National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

THE HUMAN FACTOR – IMPROVING CYBER SECURITY AWARENESS IN THE ROYAL CANADIAN NAVY

Lieutenant-Commander Darren Sleen

JCSP 45

Exercise *Solo Flight*

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 45

Exercice *Solo Flight*

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 45 – PCEMI 45
MAY 2019 – MAI 2019

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

THE HUMAN FACTOR – IMPROVING CYBER SECURITY AWARENESS IN THE ROYAL CANADIAN NAVY

Lieutenant-Commander Darren Sleen

THE HUMAN FACTOR – IMPROVING CYBER SECURITY AWARENESS IN THE ROYAL CANADIAN NAVY

INTRODUCTION

An institutional level effort to inculcate cybersecurity awareness, education and training at all levels of the Royal Canadian Navy (RCN) workforce is a significant institutional problem that will require creative solutions to create a rapid cultural shift.

As part of the information warfare domain, cyber considerations permeate every part of modern naval operations.[1] This situation is evident on board a modernized Canadian *Halifax*-class frigate. Operations at sea are dependent on the proper functioning of information and communication technology (ICT) networks. The Integrated Platform Management System (IPMS) monitors and controls propulsion, electrical generation, auxiliaries and damage control machinery.[2] The Navigation Data Distribution System (NavDDS) measures and distributes position, navigation and timing (PNT) information. Weapons and sensors are controlled by the Combat Management System 330 (CMS 330). The Naval Information System (NavIS) provides access to on-board classified and unclassified computer networks that are connected ashore through satellite communications. At a deeper level, each of these networks is connected to a multitude of sub-networks and components. This network of networks has become "…a vital enabler and a significant vulnerability for the Canadian Armed Forces."[3]

---

[1] Department of National Defence, *Royal Canadian Navy Information Warfare Strategy Paper,* (Ottawa: Royal Canadian Navy, September 2016), 1-2.

[2] L3 MAPPS, *Integrated Platform Management System,* Information Pamphlet, last accessed 27 April 2019, https://www.l-3mps.com/products/products-details.aspx?id=029

[3] Department of National Defence*, Royal Canadian Cyber Strategy 2018-2025 version 1* RDIMS #426259 (Unapproved DRAFT), (Ottawa: Director of Naval Information Warfare 6-4, n.d.), ii.

It is clear in recent documentation that the RCN is cognizant of the cybersecurity threats to which a warship is exposed, and keenly interested in improving the organization's cyber-resilience.[4] A number of strategic-level initiatives are underway to accomplish this goal that will be discussed later in this paper. Given the small number of personnel available to work towards strategic-level solutions and the bureaucratic challenges that they face, the implementation of holistic solutions will likely take years.[5] At the same time, the RCN is building more connectivity into ships. Notably, the recent implementation of the Internet Services to Sailors System (IS2S) that enables wireless internet connectivity for personal electronic devices at sea offers a multitude of new entry points for cyber threats into the ship.[6]

A constant factor identified across the RCN's cybersecurity efforts is the need to create effective awareness and training campaigns across the workforce.[7] Given the continuously evolving cyber threat environment, this is an effort that will require a flexible approach to remain relevant in the long term.

The RCN faces a challenging cyber threat environment due to the multiple technology domains on board and a threat that is evolving faster than institutional efforts can adapt. The RCN should address these challenges by rapidly establishing scalable methods of increasing its cybersecurity culture by leveraging small changes in existing collective training and readiness documents, modify fault reporting processes and

---

[4] Department of National Defence*, Royal Canadian Cyber Strategy 2018-2025 version 1…,* 1-5.

[5] As an example, there are only four officers working full-time specifically on cybersecurity policy within the RCN; Christopher Heckman, "RCN Cyber Strategy 2018-2025 Briefing version 1.0," powerpoint presentation, (Ottawa: Directorate of Naval Information Warfare, March 2019), slide 7.

[6] Department of National Defence, *High-Level Design Systems Security Risk Assessment Report for* Halifax-*Class Internet Services to Sailors System* 2183A-2100-02-10-02 (DNPS 9-4-2), (Ottawa: Director Naval Platform Systems, 9 August 2018), 6.

