 5 March 2021

As Table 4.3 demonstrates, there is very little information available to analyze the 1 CAD Cyber Team proposal. At this time, the principal strength identified is that the proposal has a general framework for how it will operate, but seeks to include the respective functional experts in the detailed development of the 1 CAD Cyber Team's responsibilities and CONOPS. Further, the proposal includes 2 CAD as a key stakeholder in moving the CMA Program forward, which matches the earlier assessment of a need to develop cyber competencies across occupations at the Tactical and Operational levels. Finally, the proposal is aligned to the cyber doctrine and the team's development is an identified step from the 1 CAD CMA Roadmap.[156]

From the available documentation, the weakest link of the 1 CAD Cyber Team proposal appears to be the lack of reporting relationships, and therefore accountability, for designated "Cyber Reps" within the identified 1 CAD directorates. This organization acknowledges the

[156] Ibid.

shortfall of personnel, and the challenges surrounding creating new positions, but it is expected to have substantial challenges in respect to capacity and prioritization of CMA activities without command influence. Another important gap for the Team, related to the Identify function, is the assignment of authority, accountability and responsibility related to the RARM, ORAT and MALA risk management processes, inclusive of the previously proposed adjustments to align for CMA. Relative to this observation, it is recommended that the Fleet Readiness Cyber Rep pre-coordinate with the Operational Airworthiness staff. As the proposal for the 1 CAD Cyber Team does not address the four factors for analysis, it is recommended that these be considered as a supporting framework for future development of the Team with the identified stakeholders. Critical to this development effort is the consideration for how the operational level will control and communicate with the tactical level in respect to Protect, Detect, Respond and Recover.

RCN Fleet Cyber Team

The RCN is tasked to "generate combat-capable, multipurpose maritime forces" in support of CAF missions at home and abroad.[157] Supported by the Naval Staff Headquarters, the Maritime Forces Pacific and Maritime Force Atlantic formations generate, sustain and employ an armed force for their respective coast. As such, the majority of all naval PT, operators and support personnel are located at these two bases. Like the RCAF, the RCN is fundamentally reliant on PT to accomplish its mission, emphasizing the need for a CMA team with system expertise.

The RCN Fleet Cyber Team (FCT) construct is part of a holistic RCN Cyber Strategy which guides cyber force development, generation and employment through 2025.[158] The

[157] "About the RCN," DND Canada, last modified Feb 11, 2019, accessed Mar 28, 2021, http://www.navy-marine.forces.gc.ca/en/about/index.page.

[158] Government of Canada. Department of National Defence, *DRAFT V1.5 - Fleet Cyber Team CONOP* (Ottawa: DND Canada,[2021a])., 1.

comprehensive approach of the RCN explicitly considers the existing IT support and cyber security activities conducted by naval Network Operations Centres (NOC), and states that the FCTs shall integrate with their respective coast's NOC.[159] In respect to PT, the strategy clearly describes that naval CMA activities will "directly inform and enable DCO planning and execution" such that these systems may be monitored and defended.[160] Therefore, the FCT's scope of responsibility is focused on PT, and is inclusive of both CMA and DCO-IDM. However, due to CFNOC's focus on CAF-wide enterprise IT systems, it is identified that the FCT will also take responsibility for "shipboard IT networks … and shore-based NOC infrastructure."[161] Further, the RCN describes that these activities are intrinsic to operational readiness, and therefore will be integrated as validation requirements in the readiness state for personnel and materiel.[162]

The FCT's purpose is to provide targeted cyber protection for FE missions and FG of cyber-ready platforms and personnel. They link higher headquarters direction and operational priorities in respect to cyber readiness and cyber resilience of ship and submarine borne technology. In this role, they have a close interface with ADM MAT Director General Marine Equipment Program Management and capital projects (Director General Major Project Delivery) in order to implement the platform protection and cyber risk mitigation strategies developed by these non-RCN departments.[163] In summary, the scope of FCT's functions ranges from "pre-planned deliberate analysis of systems for vulnerabilities, to the continuous in-depth monitoring of systems for threat exploitation, and finally to rapid reaction to cyber incidents."[164] In order to

---

[159] Ibid., 2.

[160] Government of Canada. Department of National Defence, *Royal Canadian Navy Cyber Strategy 2020-2025* (Ottawa: DND Canada,[n.d.]), 13.

[161] Ibid.

[162] Ibid., 14.

[163] Government of Canada. Department of National Defence, *DRAFT V1.5 - Fleet Cyber Team CONOP*, 5.

[164] Ibid., 9.

accomplish these activities, the FCT CONOPS identifies tasks and responsibilities across all of the NIST Framework functions.

The FCT CONOPS, while a draft, is a robust and detail oriented document that ties directly to the Commander RCN's cyber strategy. It was written primarily by Naval Warfare Officers (operators) but includes input from network security personnel (operators with advanced training) on both coasts.[165] While maintenance branch personnel were not involved in writing the CONOPS, they are identified as stakeholders, and the document demonstrates a balance of technical expertise and mission focus.[166] This is best reflected in the general organizational construct, where "cyber experts [are] closely supported by knowledgeable naval system subject matter experts."[167] The organization will typically operate in functional groupings (Figure 4.4), but a classical organization structure is also proposed (Figure 4.5). As of April 2021, none of the positions have been filled, but three Corporal Cyber Operator positions per coast (for a total of six positions) have been allocated, and one Sergeant Cyber Operator position per coast (two additional positions, eight total) will be allocated in 2022. This build-up will be coordinated by the Maritime Component Commander's Cyber Operations staff officer, and will be completed gradually.[168]

[165] LCdr Matthew Bowman (DNIW), email conversation with author, 5 March 2021.
[166] LCdr Matthew Bowman (DNIW), email conversation with author, 23 March 2021.
[167] Ibid., 11.
[168] Ibid., 4.

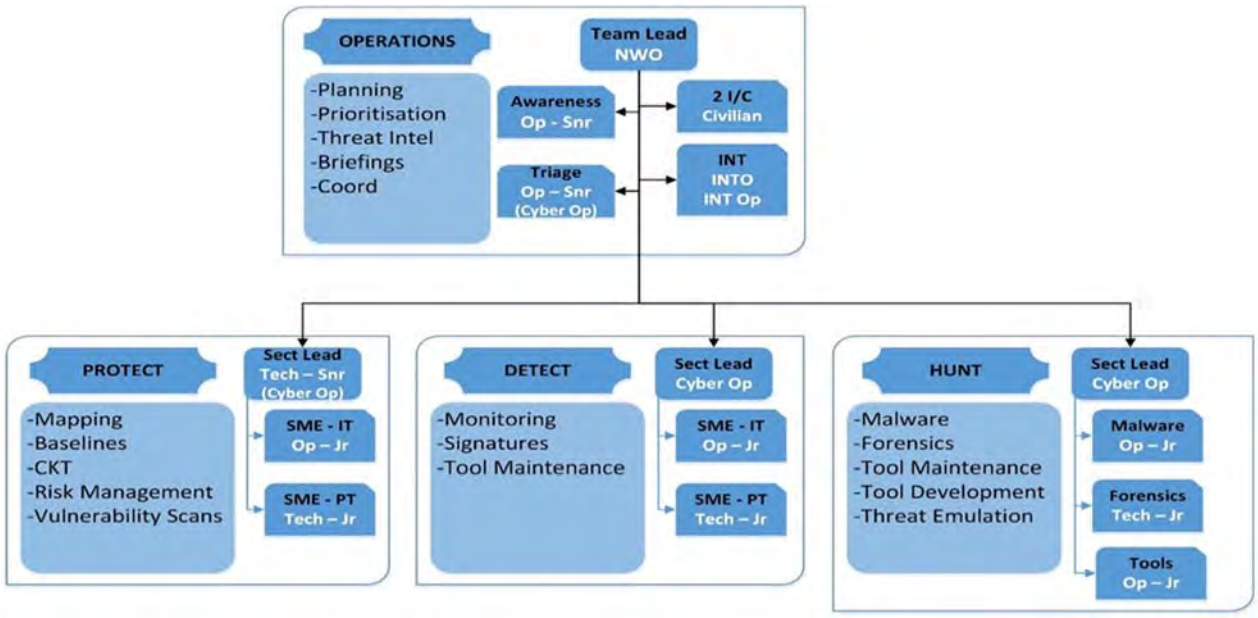

Figure 4.4 – RCN FCT Functional Organization Structure
Source: Department of National Defence, *DRAFT v1.5 - Fleet Cyber Team CONOP*, 11.

