National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

THE INVISIBLE ENEMY: CHALLENGES IN DEFENDING NAVAL VESSELS FROM MALIGN ACTIVITY IN CYBERSPACE

Lieutenant-Commander Christopher P. Heckman

JCSP 47

Service Paper

Disclaimer

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

PCEMI 47

Étude militaire

Avertissement

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

Canada

CANADIAN FORCES COLLEGE - COLLÈGE DES FORCES CANADIENNES

JCSP 47 - PCEMI 47
2020 – 2021

SERVICE PAPER – ÉTUDE MILITAIRE

THE INVISIBLE ENEMY: CHALLENGES IN DEFENDING NAVAL VESSELS FROM MALIGN ACTIVITY IN CYBERSPACE

By Lieutenant-Commander Christopher P. Heckman

Word Count: 2,627

Nombre de mots : 2.627

THE INVISIBLE ENEMY: CHALLENGES IN DEFENDING NAVAL VESSELS FROM MALIGN ACTIVITY IN CYBERSPACE

> *A multi-dimensional and layered approach to the defence of maritime forces will be required…Clearly, protection in the cyber domain will become as vital as protection in the physical domain, requiring measures that assure the integrity and performance of our operational networks in the face of physical or cyber attacks*.
>
> - Commander of the RCN, *Leadmark 2050: Canada in a New Maritime World*

AIM

1. This service paper will explain why the Royal Canadian Navy (RCN) requires a Defensive Cyberspace Operations – Internal Defensive Measures (DCO-IDM) capability to defend against threats in cyberspace, with a view to providing recommendations on the approach the RCN should take in acquiring a DCO-IDM capability. This paper includes several terms that may be unfamiliar; a glossary has been included at Annex A for convenience.

INTRODUCTION

2. The relationship between sailors and the equipment they use to conduct modern naval warfare conjures an image of human and machine being fused together, both relying on the other to achieve success. The RCN has a history of prioritizing technological modernization. The Tribal Class Update Modernization Project transformed all four Tribal Class destroyers into area air defence platforms with modernized command and control (C2) and signals intelligence systems between 1987 and 1994 at a cost of $1.5 billion.[1] From 2010-2018 the Halifax Class Modernization project enhanced RCN frigates by integrating a new Combat Management System, as well as advanced radar, missile, electronic warfare, and C2 systems for $4.3 billion.[2] Finally, as part of the National Shipbuilding Strategy announced in 2010, the Canadian Surface Combatant (CSC) project represents one of the largest and most technologically advanced procurements in Canadian history, with an estimated cost of $56-60 billion for 15 ships.[3] Given the

---

[1] Marc Milner, *Canada's Navy: The First Century* (Toronto: University of Toronto Press, 2000), 287-88.

[2] Government of Canada, "Halifax-Class Modernization and Frigate Life Extension," Department of National Defence, December 13, 2018, last accessed 5 February 2021, https://www.canada.ca/en/department-national-defence/services/procurement/halifax-class-modernization.html.

[3] Government of Canada, "Canadian Surface Combatant," Department of National Defence, March 11, 2020, last accessed 5 February 2021, https://www.canada.ca/en/department-national-defence/services/procurement/canadian-surface-combatant.html.; see also Government of Canada, "Canadian Surface Combatant (CSC) Quad Chart" (Ottawa, Canada: Department of National Defence, April 1, 2019), last accessed 5 February 2021, https://www.canada.ca/content/dam/dnd-mdn/documents/quad-charts/csc-quad-chart-en.pdf.

significant investment in modernization and the dependence that modern naval vessels have on technology, one might assume that naval vessels have defensive capabilities in all warfare domains. This is not yet the case in the cyberspace domain.

3. To explain why a DCO-IDM capability is required to defend naval cyberspace, this paper is structured in six parts. First, it will provide a brief overview of what DCO-IDM is. Second, it will describe why the existing Department of National Defence (DND) and Canadian Armed Forces (CAF) approach to Information Technology security (ITSEC) only addresses one aspect of the problem, resulting in a capability gap. Third, it will provide a brief overview of cyber vulnerability management and exploitation. Fourth, it will describe how these vulnerabilities represent operational risk. Fifth, it will describe how current ad-hoc DCO-IDM initiatives have demonstrated a requirement for a full DCO-IDM capability to manage operational risk. The paper will conclude with a summary of recommendations.

DISCUSSION

What is DCO-IDM?