[7] Footnote about the ubiquity of the call for cybersecurity education

establish a learning culture that will actively engage tactical-level personnel and enable the future implementation of larger-scale institutional cybersecurity programs.

The RCN discussion throughout the paper is framed around considerations associated with the personnel and equipment on board *Halifax*-class frigates, given the proliferation of networks on board due to the recently completed *Halifax*-class Modernization/Frigate Life Extension (HCM-FELEX) project.[8] The wholesale change of networks has created a *system of systems* that has created a challenge for security testing, crew training and has opened new potential for vulnerability. [9] It therefore serves as a strong case study. Laying the foundation for increased cybersecurity in the current fleet will set the conditions for a more informed and capable team in future ships, such as the Canadian Surface Combatant.

The first section of the paper will describe the cybersecurity problem space for the RCN and focus on the need for a rapid cultural change within the workforce to build a critical mass of cyber awareness. The second section will explain the current obstacles to building cybersecurity awareness with shipboard personnel. The final section will provide specific recommendations for building awareness and training efforts into existing structures for shipboard personnel.

---

[8] Department of National Defence, "Halifax-Class Modernization (HCM) / Frigate Life Extension (FELEX) Backgrounder," DND/CAF website, last modified 6 July 2018, http://www.forces.gc.ca/en/news/article.page?doc=halifax-class-modernization-hcm-frigate-life-extension-felex/hkm9beb0

[9] Department of National Defence, *High-Level Design Systems Security Risk Assessment Report for* Halifax-*Class Internet Services to Sailors System…,* 12.

SECTION 1: THE RCN CYBER PROBLEM SPACE

This section will introduce the importance of the human factor in maintaining a cyber-resilient force. Next, it will discuss the threat environment through a number of historical examples. Finally, it will argue that many of the institutional challenges to increasing the cybersecurity culture result from the network infrastructure taxonomy on board *Halifax*-class ships that results in dispersion of responsibility, disparity in training and weaknesses in reporting processes.

The Human Factor and Building Resilience

In the cybersecurity domain, the human factor is more vulnerable than any technical exploit.[10] Up to 95 percent of cyber attacks have a connection to a human error or a social engineering operation by a malicious actor.[11] One of the main advantages that the RCN, has over other many non-military organizations is that there is already an ingrained security culture. Physical security controls are generally robust and shipboard personnel undergo regular training to ensure proficiency. In force protection terms, the RCN presents a hard target to malicious actors in the physical realm, offering some advantage in the cyber realm because network components are difficult to access directly. In the cyber realm, however, physical access to the target of attack is unrequired, and adds significant risk to the attacker, making it an unlikely vector. For this reason, the existing physical security culture of shipboard personnel needs to be expanded to the cyber domain.

---

[10]A. Da Veiga and J.H.P Eloff, "An Information Security Governance Framework," *Information Systems* Management 24, no. 4 (2007): 362.

[11] Department of Defense, *Department of Defense Cybersecurity Culture and Compliance Initiative,* (Washington: Secretary of Defense, September 2015), i.

When considering RCN operations, there are four key risks that must be considered in the human domain with respect to cyber security. First, the risk of a lapse in physical security controls on board the ship which allows a malicious actor access to the cyber infrastructure of the ship. Second, a lapse in operational security in which a crew member releases information purposely or inadvertently about shipboard networks that opens the door to an attack. Third, the intentional deceit (social engineering) of a crew member through a phishing attack or similar method that enables access to shipboard systems or injects a vulnerability.[12] Fourth, a malicious actor could compromise a crew member's personal electronic device and introduce a threat to the ship.

The most critical step in mitigating these risks is to build awareness and conduct training at all levels to recognize when something is wrong through effective training, establish effective reporting channels and accept mistakes to encourage reporting and contribute to a learning culture.

To illustrate the necessity of increasing the overall cyber security culture in the RCN, consider the recent vulnerability testing exercises conducted in nine *Halifax*-class ships as a combined effort by several teams over the past year.[13] After having provided general cyber awareness briefings, the training team sent a number of targeted phishing emails to members of the ships' companies inviting the recipients to click a hyperlink.[14] The emails had clear indicators of being phishing attempts, such as having incorrect originator email addresses and suspicious hyperlink addresses. During the first six

---

[12] Phishing is a cyber attack in which a malicious actor sends an email with the goal of enticing the recipient to reveal information, send sensitive details or money, or place malware on the recipients system. Spear phishing is a more advanced attack in which the sender specifically targets the recipient and poses as a trusted sender.