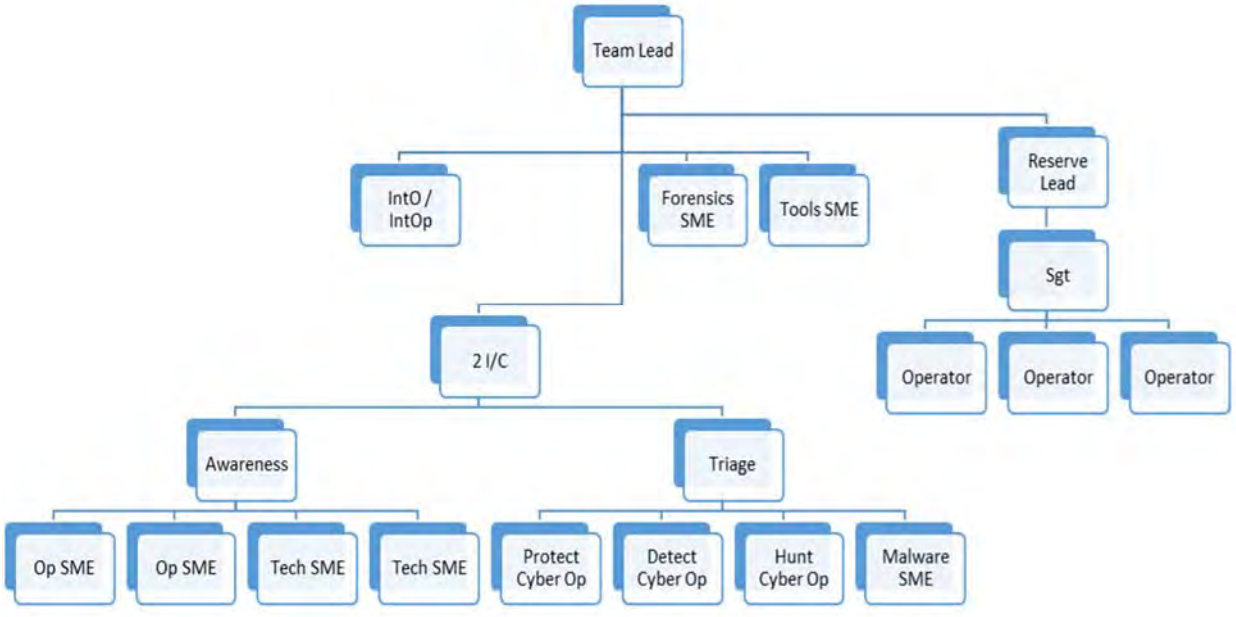

Figure 4.5 – RCN FCT Hierarchical Organization Structure
Source: Department of National Defence, *DRAFT v1.5 - Fleet Cyber Team CONOP*, 9.

Table 4.4 – RCN FCT Assessment

Factor	Analysis
Integral CMA capacity for FG & FE	- A relatively large FCT is established at each coast providing support to their geo-located units. - FCT personnel will be embarked in support of FE and deployments with an identified cyber threat. - Tight integration of FCT and NOC reflects doctrine's "blue cyberspace" coverage from CMA and Net Ops. - Coverage of on-board IT, coordinated with CFNOC. - Responsibility for tasks within all NIST functions.
Occupational breadth	- Organization matches cyber and system experts along functional tasks. - Technical and Operator SMEs cover the two broad groups of naval systems (combat and marine systems) - Intelligence liaison is integrated into team construct.
Cyber expertise in risk management	- Incident reporting chain to be coordinated with DGIMO and Comd RCN, but is not yet developed. - Acknowledges reporting through IS Response Recover
Standards and evaluation	- Cyber readiness verifications to be developed and integrated into CFCD 129 and verified in CFCD 102.

Source: Department of National Defence, *DRAFT v1.5 - Fleet Cyber Team CONOP*, 1-37.

The results of the case study show a thorough planning effort to develop the FCT, and strengths are observed across the four assessment factors. Related to the integral CMA capacity, the RCN FCT has the luxury of developing one large, and robust team on each coast to support the distribution of RCN assets. This creates a deeper pool of cyber and systems expertise, reinforced by occupational breadth, and is supported by the plan to integrate with the NOCs and the Net Ops organizations under N6 staff. Further, it enables the assumed responsibility by the FCT for onboard IT systems to ensure comprehensive coverage of naval systems. While not fully described in the CONOPS, this arrangement is expected to facilitate consistency in cyber incident reporting, flow of communication for threats/vulnerabilities, and generates efficiencies in human resources. Another strength is the assignment of responsibilities across the NIST functions, as well as some DCO-IDM tasks. This is a logical extension of the FCT given the

proposed size of the organization, and its integrated systems and cyber expertise. Finally, the FCT CONOPS plan describes how it will support FG and FE operations both at home and abroad. This is accompanied by a thorough description of the command and control structure, reporting relationships, and accountabilities to higher headquarters for FG and FE operations.[169] Similarly, formal documentation is referenced for reporting readiness measures and incident reporting, although these changes are to be completed.

Few areas of improvement are identified from this proposal; its challenge will be implementation, staffing, and refinement of processes. One specific observation is the need to delineate roles and responsibilities related to risk management, as the current proposal suggests redundancy in reporting channels (DGIMO, RCN, WSM). This is a critical step in the Identify function, and like the RCAF observations, requires control and coordination by the Operational level. Another area for further development, requiring engagement by both the RCN and the RCAF, will be addressing CMA for shipborne helicopters.

In summary, the RCN FCT CONOPS clearly describes the activities, reporting relationships and area of responsibility. This big picture view of how the FCT will function is thought to be sufficient as a starting point for implementation. As personnel are assigned to the FCT in the near future, it is critical that risk management and Respond activities are addressed, as well as the proposed updates to readiness verification standards. With the current staffing efforts aimed at non-commissioned Cyber Operators, there is a risk that the focus of the FCT development will turn from people and processes to technology: established accountabilities, authorities, responsibilities and procedures need to be in place prior to this shift in order for effective control of cyber mission assurance activities.

---

[169] Ibid., 13.

Analysis

As a result of the analysis of these four organizations, several conclusions can be drawn. First, as a strength, each of the organizations considered occupational breadth in their proposals. This reflects an understanding and commitment to treating CMA as an ops-focused, technically enabled, program. However, this need for breadth poses a major challenge, as it equates to a bigger team size, particularly if there is to be depth of expertise for a range of tasks as the RCN FCT proposes. For the RCAF, with significant geographic dispersal of 18 main operating bases, staffing of large CMA-focused organizations is neither practical nor feasible.[170] Therefore, with a balance of organization size and capacity, the conclusion is that CMA support should be provided at the Wing level, or in a large ATF, vice integrated in Squadrons. This also implies a surge capacity is provided elsewhere, as local CMA support will be primarily limited to the Detect function, with some ability to Respond and Recover. In these core functions, as the case studies show, it should also be recognized that there are efficiencies to be gained by accomplishing both CMA and DCO-IDM activities. That being said, with the MDT focused on Detect, their principal accountability in the event of a cyber incident is initiating the risk management process.