4. In 2015 the CDS articulated his strategic objectives for DCO in the *CDS Initiating Directive for Defensive Cyber Operations*. The most notable objectives are that a DCO capability will provide DND/CAF with an ability to identify, characterize, analyze, withstand, and respond to cyber threats.[4] A comprehensive list of these objectives has been included as Annex B. DCO has been subdivided into two categories, DCO-IDM and DCO - Response Actions (DCO-RA).[5] DCO-IDM are defensive operations conducted in or through one's own cyberspace to ensure freedom of action.[6] As DCO-RA is closely aligned with Offensive Cyberspace Operations (OCO),[7] and both are CAF capabilities, this paper will focus solely on DCO-IDM in the naval context.

---

[4] Government of Canada, "CDS INITIATING DIRECTIVE FOR DEFENSIVE CYBER OPERATIONS" (Ottawa, Canada: Department of National Defence, February 2, 2015), 8.

[5] Government of Canada, "TERMIUM Plus® Record 1 - Defensive Cyber Operations - Response Action (DCO-RA)," https://www.btb.termiumplus.gc.ca, May 11, 2017, last accessed 5 February 2021, last accessed 5 February 2021, https://www.btb.termiumplus.gc.ca/DefensiveCyberOperationsResponseAction.

[6] Government of Canada, "TERMIUM Plus® Record 3 - Defensive Cyberspace Operations (DCO)," https://www.btb.termiumplus.gc.ca, March 15, 2017, last accessed 5 February 2021, https://www.btb.termiumplus.gc.ca/DefensiveCyberspaceOperations; see also Government of Canada, "TERMIUM Plus® Record 1 - Internal Defensive Measures (IDM)," https://www.btb.termiumplus.gc.ca, July 15, 2016, last accessed 5 February 2021, https://www.btb.termiumplus.gc.ca/InternalDefensiveMeasures.

[7] Government of Canada, "TERMIUM Plus® Record 1 - Offensive Cyber Operation (OCO)," https://www.btb.termiumplus.gc.ca, May 16, 2017, last accessed 5 February 2021, https://www.btb.termiumplus.gc.ca/OffensiveCyberOperation.

5. The *Joint Doctrine Note – Cyber Operations 2021*[draft][8] helps clarify what DCO-IDM entails by providing a list of DCO-IDM activities. The following list summarizes the activities most germane to this paper; the complete list of DCO-IDM activities has been included as Annex C:

a. cyber threat intelligence;
b. criticality, vulnerability, and risk assessment and analysis;
c. identification of security controls and likely adversary action;
d. monitoring and response actions; and,
e. development of a risk mitigation plan.[9]

6. The remainder of this paper will describe why the RCN will remain vulnerable without an ability to execute these DCO-IDM activities.

Information Technology security is no longer sufficient on its own

7. Witnessing the aftermath of cyber attacks during the past several years has caused government organizations and private industry to seek new security and defence capabilities, as described in the Canadian *National Cyber Security Strategy* released in 2018.[10] For example on 3 July 2020 a ransomware attack on the Royal Military College (RMC) resulted in the complete shutdown of the school until a contingency plan restored core services.[11] The IT security industry has recognized and responded to the increased focus on cyberspace by rebranding itself as cyber security and offering an extensive suite of cyber security products.

8. This rebranding is illustrated in a comparison between the definition of IT security and cyber security. IT security is defined as "safeguards to preserve the confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information."[12] The definition of cyber security, "the body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure

---

[8] Government of Canada, "Draft Joint Doctrine Note - Cyber Operations 2021" (Ottawa, Canada: Department of National Defence, 2021).

[9] Ibid., 4–4.

[10] Ralph Goodale, National Cyber Security Strategy (Public Safety Canada, 2018), 12-15.

[11] Matt Scace, "National Defence Assessing Possible Damage of RMC Cybersecurity Incident," Kingston Whig-Standard (1993), 2020, last accessed 5 February 2021, http://cfc.summon.serialssolutions.com.cfc.idm.oclc.org/NationalDefenceAssessingPossibleDamageofRMCCybersecurityIncident.

[12] Government of Canada, "TERMIUM Plus® Record 2 - IT security (ITSEC)," https://www.btb.termiumplus.gc.ca, September 2, 2015, last accessed 5 February 2021, https://www.btb.termiumplus.gc.ca/ITsecurity.

confidentiality, integrity and availability,"[13] simply expands on the term "safeguards" in the previous definition. This can largely be attributed to a common misconception that cyberspace is *solely* the IT space, only bigger. There is little contention that cyberspace does expand the traditional IT footprint. The capability gap described in this paper is related to the idea that cyberspace also encompasses new technologies *other than* IT, which will now be discussed.