[13] The team was comprised of staff from Sea Training Group, Maritime Component Commander Cyber Ops, the Directorate of Naval Information Warfare and Maritime Forces Pacific Headquarters.

[14] Christopher Heckman, "RCN Cyber Strategy 2018-2025 Briefing version 1.0," powerpoint presentation, (Ottawa: Directorate of Naval Information Warfare, March 2019), slide 8.

exercises, out of 311 phishing emails, 25 percent of the users clicked on the simulated malicious link. On board one ship, there was a 58 percent success rate for the attack.[15] It should be noted that these exercises were relatively unsophisticated cyber-attacks, and indicates that the questioning attitude required in the RCN cybersecurity culture needs to be further developed.

A recent United States Navy (USN) Cybersecurity Review stated that their "culture is characterized by a lack of understanding and appreciation of the threats, and an inability to anticipate them."[16] The results of the initial vulnerability testing exercise described above suggest that there are similar problems in the RCN, indicative of a weak cybersecurity culture.

Threat Environment

The cyber threat environment is a complex world of malicious actors ranging from lone hackers to fully developed state cyber warfare capabilities. What is beyond debate is the fact that cyber conflict is already occurring on an ever-increasing scale, making *Halifax*-class ships a possible target, particularly for state actors. The scale of the problem is evident in a 2015 US Department of Defense (DoD) document, stating that in a 10 month period, there were 30 million attempts to penetrate DoD systems, of which approximately 0.1 percent were successful.[17] The current United States Navy (USN) Chief of Naval Operations put the situation in context when he stated that "the threats

---

[15] MCC Cyber Ops and Plans and MARPAC N6 IPG, "CRR 3-15 Briefing: Cyber Security and Threat Awareness Brief," powerpoint presentation, last accessed 25 April 2019, http://halifax.mil.ca/SEA_TRG/pages/references.html

[16] Department of the Navy, *Secretary of the Navy Cybersecurity Readiness Review,* (Washington: Secretary of the Navy, March 2019), 7.

[17] Department of Defense, *Department of Defense Cybersecurity Culture and Compliance Initiative,* (Washington: Secretary of Defense, September 2015), 1.

reach well beyond what you would consider a traditional computer or information technology network into the control systems and indeed almost every aspect of our…Navy mission."[18]

The USN was forced into a proactive posture on cybersecurity after an embarrassing 2012 attack on their unclassified Smart Web Move website, in which a hacker group stole the personal information of 220 000 USN personnel and their families, followed by the penetration of the USN unclassified computer network by hackers in 2013.[19] In 2018, there was a credible report that Chinese government hackers had stolen a "massive amount of highly sensitive data related to undersea warfare" from a Navy contractor.[20] These two incidents demonstrate the breadth of threat vectors and motivations. The first attack on the Smart Moves website was conducted by a hacker group with assistance from a USN sailor, who claimed that his motivation was recreational.[21] The second attack on the Navy contractor was attributed by a group supported by the Chinese government, with motivations that can be assumed to be to gain an advantage on American defence capabilities.[22]

Both of the above examples were related to information theft on traditional computer networks. Reports about attacks that have impacted mission-critical networks on board naval ships are difficult to find in the unclassified domain, however, given the

---

[18] Admiral John Richardson, Quoted in: Deputy Chief of Naval Operations for Information Warfare, "The Cyber Threat is Real," USN website, last modified 2 October 2017, https://www.navy.mil/submit/display.asp?story_id=102685

[19] Department of Justice, "Former Navy Nuclear System Administrator Charged with Hacking the United States Navy and National Geospatial-Intelligence Agency's Computer Systems," news release, last modified 5 May 2014.; Department of the Navy, *Secretary of the Navy Cybersecurity Readiness Review,* (Washington: Secretary of the Navy, March 2019), 12.

[20] Ellen Nakashima and Paul Sonne, "China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare," *The Washington Post* 8 June 2018, last accessed 20 April 2019.

[21] Department of Justice, "Former Navy Nuclear System Administrator Charged….