This feeds into the second major observation: while each of the studied organizations identified the need to conduct risk management, there was little detail regarding authorities, responsibilities and accountabilities (ARA). As previously mentioned, risk management is the procedural linchpin to the CMA Program. As part of the Identify function, it enables all other functions to occur, and this programmatic guidance should come from higher headquarters.

---

[170] The locations included are: Comox, Patricia Bay, Edmonton, Cold Lake, Moose Jaw, Winnipeg, Trenton, North Bay, Kingston, Petawawa, St-Hubert, Valcartier, Bagotville, Gagetown, Greenwood, Shearwater, Goose Bay, and Gander. "RCAF Map," DND Canada, last modified Jun 18, 2020, accessed Mar 18, 2021, http://www.rcaf-arc.forces.gc.ca/en/rcaf-map.page.

Therefore, these ARAs and processes must be developed and communicated from the Operational level to ensure consistency in command awareness and risk acceptance. Thirdly, standards and evaluation should also be established at the Operational level as a next step towards cyber readiness. However, this is seen as a follow-on activity to the priority of risk management responsibilities and procedures.

A fourth observation from the case studies is a need to describe the interactions and relationships between the MDTs, assessed to be at the Wing level, and the Squadrons which they will support. Uniformly, each of the organizations studied identified a role to play in educating and enabling the operational units, but agreement on the ARAs of the MDT and the Squadrons need to be established. General guidelines on these responsibilities should flow from the Operational level for a baseline level of service, capacity and expertise in cyber risk management.

While not directly related to the case studies, an additional observation is made regarding the lack of a centralized resource for more substantial Respond and Recover activities. As previously discussed in relation to CONPLAN LADON, there are joint resources that may be deployed to assist with a significant cyber event that exceeds local capacity. However, as the RCN FCT recognizes and addresses, the specialist expertise for PT is non-existent. Further, there is a need to share best practices, tactical level tools and techniques, provide support to the dispersed MDTs, and act as a central touch point for 3rd line experts. The RCAF CMA Concept Paper proposes that these integration activities be centred at a 2nd line tactical level at the proposed "RCAF Cyber Mission Assurance/Resiliency Operation Centre (RCMAROC)."[171] The multitude of responsibilities proposed for the RCMAROC are enumerated in the Concept

[171] Canada. Royal Canadian Air Force, *RCAF Concept Proposal: RCAF Cyber Mission Assurance V2.4* (Trenton: DND Canada,[2018]), 5.

Proposal and are assessed as necessary, and currently unattributed for at the joint level, or in the proposed tactical and operational level organizations.[172]

Conclusion

The case studies provided a view into current plans by the RCAF in the force development of the CMA Program. Their relevance is tied to the fact that they are grounded in the reality of current staffing and experience constraints. Further, they offer an expansive view of the topic since they were largely developed in parallel by authors with widely varying backgrounds. Despite this diversity, common themes are apparent, highlighting their importance as broadly applicable conclusions for CMA organizations. It is these themes that the next chapter leverages, alongside the case study analysis factors, in order to derive a baseline tactical level organization and a more tailored operational level organization.

[172] Ibid.

CHAPTER 5 – RECOMMENDATIONS AND CONCLUSION

Introduction

This chapter will describe the proposal for a permanent organizational structure in the RCAF at the tactical and operational levels to command, control and conduct cyber mission assurance. The development of these organizations leverages each of the preceding chapters, drawing on the primary and collateral factors necessary for a CMA-focused organization. At both the tactical and the operational level, there needs to be an integral capacity to conduct CMA for both FG and FE, occupational breadth, and appropriate expertise in cyber risk management. Related to standards and evaluation, the tactical level needs to meet the established readiness level; the operational level needs to set these levels and verify their achievement.

At the tactical level, the integral CMA capacity should be established at the Wing, or ATF for expeditionary FE, with a small team (MDT) whose principal focus is the Detect activity, and minor incident Response and Recovery. These organizations need to be tightly integrated with the Squadrons, staffed with both platform and cyber expertise, and hold ARAs reflecting their role in daily operations, and initiation of risk management processes. In order to provide a surge capacity for incident response (Respond, Recover and contribution to Protect functions), a self-contained, deployable organization is recommended at 2nd line of the tactical level. In addition to incident response, this organization, the RCMAROC, would be the integrator of tactical level RCAF CMA activities.

Also residing at the tactical level, but outside the RCAF command and control chain, is 3rd line materiel support at DGAEPM. As is current practice, DTAES and the Weapon System Management (WSM) teams enable technical airworthiness, operational effectiveness and sustainment throughout the life cycle of air and ground-based aerospace systems. Their role in

CMA is therefore most closely tied to Identify and Protect, but they provide subject matter expertise that informs all of the other stages of the NIST framework. Further, they may also provide tools and technology to enable Protection, Detection, Response and Recovery. Organizational changes in DGAEPM related to CMA have already occurred, such as the cyber team in DTAES 8, and WSMs have already been directed to accomplish cyber security activities related to airworthiness.[173] Therefore, ARAs for DGAEPM will be discussed but no further organizational change is proposed.

The operational level needs to be the driver of policy, procedures and ARAs. Therefore, before moving forward to the organizational laydown, high-level recommendations related to process will be provided. The organizational structure at the operational level should be cross-functional with clear accountabilities and reporting chains. Its focus will be principally be on Identify, as well as direction related to Protect, Detect, Respond and Recover through deliberate and contingency planning. This organization will provide command guidance and reach-back expertise to the dispersed MDTs, reflecting the tenet of centralized control and decentralized execution. It will also set readiness standards, and conduct verification activities.

Tactical Level Organizations

In the near term, it is expected that MDTs will be required at each of the main operating bases for the RCAF in order to provide a blend of cyber, fleet and system specific expertise. While there may be some opportunities for a reduced footprint at secondary main operating bases, such as Comox for the CP140, the assessment shows that a minimum footprint must be available on-site to provide support to the operational units. In support of flying squadrons, the CP140 MDT-C construct is used as a template at the Wing level, with breadth and depth added

[173] DTAES Canada., *Technical Airworthiness Authority Advisory 2019-03* (Ottawa: DND Canada,[2019]).

to cover additional fleets and the expected CMA activities (Figure 5.1). It is assessed that the MDT should reside within the Operational Support Squadron (OSS), and while an MDT Lead is identified for the tasks of liaison and risk management accountability, a trade and rank are not provided. For a flying-squadron heavy Wing, it is suggested that the trade should be an AERE to account for cyber airworthiness considerations. For other Wings, a CELE, operator, Cyber Op, or a technical occupation with suitable experience, knowledge and rank could fill the role. Not included in this assessment is which positions may be suitable for reservists, but it is expected that as a bare minimum the MDT and fleet leads must be staffed full-time.

There are several special cases which need to be considered outside of this general construct for MDT support to flying squadrons. These are enumerated, but not developed here, as an area for future research. Aircraft which have an exclusively contracted maintenance support solution, such as the CH149, CC144, BE-350 and training fleets at 2 and 3 Canadian Forces Flying Training Schools, will require an alternate means of support to the extent that they are included in the CMA program.[174] Similarly, the proposed construct may need adaptation for globally-managed fleets like the CC177, or future fighter, given restricted intellectual property rights and global fleet configuration control.