The capability gap, explained

9. Traditional weapon, sensor and propulsion systems were controlled mechanically. Modern systems are controlled electronically. These traditional systems were segregated, or 'airgapped'.[14] Modern systems are integrated. Finally, traditional naval communications involved mailing correspondence at the next port of call. Modern naval communications leverage the entire radio spectrum to transmit data anywhere in the world in near real time. Combined, these factors provide a naval example of how the Cyberspace and the cyber domain[15] now encompass a much larger and more complex terrain than only IT systems such as the Defence Wide Area Network.

10. In addition to IT systems, the modern cyberspace terrain includes Operational Technology (OT), those technologies used to remotely control physical devices,[16] and Platform Technology (PT), which include "all hardware and software on ships…that monitors and/or controls data, power, command and control, surveillance, fire control, navigation, propulsion, maintenance, training and other fundamental functions of the system." [17] The OT and PT aspects of cyberspace "have the potential to dwarf the 20th century IT revolution."[18] These systems are different from IT systems because they need to need to be immediately available, require real-time response, and are directly involved in ensuring human safety.[19] These are the technologies that enable the RCN to command, float, move, and fight. Using joint terminology, naval PT enables the tactical application of the command, sense, shield, sustain, and act operational functions. For these reasons

---

[13] Government of Canada, "TERMIUM Plus® Record 1 - Cyber Security," https://www.btb.termiumplus.gc.ca, November 8, 2017, last accessed 5 February 2021, https://www.btb.termiumplus.gc.caCyberSecurity.

[14] Oxford English Dictionary, "Definition of Air-Gapped," Oxford English Dictionary, 2021, https://oed.com, last accessed 5 February 2021; The Oxford English Dictionary defines air-gapped as: (of a computer) having no direct connection to the internet or to any other computer that is connected to the internet, for security reasons.

[15] Government of Canada, "TERMIUM Plus® Record 1 - Cyberspace," https://www.btb.termiumplus.gc.ca, March 15, 2017, last accessed 5 February 2021, https://www.btb.termiumplus.gc.ca/Cyberspace.

[16] Canada, "Draft Joint Doctrine Note - Cyber Operations 2021," 1–2.

[17] Ibid.

[18] Yuriy Zacchia Lun et al., "State of the Art of Cyber-Physical Systems Security: An Automatic Control Perspective," Journal of Systems and Software, 149 (2019): 1, doi:https://doi.org/10.1016/j.jss.2018.12.006.

[19] Ibid., 3.

the ability to protect and defend not only IT, but OT and PT systems in the RCN is critical.

Vulnerabilities, exploits, and risk

11. The CAF has increased its reliance on commercial-off-the-shelf (COTS) products and technologies in military platforms. From a fiscal stewardship perspective this is a wise approach as COTS typically offer flexibility in terms of procurement, cost-effectiveness, and often benefit from the potential to arrange contracted in-service-support (ISS). In terms of security, however, the integration of COTS products into military platforms provide adversaries with new attack vectors. The next several paragraphs will explain why this is the case.

12. Security researchers, governments, and malign actors all seek to discover and exploit new vulnerabilities. New vulnerabilities are referred to as "zero-day"[20] vulnerabilities until such time as a configuration change or patch is developed to fix the problem. Security researchers typically provide information of new zero-days to the impacted vendor. This in turn provides the vendor an opportunity to fix the vulnerability then notify their customers that a configuration change or patch is available. After that initial notification, it is up to the impacted organization to decide when, or if, to address the vulnerability based on their own vulnerability management process.

13. Vulnerability information is then entered by the Common Vulnerabilities and Exposures (CVE®) community and tracked using the CVE database, an online database that serves as the standard for vulnerability and exposure identifiers.[21] Subsequently, the CVE List feeds into the US National Vulnerability Database (NVD), a standards-based US Government repository used to enable "automation of vulnerability management, security measurement, and compliance."[22] The NVD then uses a Common Vulnerability Scoring System (CVSS) to assess the potential severity of vulnerabilities based on standardized metrics. The NVD therefore represents an assessment of the potential severity of vulnerabilities. Together, the CVE database and the NVD form an open source and consolidated list of all publicly known vulnerabilities and their potential severity.

---

[20] Trend Micro, "Zero-Day Vulnerability," TrendMicro.Com, 2021, last accessed 5 February 2021, https://www.trendmicro.com/vinfo/us/security/definition/zero-day-vulnerability; A zero-day vulnerability is a vulnerability in a system or device that has been disclosed but is not yet patched. An exploit that attacks a zero-day vulnerability is called a zero-day exploit.

[21] Mitre, "About Common Vulnerabilities and Exposures (CVE)," https://www.CVE.Mitre.org, December 11, 2020, last accessed 5 February 2021, https://cve.mitre.org/about/index.html; CVE is operated by the MITRE corporation and is funded by the US Department of Homeland Security (DHS) and Cybersecurity and Infrastructure Security Agency (CISA)

[22] (NIST) National Institute of Standards and Technology, "National Vulnerability Database (NVD)," https://www.NVD.NIST.gov, last accessed 5 February 2021, https://nvd.nist.gov/general.