[22] Ellen Nakashima and Paul Sonne, "China hacked a Navy Contractor…

often-used example of the Stuxnet virus that took control of and destroyed components of Iranian nuclear facilities in 2010, it does not take a significant leap of logic to assume that sufficiently sophisticated malicious actors could direct an attack at the machinery control and combat management systems of a warship.[23]

In the aftermath of the collision of the USS *Fitzgerald* and a container ship in 2017, the USN conducted a comprehensive cyber assessment of the ship, demonstrating that there was concern about a cyber nexus to the accident at the most senior levels of leadership.[24] While the existing evidence suggests that the *Fitzgerald* collision was not attributable to a cyber vulnerability, the US Government Accountability Office reported in late 2018 that "test teams were able to defeat weapon systems cybersecurity controls," with an example of a two-person team gaining full control of a weapon system within one day.[25] The same report indicates that there were mission-critical vulnerabilities discovered in nearly every weapon system that they assessed.[26]

Complicating the situation, threats are not limited to targeted attacks against a specific military system. The combat, engineering, communications, navigation and administrative networks on board *Halifax*-class ships are based primarily on commercial off-the-shelf (COTS) hardware and software. The majority of Western militaries have moved to COTS solutions due to the significantly reduced costs of procurement

---

[23] Nicolas Falliere, Liam O Murchu and Eric Chien, *W32.Stuxnet Dossier* version 1.4, (Cupertino: Symantec Corporation, 2011), 1-3.

[24] C-SPAN, "Transcript of the Deputy Chief of Naval Operations testimony to the House Armed Services Committee," website, last modified 7 September 2017, https://www.c-span.org/video/?433297-1/admirals-testify-naval-warship-accidents&start=3641; Vice-Admiral William Moran testified about the accident investigation: "we added cyber to the list, because of obvious concerns that everything we operate has a cyber component to it."

[25] Government Accountability Office, *Weapon Systems Cybersecurity: DoD Just Beginning to Grapple with Scale of Vulnerabilities*, (Washington: US GAO, October 2018), 21-22.

[26] *Ibid*.

compared to bespoke military-specific equipment.[27] The impact of this shift in technology has been to widen the scope of vulnerabilities of the systems to include not only exposure to targeted attack, but also exposure to general threats against vulnerabilities inherent to the COTS hardware and software. A recent example of this type of general threat is the Meltdown vulnerability discovered in a wide range of modern microprocessors.[28] There is an ever-increasing number of these vulnerabilities being stockpiled by various organizations around the world.[29]

The complex threat environment is evolving rapidly, and it is highly likely that vulnerabilities are already known to adversaries.[30] In the growing shipboard network of networks, the RCN needs to increase the cybersecurity culture at every level and embrace the USN philosophy of "every sailor a cyber sentry."[31]

Network Taxonomy – The System of Systems

Having established the significant threat environment, it is important to understand the overall taxonomy of cyber systems within the *Halifax*-class, as there are ramifications to the cybersecurity efforts as a result of the dispersion of users, technicians and institutional managers. The networks on board the *Halifax*-class ships can be divided

---

[27] J.T.D.S. Turner, "Buy Cyber-Secure: Improving Cybersecurity of Procured Combat Systems," Master of Defence Studies Directed Research Project, Canadian Forces College, 2016, 3-4.

[28] Lily Hay Newman, "The Elite Intel Team Still Fighting Meltdown and Spectre," *Wired Online* (3 January 2019), last modified 3 January 2019, https://www.wired.com/story/intel-meltdown-spectre-storm/

[29] Lillian Ablon and Andy Bogart, *Zero Days, Thousands of Nights,* (Santa Monica: RAND Corporation, 2017), x-xi.

[30] Department of the Navy, *Secretary of the Navy Cybersecurity Readiness Review…,* 7.

[31] *Ibid.,* 22.

into four general domains, which can be generalized across military equipment in general.[32]

The first domain comprises the *Information Technology* (IT) networks of hardware and software integral to the traditional computer networks on board. These networks enable crew access to the Ship Local Area Networks (ShipLAN) and onward access to the Defence Wide Area Network (DWAN) and other networks such as the Defence Resource Management Information System (DRMIS) and human resource management networks for personnel management and health services. Many users also have access to the classified networks through the Secure Local Area Network (SecLAN).[33] The IT on board the ships does not differ significantly from that found in facilities ashore, or in a private business, and is generally susceptible to the same threats. IT is managed by the Naval Communicator (NavComm) occupation within the Operations Department. The networks are accessed by everyone on board, and there is significant support to this system from shore-based network operations centres. The Assistant Deputy Minister (Information Management) (ADM(IM)) is the responsible authority for most of this equipment.