The CH146 Griffon, given numerous small operating locations across the country for Search and Rescue, Combat Support and Tactical Aviation, may have “hubs” for CMA support at larger bases, such as Edmonton, Valcartier and Gagetown.[175] These locations would provide CMA support to nearby satellite locations, for example: Edmonton supports Cold Lake. Another

[174] The requirement is exclusively for operational risk management as derived from the Cyber Key Terrain Analysis (CKTA), as all fleets are already subject to airworthiness regulations for cyber threats to safety of flight.

[175] "RCAF Map," DND Canada, last modified Jun 18, accessed Mar 18, 2021, http://www.rcaf-arc.forces.gc.ca/en/rcaf-map.page. Use and basing of CH146 helicopters for search and rescue and combat support is under a long term transition and will need further assessment as their operating locations evolve.

alternative for the CH146 fleet could be for 400 Squadron in Borden, with a mandate for 1st and 2nd line maintenance, to provide CMA support to squadrons nation-wide. Both of these options would more closely resemble the FCT concept employed by the RCN, providing a larger, centralized team for fleet CMA support.

A similar situation arises for the CH148, which are principally embarked on RCN ships for FE. Here it is suggested that RCAF technical expertise could be embedded within the RCN FCTs as collaborative support to maritime assets. Finally, some legacy fleets, such as the CC130H for Search and Rescue or Air to Air Refuelling, CC138 Twin Otter, or the CT144 "Snowbirds" have minimal routes for cyber vulnerability, or a short remaining service life, that may exclude them from operational cyber risk management. The priority, or exclusion of certain systems, is considered by the Cyber Key Terrain Analysis.

In addition to support for aircraft fleets, there is a need to support ground-based aerospace PT. Examples of this are the tactical control radars (TPS70), mobile air traffic management system (MPN25), fixed air traffic management systems and navigational aids, the North Warning System (NWS), and other radar and communications equipment. With the exception of the major NORAD assets (CADS, NWS), it is proposed that CMA support for these systems be rolled into a Wing MDT structure. In this sense, ground based systems are treated similarly to a flying squadron providing for uniform CMA support from a single on-Wing organization. In addition to the generic Wing laydown (Figure 5.1), a sample of what this could look like for 8 Wing Trenton is provided as an example at Figure 5.2. Given the unique structure and role of CADS, it is recommended that the MDT proposal covered in chapter 4 is implemented as a component of the CIS Flight, with an additional consideration for closer

integration with operators. Finally, CMA support to the NWS is not studied here, and is identified for future research or as a component of the NORAD modernization program.

Finally, the 2nd line supporting organization (RCMAROC) should be established at one of the larger, multi-fleet Wings. 8 Wing Trenton is proposed as it is home to five aircraft fleets, 8 Air Communications and Control Squadron (8 ACCS), Aerospace and Telecommunications Engineering Support Squadron (ATESS) and the RCAF Aerospace Warfare Centre.[176] Given the existing, specialized technical support and production services provided by ATESS, it is a logical fit for the RCMAROC; however, further study and development of its organizational structure is needed as part of the CMA force development effort.[177]

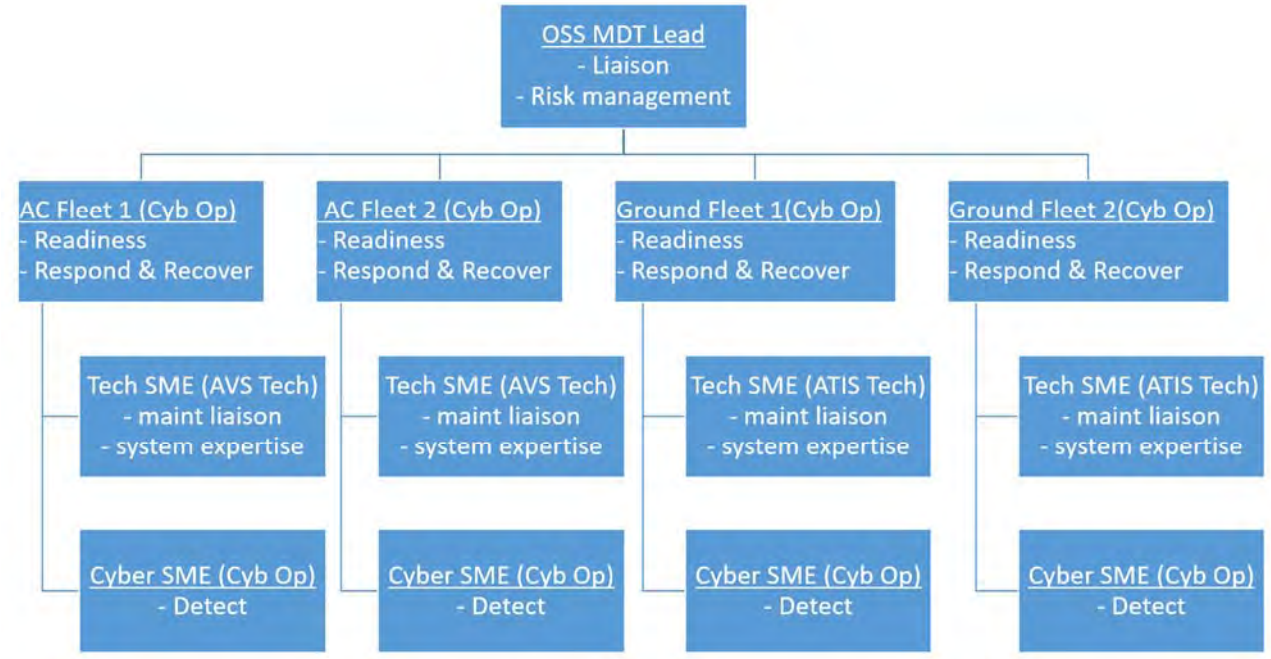

Figure 5.1 – Generic Wing MDT Laydown

[176] "RCAF Map," DND Canada, last modified Jun 18, accessed Mar 18, 2021, http://www.rcaf-arc.forces.gc.ca/en/rcaf-map.page.

[177] ATESS has been discussed as the probable location for the RCMAROC by various stakeholders in CMA force development efforts. Capt Alec Harlow (415 Sqn), telephone conversation with author, 12 February 2021.

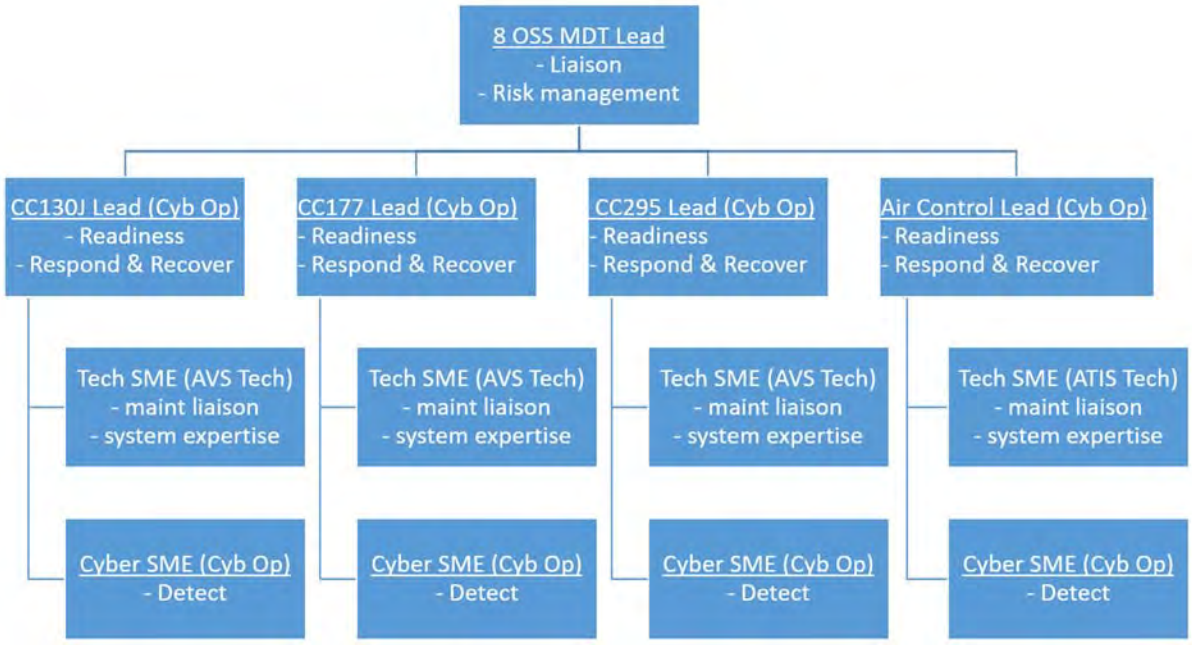

Figure 5.2 – Example 8 Wing MDT Laydown

Note: CH146 and civilian maintained fleets are excluded from this potential force laydown