14. Cyber security personnel use this information to assess organizational vulnerabilities and risk, and then to provide decision makers with risk management recommendations for remediation. However, malign actors armed with the same information only need to identify what version of software, firmware, or hardware, an organization is using to assess a target organization's vulnerabilities in the same way. This situation can be visualized as two opponents, each seeking to gain an advantage in cyberspace by protecting and defending themselves through DCO-IDM while simultaneously seeking to exploit the other through OCO. This idea is foundational to how the operational function of shield is conducted in the cyberspace domain.

15. The previous paragraphs provide a broad overview of standard vulnerability identification through remediation. It must be recognized that knowledge of zero-day vulnerabilities may also be withheld and weaponized. Defending against zero-day attacks is difficult, thus making knowledge of zero-day vulnerabilities valuable. Zero-day exploits are typically held in reserve and deployed judiciously and covertly. For example, from 2012 to 2019 only 60 zero-day exploits were observed, the majority being used by Russia and China.[23] A DCO-IDM capability is required to defend against such threats.

Operational Impacts of Vulnerability Exploitation

16. A simple way of thinking about the operational impact of an adversary gaining control over an IT, OT, or PT system is that anything an operator can do with an IT, OT or PT system, an adversary can do.

> Cyber attacks can target any weapon subsystem that is dependent on software, potentially leading to an inability to complete military missions or even loss of life. Examples of functions enabled by software—and potentially susceptible to compromise—include powering a system on and off, targeting a missile, maintaining a pilot's oxygen levels, and flying aircraft. An attacker could potentially manipulate data in these systems, prevent components or systems from operating, or cause them to function in undesirable ways.[24]

17. In 2018 the United States (US) Department of Defence (DoD) was preparing to spend $1.66 trillion on its major weapon systems. The US Government Accountability

---

[23] Kathleen Metrick, Parnian Najafi, and Jared Semrau, "Zero-Day Exploitation Increasingly Demonstrates Access to Money, Rather than Skill — Intelligence for Vulnerability Management," https://www.Fireeye.Com, April 6, 2020, last accessed 5 February 2021, https://www.fireeye.com/blog/threat-research/2020/04/zero-day-exploitation-demonstrates-access-to-money-not-skill.html.

[24] United States Government Accountability Office, "Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities," (Washington, DC, United States of America: United States Government, October 2018), 1, last accessed 5 February 2021, https://www.gao.gov/assets/700/694913.pdf.

Office (GAO) was asked to conduct an assessment of the state of DOD weapon systems cyber security. They found that "in operational testing, DOD routinely found mission-critical cyber vulnerabilities in systems…using relatively simple tools and techniques, testers were able to take control of systems and largely operate undetected."[25] After gaining this initial access attackers could, "move throughout a system, escalating their privileges until they had taken full or partial control of a system…They could see, in real-time, what the operators were seeing on their screens and could manipulate the system."[26]

18. Although these examples are based on US DOD exploiting their own platforms, it should be assumed that nation states with cyber capabilities comparable to the US can achieve similar results if targeting RCN naval platforms. As described in the A-Z Maritime Concept for Information Warfare, "with an ever increasing cyber threat environment, FVEYs partners cannot wait to build cyber after an attack or intrusion occurs."[27]

Ad-Hoc DCO-IDM initiatives indicate a comprehensive DCO-IDM capability is required

19. *Concepts and doctrine*. ADM(IM) have been prioritizing the development of concepts and doctrine in collaboration with the CAF. The primary DND/CAF cyber reference was the 2017 version of the *Joint Doctrine Note - Cyber Operations*. This document has since been significantly updated, with a new version expected to be published in 2021. The JDN was used to inform the *RCN Cyber Strategy: 2020-2025* and was integral in the planning and coordination of the ad-hoc DCO-IDM activities that will be described next.

20. *Equipment*: Situational awareness applies to cyberspace similarly to other warfare domains. Cyber security tools are used to scan IT, OT, or PT systems to create a network map and monitor the systems for indicators of compromise. Additionally, these tools often leverage the CVE database and NVD described earlier to integrate vulnerability and severity information. Some of these tools use dashboards to visualize those results, providing military commanders with a cyber situational awareness product.