The second domain is *Operational Technology* (OT), which are systems that control physical devices. The primary example of on-board OT is the IPMS that monitors and controls the propulsion, electrical, damage control and auxiliary systems on board the ship. The IPMS is analogous to the Industrial Control Systems/Supervisory Control and

---

[32] Definitions are from the Department of National Defence*, Royal Canadian Cyber Strategy 2018-2025 version 1* RDIMS #426259 (Unapproved DRAFT), (Ottawa: Director of Naval Information Warfare 6-4, n.d.), 2, 22-23.; The fourth domain "Morale Technology" was created by the author to differentiate it from the rest of the IT on board due to the considerable difference in cybersecurity concerns

[33] Jennifer Waywell, "Cyber Security and the Halifax-Class Modernization," *Maritime Engineering Journal* 82 (March 2017), 20-21.

Data Acquisition Systems (ICS/SCADA) that are used in industrial applications and critical infrastructure around the world, such as in manufacturing facilities and power plants. OT is the type of technology which was attacked by Stuxnet. In the case of IPMS, while the primary users of this equipment for control functions are the Marine Technicians (MarTechs) within the Marine Systems Engineering Department, parts of the system are accessed from remote terminals throughout the ship by a wide range of users during damage control operations. While the specific L3 MAPPS IPMS in use on board the *Halifax*-class is in use by 18 navies worldwide, it is niche equipment within the CAF when compared to the IT assets across the organization.[34]

The third domain is *Platform Technology* (PT), which is the cyber infrastructure that controls the weapons, C4ISR and navigation systems on board.[35] In the *Halifax*-class, the primary example of PT is the integrated CMS330, including the hardware and software that control the individual components of the system, such as the gun, missile systems, radars, tactical data link and the interrogation friend or foe (IFF) system.[36] While one can draw comparisons to the proprietary navigation, radar and control equipment on board commercial aircraft and ships, for much of PT, there is no civilian equivalent to many aspects of it due to the specific military applications of the technology. These systems are used by a large percentage of the ship's company within the Operations Room and in a variety of equipment spaces. The technicians responsible for these networks at sea are the Weapons Engineering Technicians (WEng Techs) within the Combat Systems Engineering Department.

---

[34] Naval Technology. "L3 MAPPS Integrated Platform Management Systems," website, last accessed 2 May 2019, https://www.naval-technology.com/contractors/consoles/l-3-mapps2/

[35] C4ISR means command, control, communications, computers, intelligence, surveillance and reconnaissance.

[36] Jennifer Waywell, "Cyber Security and the Halifax-Class Modernization," ..., 21.

The fourth domain, which will be referred to as *Morale Technology* (MT) is the recent addition of the IS2S system that enables the connection of personal electronic devices (PEDs) to the internet from within the ship while at sea. This network is a subset of IT, but it differs considerably from the other IT onboard in that it is the only system into which a crewmember can legally connect personal devices, including mobile phones, computers and gaming devices. It also differs in that there is no monitoring of internet traffic, and no intention to do so.[37] The ship's infrastructure is managed by the Naval Communicators, but there is no management of the PEDs which connect to it. The authorities for OT, PT and MT reside within the Assistant Deputy Minister (Materiel) (ADM (Mat)) Group.[38]

The most significant difference relevant to the increase of cybersecurity awareness and training between these domains is that there is a dispersion of responsibility amongst different occupations for the operation, and a division of responsible authorities at the institutional level resulting in cybersecurity culture gaps, particularly within the mission-critical OT and PT domains. This theme will be discussed in further detail in the next section.

---

[37] Department of National Defence, *High-Level Design Systems Security Risk Assessment Report for* Halifax-*Class Internet Services to Sailors System…,* 14.

[38] Christopher Heckman, telephone conversation with author, 23 April 2019; LCdr Heckman is the RCN Senior Staff Officer for Cyber Policy and Readiness within the Directorate of Naval Information Warfare.