Operational Level

The interim recommendation for a cross-functional 1 CAD Cyber Team meets many of the CMA organizational considerations. While there is some informal documentation on how the team will function, it presently lacks substantiation on applicable policy, procedures and ARAs. Given that the activities and reporting conducted by the tactical level are driven by an understanding of the expectations and command direction from higher headquarters, it is critical that these are established before moving forward with an organizational design. To align with doctrine, as well as operational level responsibilities proposed for the RCN FCT, the NIST Framework will be used for these process-based recommendations.

Related to the Identify function, 1 CAD has authority to manage the RARM, ORAT and MALA risk management processes. Relative to CMA, the RARM and ORAT are suitable as proposed to encompass cyber risks within their respective airworthiness and operational risk

management framework. However, to align with these existing risk assessment frameworks, there should be an assignment of authority for the tactical level to maintain and update the MCAAV tool by fleet. DGAEPM, specifically the WSM, should be ultimately responsible for maintaining the MCAAV database on behalf of 1 CAD. All cyber risk assessments will be predicated on this tool to ensure a holistic view of the fleet's vulnerabilities by mission. The operational level retains its accountability for risk acceptance as delineated by existing RARM and ORAT policy. For the MALA, as identified in chapter three, there are no proposed changes to ARAs, but updates are required to incorporate cyber considerations. This may or may not involve the MDT in providing MCAAV assessments under certain operational conditions. These proposed changes do not drive an organizational change at the operational level, but they are a touch-point with the Wings and ATFs, and should be considered in the list of tasks for the 1 CAD Cyber Team.

The Detect function will be principally executed by the tactical MDTs.[178] However, 1 CAD Cyber Team has a role in determining to what extent this capacity must be forward deployed when planning expeditionary operations. Similarly, they need to manage and understand the various capacities that each Wing or ATF possess, as it is expected that these will vary according to fleet designations in the CKTA. Iterations of the CKTA as part of the operational planning process may be necessary to help determine the organizational size and responsibilities of a deployed MDT. ARAs related to updating the CKTA need to be documented.[179] In regards to operational planning, the ARAs remain unchanged for 1 CAD, but underscore the importance of a cross-functional team with cyber expertise that is able to advise

[178] It is expected that CFNOC will also have a role, particularly if data feeds are able to be centralized. Maj Kim Kieres, email conversation with author, 1 April 2021.

[179] Discussions with Maj Kim Kieres indicate that these are going to be the responsibility of the Cyber Plans and Cyber Ops officers in the 1 CAD Cyber Team. A draft CADO is in progress to this effect.

on available CMA support capacity and existing risk assessments for ground and air-based equipment.

Protect is primarily accomplished by DGAEPM through built-in security on RCAF air and ground platforms and 1st line maintenance, i.e. patching. 1 CAD responsibility again remains related to command risk acceptance of technological solutions that maintain the approved risk level by mission on a given system. When Protect activities are required as risk mitigation, 1 CAD holds the responsibility to authorize these activities. Protect can also be thought of as verifying readiness, which has been recommended for implementation through the existing 1 CAD SETs. 1 CAD owns both the FG readiness standards, and the teams which will conduct the verifications.

Respond and Recover are linked, with the majority of minor incidents covered by the tactical MDTs. Significant cyber incident Response and Recovery is supported by the proposed 2nd line tactical organization (RCMAROC). The proposed MDTs and RCMAROC are under the 1 CAD chain of command and therefore ARAs for mitigating activities in Respond and Recover can remain unchanged from existing risk assessment authorities (RARM, ORAT). Throughout all Respond and Recover activities, the MDT should remain the conduit to the operational level in order to maintain consistent ARAs and reporting chains for all incidents, as well as ensure fleet/system-specific expertise.

From these function based assessments, there is a clarification of ARAs identified, particularly in assigning responsibilities to the MDTs and coordinating with DGAEPM. Few of these translate into actual organizational change, but they add additional tasks and responsibilities to inform and support ARA holders. While the proposal for an organization structure is provided for steady-state implementation of CMA, it is acknowledged that more

resources may be required to implement these changes than to maintain them once established. Given personnel staffing challenges, these are expected to be accomplished through prioritization vice temporary increases in personnel.

The two directorates most affected by the aforementioned tasks are Aerospace Readiness and Fleet Readiness. These directorates own the staff officers with operational expertise on the affected systems, and they are the touch point for input or development of RARMs and ORATS. In the implementation of CMA, it is expected that they will draft MALA changes for their reflective fleets. Further, they will likely be stakeholders in establishing readiness criteria by fleet for standards and evaluation. Finally, Fleet Readiness holds operational airworthiness responsibilities, and therefore owns the responsibility to ensure that OAA considerations are incorporated in cyber readiness and risk management processes.

Drawing on these process-driven recommendations, adjustments to the 1 CAD Cyber Team organization are provided in Figure 5.3 in red. Not depicted in this figure is the command and control relationships. Each of the Cyber representative (Rep) are proposed to be retained by their respective Director, while the Cyber Readiness Coordinator (Coord) reports directly to the 1 CAD Functional Integration Team – Cyber. Prioritizing assignment of these personnel will need to be command driven, but it is assessed that there are insufficient personnel to have directly assigned resources that report to the Cyber Readiness Coord. The Cyber Plans, Cyber Operations and A2 Cyber positions report directly to A3, A5 and A2 respectively, with a coordinating relationship to the Functional Integration Team – Cyber and Cyber Readiness Coord. Finally, for consistency with joint cyber organizations, it is proposed that the term Cyber Component Coordination Element - Air (CCCE – Air) be assigned to the Ops and Plans cell, as while they

report to the JFACC, they have a critical coordination responsibility with JFCCC for cyber operations and FE considerations.