21. The ADM(IM) Cyber Defence – Decision Analysis and Response (CD-DAR) project, which moved into its definition phase in June 2020, is intended to provide DND/CAF with some DCO-IDM capability. Underscoring a theme in this paper, however, CD-DAR will only encompass DND/CAF Information Technology (IT)

---

[25] Ibid., What GAO Found.
[26] Ibid., 22.
[27] AUSCANZUKUS, "Maritime Concept for Information Warfare," 2014, 9.

systems.[28] It is therefore unlikely that naval OT or PT systems will integrate into what CD-DAR eventually delivers.

22. *Personnel*. The RCN has access to several cyber security personnel through its relationship with the Director General Maritime Equipment Program Management (DGMEPM), which falls under Assistant Deputy Minster Materiel (ADM(Mat)). DGMEPM have a contract with the Naval Engineering Test Establishment (NETE), a Government Owned Contractor Operated organization, who have several cyber security engineers on staff. DGMEPM has also started generating System Security Engineering (SSE) specialists within the naval engineering trades. Together, the DGMEPM SSE specialists and NETE provide the RCN with technical risk assessments of naval vessels, amongst other cyber security activities.

23. The Assistant Deputy Minster of Information Management (ADM(IM)) is the departmental lead for cyber development in DND/CAF. ADM(IM) has cyber security engineers on staff and are in the process of establishing the Cyber Operator trade for the CAF. Their efforts have the potential to address many of the challenges described in this paper. Their resources are limited, however, and their focus on IT does not address naval concerns with OT and PT systems.

24. The RCN has collaborated with the Canadian Forces Network Operations Centre (CFNOC) to conduct manual assessments of naval IT systems. Similarly, DGMEPM have manually conducted assessments of several naval PT systems. The results of these activities, which are classified, provide a compelling body of evidence to substantiate the requirement for an integrated DCO-IDM capability in all naval vessels. Vulnerabilities exist and the RCN lacks the ability to regularly monitor critical systems.

25. Manually conducting DCO-IDM activities is unsustainable for CFNOC and DGMEPM, and is not scalable to the entire RCN fleet. Thus, DCO-IDM tools and trained cyber security personnel are required to maintain cyberspace situational awareness and provide commanders with operational risk assessments. Without such a capability, commanders are inadvertently accepting risk of which they are simply unaware.

CONCLUSION

26. The RCN relies on IT, OT and PT systems to command, float, move, and fight. New capabilities must be developed to ensure these systems remain secure and defended against modern threats. Managing risk in cyberspace requires close collaboration between

---

[28] Government of Canada, "Letter of Interest - CD-DAR Draft ITQ" (Ottawa, Canada: Public Works and Government Services Canada, July 9, 2020), last accessed 5 February 2021, https://buyandsell.gc.ca/cds/public/2020/07/09/1ce19d2d76f0ae9df8ba95d86e5efda9/ABES.PROD.PWQE.B049.E27831.EBSU000.PDF.

DND/CAF organizations as well as private industry and Allies. This paper argues that a DCO-IDM capability is required for the RCN to maintain cyberspace situational awareness, conduct threat-based risk management, and defend naval systems when required. Without a DCO-IDM capability the RCN operational community will lack the information necessary to make well-informed risk decisions.

27. One of the top RCN cyber objectives articulated in the *RCN Cyber Strategy: 2020-2025* is to "defend naval platforms from cyber threats."[29] Until the RCN acquires a DCO-IDM capability, however, its primary defence against cyber attack will remain an assumption that adversaries lack the intent to attack naval platforms through cyberspace.

RECOMMENDATIONS

28. The following list offers specific recommendations on the approach the RCN should take in acquiring a DCO-IDM capability:

a. Collaborate with ADM(IM) to:
   i. identify which PRICIE-G elements of DCO-IDM the RCN should expect to receive from ADM(IM) versus those that will need to be developed by the RCN;
   ii. ensure that IT, OT, and PT systems in HMC ships and submarines are included in any joint cyber capability development efforts, such as CD-DAR; and
   iii. support ADM(IM) cyber doctrine development efforts to align joint efforts and include a naval perspective;
b. Collaborate with Director General Departmental Security, as the DND/CAF Chief Security Officer (CSO) for DND/CAF,[30] to identify how the existing IT security organization applies to OT and PT systems in HMC ships and submarines;
c. Collaborate with ADM(Mat) to enhance system security engineering knowledge within the naval engineering community and leverage their expertise in naval OT and PT to inform DCO-IDM capability development; and
d. Prioritize the resourcing and implementation of those DCO-IDM components described in the *RCN Cyber Strategy: 2020-2025* to ensure

---

[29] Royal Canadian Navy, "RCN Cyber Strategy 2020-2025" (Ottawa, Canada: Government of Canada, 2020), 15.