SECTION 2: OBSTACLES TO BUILDING RESILIENCE

This section will discuss the institutional obstacles to creating a robust cybersecurity culture by highlighting the impact of the dispersion of responsibility for network systems, the complexity of the governance structure in place and the slow pace of change for holistic institutional initiatives. It will conclude by recommending that low-level simple changes in targeted areas can have a greater immediate impact on creating a more robust cybersecurity culture.

Dispersion of Responsibility, Lack of Training

The dispersion of responsibility for at-sea technical support across three different departments for the four technology domains within the ship has created silos of differing training and ability that has resulted in gaps in the human firewall that must be filled to create cyber-resiliency. The NavComm occupation group has been dealing with IT for many years and the requisite cybersecurity training has been formally built into their career paths.[39] One of the leading cyber experts in the RCN led a Canadian cybersecurity team composed of NavComms to the international military Exercise CYBER FLAG in 2018. Based on his experience, he assessed NavComm formal training as adequate to meet significant cybersecurity challenges.[40] On the other hand, there is no formal cybersecurity training provided to the MarTechs who act as IPMS Technicians (OT), nor to the WEng Techs who provide support to most of the PT onboard.[41] This issue is

[39] Mark Chambers, email to the author, 8 April 2019. CPO1 Chambers is the NavComm Occupation Manager at the Directorate of Naval Personnel & Training.

[40] Christopher Heckman, telephone conversation with the author, 23 April 2019.

[41] Meryl Sponder, email to the author regarding lack of cybersecurity training for WEng Techs who work on PT, 15 April 2019. LCdr Sponder is the Sea Training Pacific Combat Systems Engineering Officer and confirmed the fact with the Naval Training Development Centre.; Adrian Mascarenhas, email

recognized within the RCN, and a cyber training needs analysis (TNA) is in the concept stage.[42] The TNA is expected to take several months, which will be followed by a significant time to incorporate the training into formal career courses and to create delta-training for those already in the Fleet.

The other significant institutional challenge is the different reporting structure for incidents. Assistant Deputy Minister (Information Management) (ADM (IM)) as the Joint Cyber Force Commander is primarily focused on IT-related incidents. There is strong shore support for IT incidents through shore-based network operations centres and ultimately to the Canadian Forces Network Operations Centre (CFNOC). Enterprise tools, including network monitoring, malware detection and firewalls are widely available and in use.[43]

There is a less robust identification and reporting structure for OT and PT issues. While acknowledging that vulnerabilities can exist in IT and remain unrecognized or dormant, it is more difficult to pinpoint an issue with PT and OT as being related to a cyber-vulnerability. If equipment associated with PT and OT fails as a result of a cyber vulnerability or exploit, it would likely require repeated similar incidents either in one ship or across multiple ships to recognize a software issue as the underlying cause, particularly if the fault cleared with a system reboot, masking indications of a cyber vulnerability. The normal reporting scheme for equipment failures in this case is through the Naval Operational Deficiency (NAVOPDEF) process.[44] This process alerts the

---

to the author regarding lack of cybersecurity training for MarTechs who work with IPMS, 8 April 2019. LCdr Mascarenhas is the acting section head for the group that is responsible for IPMS to ADM(Mat).

[42] David Mercer, email to the author, 22 April 2019. Cdr Mercer is a strategic training manager at the Directorate of Naval Personnel and Training.

[43] LCdr Christopher Heckman, telephone conversation with the author, 23 April 2019.

[44] Royal Canadian Navy. *Naval Order 3250-7 Royal Canadian Navy Operational Deficiency Process*, (Ottawa: Royal Canadian Navy, 2016).

operational authority that a ship has lost a capability and describes the anticipated operational impact to the ship's mission. NAVOPDEFs contain a number of details about the fault, and shore authorities will investigate the issue, however, because of the large number of NAVOPDEFs generated, the operational prioritization of assessing issues and the limited human resources to deal with the Canadian Fleet, the recognition of patterns indicative of cyber vulnerabilities requires a dedicated effort of data collection and analysis, for which the human resources and system does not yet exist. Adding to this challenge is that classification issues often restrict the number of personnel ashore who can access and work with the data.[45]

The dispersion of responsibility for the technology domains in the *Halifax*-class ship at all levels is a recognized concern.[46] Because of the complexity of the process required to change formal training across several occupation groups, and the lack of human resources to manage and track NAVOPDEF issues, these problems will take years to address, during which time systems remain vulnerable.