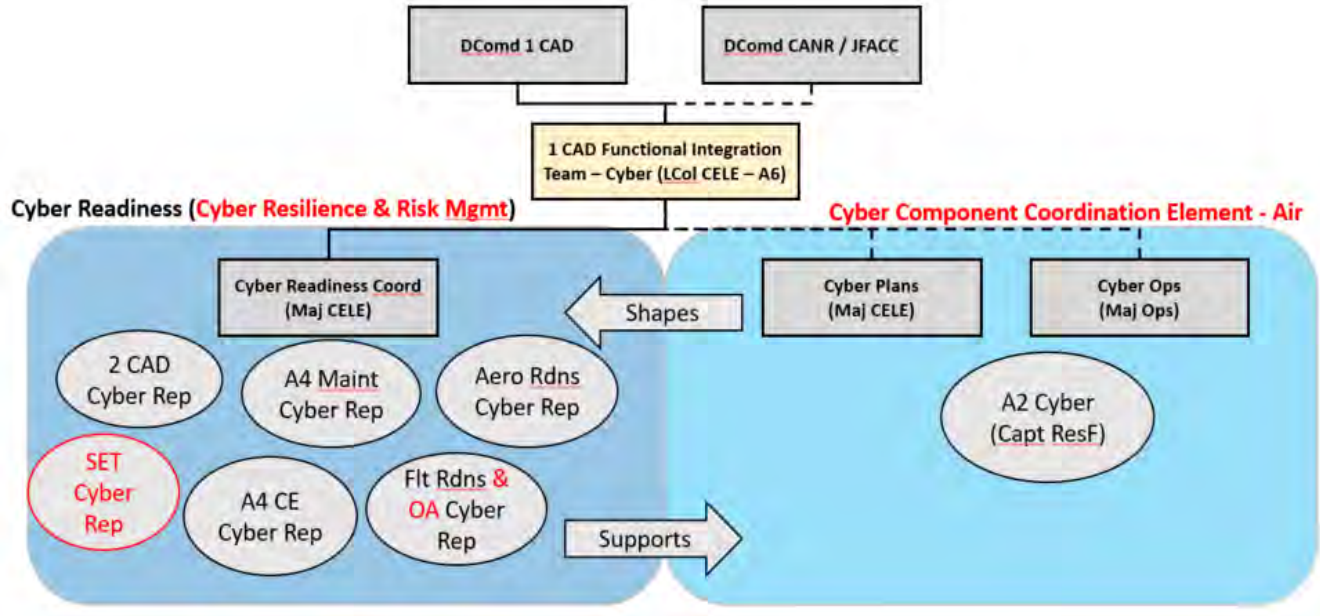

Figure 5.3 – Proposed 1 CAD Cyber Team Laydown

Areas for Further Study

The proposals presented in this chapter are representative of organizational structures that will enable steady-state CMA in the RCAF. Excluded from this assessment, although discussed in earlier chapters is the road to implementing the program and achieving maturity. Key considerations for this transition is the need to educate RCAF members on CMA, and to ensure cyber is integrated as a component of occupation training in addition to position-specific competencies. At current time, the management of key CMA positions is accomplished through employing those with existing knowledge, and advanced training through short-courses.[180] While this has allowed early cyber force development efforts to be pursued, it is insufficient for long-

[180] LCdr Matthew Bowman (DNIW), email conversation with author, 23 March 2021. Simon Larocque (DTAES), telephone conversation with author, February 8, 2021.

term program success. Existing training needs assessments, such as that conducted for DGAEPM, need to be implemented and other training needs assessments should be conducted to ensure that technical, operator and supporting trades in the RCAF are sufficiently prepared to operate in the cyber-contested environment.

When training has been implanted through occupation and professional development, the next challenge is a cultural change for cyber-awareness. Much like the evolution that has occurred with Flight Safety since the 1960s, there will need to be an acceptance and ownership of the responsibility for cyber security and resiliency by all members of the RCAF.[181] While the research in this paper shows that command and staff levels of the RCAF have begun to understand that CMA is an operationally driven program, further research is needed to describe how this shift can be accomplished across the organization.

Another area for further development is determining a division of responsibilities and competencies for OT and PT with CFNOC. Clearly described in their Concept of Operations is the scope to conduct DCO-IDM pan-CAF, but the capacity and expertise to achieve this is not yet present in the organization. A solution, such as that envisioned by some of the organizational case studies, is that the RCAF will own DCO-IDM responsibilities and leverage existing platform subject matter experts for this purpose. While this is anticipated to be an efficient means for conduct, further research is needed in this area.

A final area not explored in this paper is the ability to shift MDT responsibilities away from geo-located support on Wings to operations to a remote and centralized location. While this could achieve substantial savings in terms of personnel, as the central RCN FCT demonstrate, the ability to conduct Protect, Detect, Respond and Recovery activities from a distance is not yet

[181] "Flight Safety - Royal Canadian Air Force," DND Canada, last modified Oct 11, accessed Apr 13, 2021, http://www.rcaf-arc.forces.gc.ca/en/flight-safety/index.page.

feasible. First, secure, cloud-based computing for the CAF is not yet implemented, and therefore the ability to upload, process and analyze data from air and ground-based systems is not technically supportable. Second, for the aforementioned reasons of training and establishment of a cyber-aware culture, the MDTs have an implied task to champion the CMA programs locally. This need was clearly acknowledged by each of the case studies, and explains why the proof-of-concept organizations are co-located with their supported fleets. In the near term, this is thought to be necessary for CMA Program success.

Conclusion

The CAF's CMA program enables continuous risk management for physical assets against persistent and constant cyber threats. While the majority of these threats have effects that are below the threshold of the LOAC, the ability to Protect, Detect, Respond and Recover is crucial to maintaining freedom of action and assuring mission success. Further, there is a need to Identify the policy and processes that guide the CMA program. This paper assessed that there are currently gaps in the RCAF's ability to conduct all five functions: Identify, Protect, Detect, Respond and Recover. To achieve lasting competency and capacity for CMA in the RCAF, it was proposed that ARAs related to their conduct, and cyber expertise, must be embedded in a permanent organizational structure that spans the operational and tactical levels.

Supported by a review of RCAF C2 doctrine, existing risk management authorities, and cyber force structures at the joint level, it was assessed that the Identify function is principally the responsibility of the operational headquarters at 1 CAD. The tactical level should have primary responsibility for the Detect function, as well as an initial capacity to Respond and Recover. An enhanced ability to Respond and Recover should be a tactical level, as a 2nd line responsibility, while 3rd line (DGAEPM) holds the principal responsibility for Protect. Finally,

risk acceptance and the capacity to set standards and evaluate their achievement of the functions must remain at the operational level.

Following these recommended broad assignments of authority, numerous conclusions were drawn in regards to criteria for success in steady-state, CMA-focused organizations. From doctrine and theory, it was assessed that a CMA-focused organization requires: an integral CMA capacity for FG and FE, occupational breadth, cyber expertise in risk management, and established and verified standards. From a case study analysis of proof-of-concept CMA-focused organizations against these requirements, several organizational conclusions were drawn. First, that a CMA-focused organization should be embedded at the Wing, or large ATF, level. Secondly, there is a need for clear lines of communication and delineation of ARAs between all stakeholders: squadrons, CMA-focused organizations, and the operational level HQ. Thirdly, there remains a significant gap in the operational level's development of the Identify function: principally the associated ARAs for cyber risk management.

As the cyber force development process matures, and each of the proof-of-concept organizations are staffed and begin operations, it is expected that further lessons will be learned for successfully integrating CMA into the RCAF. In support of these efforts, this paper has proposed organizational structures that support the RCAF CMA Program at steady-state: a vision of what the RCAF could look like in five to ten years. This includes a cross-functional Cyber Team at the 1 CAD headquarters which has described the processes and ARAs of CMA, and ensures their implementation at both the tactical and operational levels. For the tactical level Wings and ATFs, it is the establishment of an organization with dedicated cyber and technical experts working together to provide the necessary knowledge and capacity for CMA. The sum of these dedicated personnel and organization structures will form the backbone of CMA,

facilitating the application and implementation of processes and technology to ensure the RCAF's freedom of manoeuvre in today's cyber-contested environment.

APPENDIX 1 - GLOSSARY

Cyber Domain. All infrastructure, entities, users and activities related to or affecting cyberspace. (DTB 694360)

Cyber Mission Assurance (CMA). A subset of Mission Assurance that focuses on the ability of an organization, service, infrastructure, platform, weapon system, and/or equipment to operate and accomplish their mission in any cyber contested domain. (DTB 695102)
Note: CMA is differentiated from Offensive and Defensive Cyber Operations by the characteristic that it is a risk management activity instead of an operation conducted in cyberspace.