[30] Government of Canada, "DAOD 2006-0, Defence Security," Department of National Defence, September 27, 2019," https://www.canada.ca, last accessed 5 February 2021, https://www.canada.ca/en/department-national-defence/corporate/policies-standards/defence-administrative-orders-directives/2000-series/2006/2006-0-defence-security.html.

the RCN remains a valuable FVEY and NATO partner capable of executing naval operations in a cyber contested environment.

ANNEX A

GLOSSARY OF TERMS

Cyberattack: "An attack that involves the unauthorized use, manipulation, interruption or destruction of, or access to, via electronic means, electronic information or the electronic devices or computer systems and networks used to process, transmit or store that information."[31]

Cyber security: "The body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability."[32]

Cyberspace: "The element of the operational environment that consists of interdependent networks of information technology structures—including the Internet, telecommunications networks, computer systems, embedded processors and controllers—as well as the software and data that reside within them."[33]

Defensive Cyber Operation (DCO): "A defensive operation conducted in or through cyberspace to detect, defeat and/or mitigate offensive and exploitive actions to maintain freedom of action."[34]

Defensive Cyber Operation - Internal Defensive Measures (DCO-IDM): "internal defensive measures: In defensive cyber operations, measures and activities conducted within one's own cyberspace to ensure freedom of action."[35]

Defensive Cyber Operation - Response Action (DCO-RA): "In defensive cyber operations, measures and activities conducted in or through cyberspace, outside of one's own cyberspace, against ongoing or imminent threats to preserve freedom of action."[36]

Information Technology (IT): "Includes any equipment or system that is used in the automatic acquisition, storage, manipulation, management, movement, control, display,

---

[31] Government of Canada, "TERMIUM Plus® Record 1 - Cyber Attack," https://www.btb.termiumplus.gc.ca, October 6, 2017, last accessed 5 February 2021, https://www.btb.termiumplus.gc.ca/CyberAttack.

[32] Government of Canada, "TERMIUM Plus® Record 1 - Cyber Security."

[33] Government of Canada, "TERMIUM Plus® Record 1 - Cyberspace."

[34] Government of Canada, "TERMIUM Plus® Record 3 - Defensive Cyberspace Operations (DCO)."

[35] Government of Canada, "TERMIUM Plus® Record 1 - Internal Defensive Measures (IDM)."

[36] Government of Canada, "TERMIUM Plus® Record 1 - Defensive Cyber Operations - Response Action (DCO-RA)."

switching, interchange, transmission, or reception of data or information. It includes all matters concerned with the design, development, installation, and implementation of information systems and applications to meet business requirements. Examples of IT include cable infrastructure, endpoint devices, wireless mobile devices, databases, servers, operating systems, user accounts and applications."[37]

Information Technology (IT) security: "Safeguards to preserve the confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information."[38]

Offensive Cyber Operation (OCO): "An offensive operation intended to project power in or through cyberspace to achieve effects in support of military objectives."[39]

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. Examples of OT include Supervisory Control and Data Acquisition (SCADA), Programmable Logic Controller (PLC) devices, and/or Industrial Control Systems (ICS), such as systems controlling a facility's power, heating ventilation and air conditioning (HVAC), and intrusion detection systems on bases. OT is increasingly interfaced to IT systems and requires specialized, often proprietary components to control physical or mechanical functions."[40]

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 . Examples of PT include avionics, vehicle weapons control systems, and integrated platform management systems. PT is typically delivered through defence contracts and is increasingly reliant on digital or electrical components."[41]

Vulnerability: "An inherent weakness in an entity, system, platform or piece of equipment that exposes it to harm."[42]

---

[37] Government of Canada, "Draft Joint Doctrine Note - Cyber Operations 2021," 1–2.
[38] Government of Canada, "TERMIUM Plus® Record 2 - IT Security (ITSEC)."
[39] Government of Canada, "TERMIUM Plus® Record 1 - Offensive Cyber Operation (OCO)."
[40] Government of Canada, "Draft Joint Doctrine Note - Cyber Operations 2021," 1–2.
[41] Ibid.
[42] Government of Canada, "TERMIUM Plus® Record 1 - Vulnerability," https://www.btb.termiumplus.gc.ca, May 27, 2019, https://www.btb.termiumplus.gc.ca/Vulnerability.

ANNEX B

DND/CAF STRATEGIC OBJECTIVES FOR DCO

The strategic objectives for this directive are as follows:

a. Ensure the confidentiality, integrity and availability of critical DND/CAF CIS, data, and associated infrastructure;

b. Enhance the ability of DND/CAF to identify, characterize and analyze cyber threats;

c. Enhance the ability of DND/CAF to withstand and respond to cyber threats;

d. Ensure freedom of manoeuvre of DND/CAF in the cyber domain;

e. Establish a dynamic, agile, and responsive capability to conduct DCO;

f. Contribute to the wider GC approach to cyber security IAW ref A; and

g. Share information and cooperate with key allies and partners on DCO.[43]

[43] Canada, "CDS INITIATING DIRECTIVE FOR DEFENSIVE CYBER OPERATIONS," 8/13.

ANNEX C

DCO-IDM PLANNING CONSIDERATIONS

0415. Deliberate DCO planning should proceed in an orderly and disciplined fashion by evolving requirements into specific DCO tasks and activities through a process which considers all relevant factors including CIS planning. Crisis DCO planning will follow a condensed OPP process or available CONPLAN. Some planning considerations, activities and key requirements for the security and defence of cyberspace include:

a. threat intelligence products on adversary capabilities, intent and overall goal;
b. criticality assessment, to include the identification of key terrain in cyberspace and a defended asset list aligned with overall mission tasks and objectives as they progress to different phases from peacetime to conflict;
c. vulnerability analysis, that is, the determination and prioritization of cyber vulnerabilities and the linking of these known cyber vulnerabilities to adversary capabilities and intent;
d. risk management analysis;
e. external defensive measure advantages that can be realized from grey cyberspace;
f. defining a list of pre-approved controls and measures and their associated authorities such that when/if an event/incident happens, direction for execution of those pre-approved actions can occur swiftly (pre-approvals, credentials, access should have been already been established);

g. the determination of existing technical, physical and procedural security controls;

h. the establishment of clear indicators of attack (IoAs) and indicators of compromise (IoCs);

i. the identification of the potential effects of the adversary's action and the cyber mission assurance risks involved;

j. data management, such as collecting, storing, structuring, and integrating large volumes of data from multiple sources;

k. the creation of a holistic adversary focused monitoring strategy;

l. the establishment of prepared response actions to neutralize, or understand malicious actions;

m. the creation of technical threat hunt and defensive deception plans;

n. a risk mitigation plan to focus defensive resources and effort, ensuring mission assurance or acceptance of residual risk;

o. the establishment of AORs to conduct DCOs on key terrain in cyberspace, which includes authorities to conduct prioritized technical changes, reporting, responding and remediation; and

p. allied memoranda of understanding (MOUs) and DCO request for assistance.[44]

[44] Canada, "Draft Joint Doctrine Note - Cyber Operations 2021," 4-4 through 4-5.

BIBLIOGRAPHY

AUSCANZUKUS. “Maritime Concept for Information Warfare.” 2014.

Goodale, Ralph. *National Cyber Security Strategy*. Public Safety Canada, 2018. Last accessed 5 February 2021. http://cfc.summon.serialssolutions.com.cfc.idm.oclc.org/NationalCyberSecurityStrategy.

Government of Canada. “Canadian Surface Combatant.” Department of National Defence, March 11, 2020. Last accessed 5 February 2021. https://www.canada.ca/en/department-national-defence/services/procurement/canadian-surface-combatant.html.

Government of Canada. “Canadian Surface Combatant (CSC) Quad Chart.” Ottawa, Canada: Department of National Defence, April 1, 2019. Last accessed 5 February 2021. https://www.canada.ca/content/dam/dnd-mdn/documents/quad-charts/csc-quad-chart-en.pdf.

Government of Canada. “CDS INITIATING DIRECTIVE FOR DEFENSIVE CYBER OPERATIONS.” Ottawa, Canada: Department of National Defence, February 2, 2015.

Government of Canada. “Draft Joint Doctrine Note - Cyber Operations 2021.” Ottawa, Canada: Department of National Defence, 2021.

Government of Canada. “Halifax-Class Modernization and Frigate Life Extension.” Department of National Defence, December 13, 2018. Last accessed 5 February 2021. https://www.canada.ca/en/department-national-defence/services/procurement/halifax-class-modernization.html.

Government of Canada. “Letter of Interest - CD-DAR Draft ITQ.” Ottawa, Canada: Public Works and Government Services Canada, July 9, 2020. Last accessed 5 February 2021. https://buyandsell.gc.ca/cds/public/2020/07/09/Letter of InterestCD-DARDraftITQ.pdf.

Government of Canada. “TERMIUM Plus® Record 1 - Cyber Attack.” https://www.btb.termiumplus.gc.ca, October 6, 2017. Last accessed 5 February 2021. https://www.btb.termiumplus.gc.ca/CyberAttack.

Government of Canada. “TERMIUM Plus® Record 1 - Cyber Domain.” https://www.btb.termiumplus.gc.ca, March 15, 2017. Last accessed 5 February 2021. https://www.btb.termiumplus.gc.ca/CyberDomain.