Cyberspace. The global domain consisting of interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process store or transmit data. (DTB 694338)

Cyberspace Resilience. The overall technical and procedural ability of systems, organizations and operations to withstand cyber incidents and, where harm is caused, recover from them with no or acceptable impact on mission assurance or continuity. (DTB 695811)

Defensive Cyber Operations (DCO). A defensive operation conducted in or through cyberspace to detect, defeat and/or mitigate offensive and exploitive actions to maintain freedom of action.
Note: A defensive cyber operation may include internal defensive measures and response action. (DTB 693742)

Defensive Cyber Operations – Internal Defensive Measures (DCO-IDM). In defensive cyber operations, measures and activities conducted within one's own cyberspace to ensure freedom of action. (DTB 694340)

Information Technology (IT). Involves both technology infrastructure and IT applications. Technology infrastructure includes and equipment or system that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information. IT applications include all matters concerned with the design, development, installation and implementation of information systems and applications to meet business requirements. (DTB 3161)

Mission Assurance. The security and resilience of systems and capabilities for mission success. (DTB 695221)

Offensive Cyber Operations (OCO). An offensive operation intended to project power in or through cyberspace to achieve effects in support of military objectives. (DTB 693752)

Operational Technology (OT). Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise. (DTB 695664)

Platform Technology (PT). Hardware and software on ships, aircraft, vehicles, weapon systems and equipment that monitors and/or controls data, power, command and control, surveillance, fire control, navigation, propulsion, maintenance, training and other fundamental functions of the system. (DTB 695775)

Resilience. The ability to recover from adverse effects. Note: Resilience is a factor of survivability. (DTB 695250)

Risk-based Cyber Mission Assurance Process (RCMAP). Mission-focused risk management process that identifies mission criticalities and their relations to the systems and the cyber domain, assesses risks and guides cybersecurity decisions to achieve resilience in the event of cyber-attacks.

Security. The condition achieved when DND and CAF personnel, information, assets and resources are protected against espionage, sabotage, subversion and terrorism, as well as against loss or unauthorized disclosure. (DTB 43546)

Additional Definitions from JDN 2017-02 *Joint Doctrinal Note on Cyber Operations*

Cyber Security Event (level 1). Cyber vulnerabilities and potential actions and/or effects that are a matter of security rather than defence. (p 3-8)

Cyber Security Incident (level 2). Cyber events that result in the compromise of a GF IT systems that are a matter of security rather than defence (p 3-9)

Significant Cyber Incident (level 3). Cyber events or incidents than can impact or have the potential ot impact military operations, therefore making them a defence matter. (p 3-9)

Cyber Attack (level 4) – Cyber actions and/or effects that are a matter of national defence and are within the parameters of the LOAC. (p 3-9) Note: LOAC defines *attack* broadly as an act of violence against the adversary, whether in offence or defence. (p 3-8)

BIBLIOGRAPHY

Albright, Brannan, and Walrond. *Did Stuxnet Take Out 1000 Centrifuges at the Natanz Enrichment Plant*. Washington: Institution for Science and International Security, 2010. https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf.

Barnes, Pux. *Command Or Control? Considerations for the Employment of Air Power in Joint Operations*. Trenton: Canadian Forces Aerospace Warfare Centre, 2014a.

———. "The JFACC and the CAOC-Centric RCAF: Considerations for the Employment of Air Power in Joint Operations." *RCAF Journal* 3, no. 3 (Summer, 2014b): 12-20. http://www.rcaf-arc.forces.gc.ca/en/cf-aerospace-warfare-centre/elibrary/journal/2014-vol3-iss3-04-the-jfacc-and-the-caoc-centric-rcaf.page.

———. *Mission Command and the RCAF: Considerations for the Employment of Air Power in Joint Operations*. Trenton: Canadian Forces Aerospace Warfare Centre, 2014c.

———. *The RCAF Air Task Force: Considerations for the Employment of Air Power in Joint Operations*. Trenton: Canadian Forces Aerospace Warfare Centre, 2014d.

Brent, Laura. "NATO's Role in Cyberspace." NATO. Accessed Apr 13, 2021. https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html.

Bryant, William D. *International Conflict and Cyberspace Superiority: Theory and Practice*. Abingdon, Oxon: Routledge, 2016. http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=1046692&site=ehost-live&scope=site.

Canada. *Alert AL19-202: Ryuk Ransomware Campaign*. Ottawa: Canadian Centre for Cyber Security, 2019.

Canada. 1 Canadian Air Division. *1 CAD / CANR / JFACC Cyber Mission Assurance (CMA) Overview and Brief*. Winnipeg: DND Canada, 2020.

———. *1 CAD Cyber Functional Integration Team (FIT) - Comd's Updated Guidance*. Winnipeg: DND Canada, 2015.

———. *1 CAD Orders, Volume 3, 3-310. Operational Risk Management for Air Operations*. Winnipeg: DND Canada, 2014.

———. *1 CAD Orders, Volume 5, 5-508. Standardization and Evaluation Teams*. Winnipeg: DND Canada, 2019.

———. *1 Cdn Air Div Cyber Functional Integration Team (FIT) - Comd's Guidance*. Winnipeg: DND Canada, 2012.

Canada. Canadian Centre for Cyber Security. *IT Security Risk Management: A Lifecycle Approach. ITSG-33*. Ottawa: Communications Security Establishment, 2012.

———. *National Cyber Threat Assessment 2020*. Ottawa: Communications Security Establishment, 2020.

Canada. Canadian Forces Network Operations Centre. *Canadian Forces Network Operations Centre (CFNOC) Concept of Operations*. Ottawa: DND Canada, 2019.

Canada. Chief of the Defence Staff. *CONTINGENCY OPERATION PLAN (CONPLAN) LADON - Defensive Cyber Operations - Internal Defensive Measures*. Ottawa: DND Canada, 2019.

Canada. Director General Air Readiness. *RCAF Vectors*. Ottawa: DND Canada, 2019.

Canada. Director of Air Domain Development. *Fragmentary Order (Frag O) 2018-011 to Campaign Plan - RCAF Cyber Mission Assurance Initiating Directive*. Ottawa: DND Canada, 2018.

Canada. Royal Canadian Air Force. *RCAF Campaign Plan*. Ottawa: DND Canada, 2019.

———. *RCAF Concept Proposal: RCAF Cyber Mission Assurance V2.4*. Trenton: DND Canada, 2018.

Canada. ADM(IM). *IMS 6003-1-1, Information Technology Security Incident Management*. Ottawa: DND Canada, 2018.

Canada. Department of National Defence. "22 Wing North Bay." DND Canada. Accessed Mar 26, 2021. http://www.rcaf-arc.forces.gc.ca/en/22-wing/index.page.

———. "About the RCN." DND Canada. Accessed Mar 28, 2021. http://www.navy-marine.forces.gc.ca/en/about/index.page.

———. B-GA-104-000/FP-001, *Operational Airworthiness Manual (OAM)*. Winnipeg: DND Canada, 2017.

———. B-GA-400-000/FP-001, *RCAF Doctrine*. Ottawa: DND Canada, 2015.

———. B-GA-402-001/FP-001, *RCAF Doctrine: Command and Control.* Trenton: Canadian Forces Aerospace Warfare Centre, 2018.

———. B-GJ-005-300/FP-001, *CFJP 3.0 Operations.* Ottawa: DND Canada, 2011.

———. C-05-005-001/AG-001, *Technical Airworthiness Manual (TAM)*. Ottawa: DND Canada, 2019b.