Government of Canada. “TERMIUM Plus® Record 1 - Cyber Security.” https://www.btb.termiumplus.gc.ca. November 8, 2017. Last accessed 5 February 2021. https://www.btb.termiumplus.gc.ca/CyberSecurity.

Government of Canada. “TERMIUM Plus® Record 1 - Cyberspace.” https://www.btb.termiumplus.gc.ca, March 15, 2017. Last accessed 5 February 2021. https://www.btb.termiumplus.gc.ca/Cyberspace.

Government of Canada. “TERMIUM Plus® Record 1 - Defensive Cyber Operations - Response Action (DCO-RA).” https://www.btb.termiumplus.gc.ca, May 11, 2017. Last accessed 5 February 2021. https://www.btb.termiumplus.gc.ca/DefensiveCyberOperationsResponseAction.

Government of Canada. “TERMIUM Plus® Record 1 - Internal Defensive Measures (IDM).” https://www.btb.termiumplus.gc.ca, July 15, 2016. Last accessed 5 February 2021. https://www.btb.termiumplus.gc.ca/InternalDefensiveMeasures.

Government of Canada. “TERMIUM Plus® Record 1 - Offensive Cyber Operation (OCO).” https://www.btb.termiumplus.gc.ca, May 16, 2017. Last accessed 5 February 2021. https://www.btb.termiumplus.gc.ca/OffensiveCyberOperation.

Government of Canada. “TERMIUM Plus® Record 1 - Vulnerability.” https://www.btb.termiumplus.gc.ca, May 27, 2019. Last accessed 5 February 2021. https://www.btb.termiumplus.gc.ca/Vulnerability.

Government of Canada. “TERMIUM Plus® Record 2 - IT security (ITSEC).” https://www.btb.termiumplus.gc.ca, September 2, 2015. Last accessed 5 February 2021. https://www.btb.termiumplus.gc.ca/ITsecurity.

Government of Canada. “TERMIUM Plus® Record 3 - Defensive Cyberspace Operations (DCO).” https://www.btb.termiumplus.gc.ca, March 15, 2017. Last accessed 5 February 2021. https://www.btb.termiumplus.gc.ca/DefensiveCyberspaceOperations.

Dictionary, Oxford English. “Definition of Air-Gapped.” Oxford English Dictionary, 2021. Last accessed 5 February 2021. https://oed.com/.

Metrick, Kathleen, Parnian Najafi, and Jared Semrau. “Zero-Day Exploitation Increasingly Demonstrates Access to Money, Rather than Skill — Intelligence for Vulnerability Management.” Fireeye.com, April 6, 2020. Last accessed 5 February 2021. https://www.fireeye.com/blog/threat-research/2020/04/zero-day-exploitation-demonstrates-access-to-money-not-skill.html.

Micro, Trend. “Zero-Day Vulnerability.” TrendMicro.Com, 2021. Last accessed 5 February 2021. https://www.trendmicro.com/vinfo/us/security/definition/zero-day-vulnerability.

Milner, Marc. *Canada’s Navy: The First Century*. Toronto: University of Toronto Press, 2000.

Mitre. “About Common Vulnerabilities and Exposures (CVE).” https://www.cve.mitre.org, December 11, 2020. Last accessed 5 February 2021. https://cve.mitre.org/about/index.html.

National Institute of Standards and Technology, (NIST). “National Vulnerability Database (NVD).” https://www.NVD.NIST.gov. Last accessed 5 February 2021. https://nvd.nist.gov/general.

Navy, Royal Canadian. “RCN Cyber Strategy 2020-2025.” Ottawa, Canada: Government of Canada, 2020.

Office, United States Government Accountability. “Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities.” Electronic. Washington, DC, United States of America: United States Government, October 2018. Last accessed 5 February 2021. https://www.gao.gov/assets/700/694913.pdf.

Scace, Matt. “National Defence Assessing Possible Damage of RMC Cybersecurity Incident.” Kingston Whig-Standard (1993). 2020. Last accessed 5 February 2021. http://cfc.summon.serialssolutions.com.cfc.idm.oclc.org/2.0.0/link/0/NationalDefenceAssessingPossibleDamageofRMCCybersecurityIncident.

Zacchia Lun, Yuriy, Alessandro D’Innocenzo, Francesco Smarra, Ivano Malavolta, and Maria Domenica Di Benedetto. “State of the Art of Cyber-Physical Systems Security: An Automatic Control Perspective,” Journal of Systems and Software 149, 149 (2019): 174–216. Last accessed 5 February 2021. doi:https://doi.org/10.1016/j.jss.2018.12.006.