———. *Cyber Mission Assurance Program Charter*. Ottawa: Vice Chief of Defence Staff, 2020a.

———. *Cyber Mission Assurance Program: Functional Planning Guidance 2021-22*. Ottawa: Vice Chief of Defence Staff, 2020b.

———. *DRAFT - Canadian Air Defence Sector (CADS) Mission Defence Team (MDT) Concept of Operations*: DND Canada, 2020a.

———. *DRAFT V1.5 - Fleet Cyber Team CONOP*. Ottawa: DND Canada, 2021a.

———. *DRAFT v1D - CP140 Mission Defence Team - Cyber (MDT-C) Concept of Employment. RDIMS 1968517*. Ottawa: DND Canada, 2021b.

———. "Flight Safety - Royal Canadian Air Force." DND Canada. Accessed Apr 13, 2021. http://www.rcaf-arc.forces.gc.ca/en/flight-safety/index.page.

———. JDN 2017-02. *Joint Doctrinal Note on Cyber Operations*. Ottawa: DND Canada, 2017.

———. "Materiel Group Home: About Us." DND Canada. Accessed Jan 20, 2021. DWAN intranet: http://Materiel.mil.ca/about-us/index.page.

———. "North American Aerospace Defence (NORAD)." DND Canada. Accessed Mar 2, 2021. https://www.canada.ca/en/department-national-defence/services/operations/allies-partners/norad.html.

———. "Operation IMPACT." DND Canada. Accessed Mar 2, 2021. https://www.canada.ca/en/department-national-defence/services/operations/military-operations/current-operations/operation-impact.html.

———. "Operation LENTUS." DND Canada. Accessed Mar 2, 2021. https://www.canada.ca/en/department-national-defence/services/operations/military-operations/current-operations/operation-lentus.html.

———. *Pan-Domain Force Employment Concept*. Ottawa: DND Canada, 2020.

———. *Royal Canadian Navy Cyber Strategy 2020-2025*. Ottawa: DND Canada, n.d.

———. *RCAF Flight Operations Manual*. Winnipeg: DND Canada, 2020b.

———. *Roles and Responsibilities - Joint Force Cyber Component Commander*. Ottawa: DND Canada, n.d.

Canada. DTAES. *Technical Airworthiness Authority Advisory 2019-03*. Ottawa: DND Canada, 2019.

Falliere, Nicolas, Liam O. Murchu, and Eric Chien. *W32.Stuxnet Dossier*. Cupertino: Symantec, 2010.

FireEye and Mandiant. *A Global Reset: Cyber Security Predictions 2021*. Milpitas: FireEye Inc, 2020.

Green, James A. *Cyber Warfare: A Multidisciplinary Analysis*, edited by Green, James A. 1st ed. Abingdon, Oxon; New York, NY: Routledge, 2015.

Horner, C. "Cyber Operations 101 and Planning Considerations. "Lecture, Canadian Forces College, Toronto, ON, 22 February 2021, with permission.

Martin, P. E. C. "Cyber Warfare Schools of Thought: Bridging the Epistemological/Ontological Divide." Masters of Defence Studies Research Paper, Canadian Forces College.

McGuinness, Damien. "How a Cyber Attack Transformed Estonia." *BBC News* (Apr 27, 2017). https://www.bbc.com/news/39655415#:~:text=On%2026%20April%202007%20Tallinn,in%20some%20cases%20lasted%20weeks.&text=Such%20attacks%20are%20not%20specific%20to%20tensions%20between%20the%20West%20and%20Russia.

National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity*. Gaithersburg: US Department of Commerce, 2018.

———. "The Five Functions." US Government. https://www.nist.gov/cyberframework/online-learning/five-functions.

Newman, Lily Hay. "A Ransomware Attack has Struck a Major US Hospital Chain." *Wired* (Sep 20, 2020a). https://www.wired.com/story/universal-health-services-ransomware-attack/.

———. "Ransomware Hits Dozens of Hospitals in an Unprecedented Wave." *Wired* (Oct 29, 2020b). https://www.wired.com/story/ransomware-hospitals-ryuk-trickbot/.

NORAD. “NORAD Conducts Arctic Air Defense Exercise AMALGAM DART.” NORAD. Accessed Apr 29, 2021, https://www.norad.mil/Newsroom/Article/2538728/norad-conducts-arctic-air-defense-exercise-amalgam-dart/

O'Shaughnessy, Terrence J. and Peter M. Fesler. *Hardening the Shield: A Credible Deterrent & Capable Defense for North America*. Washington: Woodrow Wilson International Center for Scholars, 2020.

Pelchat, Andre and Luc Beaudoin. ""Security Authority" Recognition between DIM SECUR and DTAES. RDIMS# 2018892."DND Canada, Ottawa.

Perez, Evan. "FBI: Hacker Claimed to have Taken Over Flight's Controls." *Cnn* (May 18, 2015). https://www.cnn.com/2015/05/17/us/fbi-hacker-flight-computer-systems/index.html.

Rheaume, Francis and Francis Painchaud. *Risk-Based Cyber Mission Assurance Process (RCMAP): Example-Driven Overview*. Valcartier: Defence Research and Development Canada, 2018a.

———. *Risk-Based Cyber Mission Assurance Process (RCMAP): Risk Assessment. DRDC-RDDC-2018-R0002*. Valcartier: Defence Research and Development Canada, 2018b.

———. *Risk-Based Cyber Mission Assurance Process: Mission Criticality Analysis and Asset Valuation. DRDC-RDDC-2018-R0000*. Valcartier: Defence Research and Development Canada, 2018c.

Rozema-Seaton, Erik. "BOXTOP 22: The Cost of Focusing on an Operational Culture." *The Royal Canadian Air Force Journal* 8, no. 4 (Fall 2019): 7-23. http://publications.gc.ca/collections/collection_2019/mdn-dnd/D12-16-8-4-eng.pdf

Schactman, Noah. "Exclusive: Computer Virus Hits U.S. Drone Fleet." *Wired* (Oct 7, 2011). https://www.wired.com/2011/10/virus-hits-drone-fleet/.

Scholes, R.G. "The RARM and ORAT for RCAF Cyber Mission Assurance." Joint College Command and Staff Program Service Paper, Canadian Forces College, Toronto, 2021.

Thorne, Bernie. "The Lockheed CP-140M Aurora, Canada's Current Long Range Patrol Fleet." *Canadian Military Journal* 21, no. 2 (Spring, 2021): 26-37. http://www.journal.forces.gc.ca/vol21/no2/PDF/CMJ212Ep26.pdf.

Transport Canada. "Airport Divestiture Status Report." Government of Canada. Accessed Apr 13, 2021. https://web.archive.org/web/20150930005553/http://www.tc.gc.ca/eng/programs/airports-status-menu-441.htm.

Turnbull, Grant. "Back Door for Hackers? F-35 Cyber Weaknesses in the Spotlight." *Global Defence Technology* no. 97 (Mar, 2019). https://defence.nridigital.com/global_defence_technology_mar19/back_door_for_hackers_f-35_cyber_weaknesses_in_the_spotlight.

United States Cyber Command. *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*. Fort Meade: US Cyber Command, 2018.

US Department of Defense. "North American Aerospace Defense Command." US DoD. Accessed Mar 26, 2021. https://www.norad.mil/About-NORAD/.

Wakelam, Randall. "The Air Force and Flight Safety: A Culture of Tolerated Disobedience," in *The Insubordinate and the Noncompliant: Case Studies of Canadian Mutiny and Disobedience, 1920 to Present*, ed. Howard G. Coombs (Kingston: The Dundurn Group and Canadian Defence Academy Press, 2007): 345-369.