Complexity of Governance and Bureaucratic Obstacles

The complexity of existing regulations and directives governing cybersecurity is significant. Among the regulations and directives that must be considered include the Treasury Board's Operational Security Standard for Management of Information Technology Security, the National Defence Security Orders and Directives, the Communications Security Establishment Canada's IT Security Risk Management policy (ITSG-33), at least 13 Defence Administrative Orders and Directives, along with coastal

[45] LCdr Christopher Heckman, telephone conversation with the author, 23 April 2019.
[46] *Ibid.*

policies and local unit policies.[47] It is an overwhelming amount of information, even for a specialist in the field. The regulatory framework and number of organizations involved slows the development and approval of any new strategies to improve the understanding and awareness of the end-user on board a ship.

Despite these challenges, the Canadian Armed Forces (CAF) have embraced the need to improve the cybersecurity posture at the most senior levels. The extant Canadian Defence Policy, *Strong, Secure, Engaged* contains several initiatives to introduce more robust cyber capabilities. Most relevant to this paper is initiative 65, which states that the CAF shall implement "cyber security and situational awareness projects [and] cyber threat identification and response."[48] This initiative is easier described than achieved. As an example, the RCN Cyber Strategy has been under consideration for approval since 2017.[49]

The Way Ahead

The RCN is limited in its human resources to develop new cybersecurity awareness programmes, update training packages and create the necessary governance documentation to support new policy. Moving these documents through the bureaucratic system takes a great deal of time, which is then followed by an implementation period for tactical level units. Methods of rapidly effecting cultural change through existing processes must be created to address the threats.

---

[47] As an example of the numerous directives, see: Assistant Deputy Minister (Information Management). "IT Security Policies," DWAN website, last accessed 5 May 2019, http://admim-smagi.mil.ca/en/security/policies-standards/index.page.

[48] Department of National Defence, *Strong, Secure, Engaged: Canada's Defence Policy*, (Ottawa: Department of National Defence, 2017), 41.

[49] Department of National Defence*, Royal Canadian Cyber Strategy 2018-2025 version 1…*

SECTION 3: LEVERAGING EXISTING FRAMEWORKS

This section will provide three specific recommended actions that can be used to leverage existing frameworks for training that can be rapidly instituted in the RCN to build awareness, increase the efficacy of training and better enable command-decision making with respect to cybersecurity on-board *Halifax*-class ships.

The first recommendation is to map all network dependencies to all activities in RCN training and readiness documentation. The second recommendation is to make a small change in the NAVOPDEF reporting process to catalyze discussion and awareness of cybersecurity and enable data collection. The final recommendation is to start building a "just culture" similar to that used in the Royal Canadian Air Force for their successful Flight Safety Program

The key factors in determining these recommendations were that they can be applied in a relatively short timeframe under RCN authority, they will be pertinent to all shipboard personnel (rather than specific occupational groups), and despite their relative simplicity, they will target documentation and activities that shipboard personnel engage with on a daily basis. The initiatives will create a more robust foundation for larger scale initiatives that are anticipated, including the introduction of CAF Cyber Operators on board ships, the creation of Fleet Cyber Units ashore, and better data availability for ADM(IM) and ADM(Mat) personnel to identify potential cyber vulnerabilities through analytics.[50]

[50] *Ibid.,* 22.

Integrating Cyber into Collective Training Events Through Network Mapping

Mapping operational network dependencies has been identified as an important element to achieving military cyber mission assurance at the unit level.[51] Understanding the impacts of a cyber-denied environment by evaluating and disseminating the expected impacts of a cyber attack will improve the planning and training at the tactical level. This section describes a recommended method of implementing this strategy within the RCN.

In the RCN, a key element of generating and sustaining forces is the collective training process. As a ship moves through a tiered-readiness program from extended-readiness, to normal-readiness and ultimately to high-readiness, it becomes capable of accomplishing increasingly complex and risky missions.[52] Attaining these levels for a ship requires validation of the correct personnel assignment (with appropriate individual training), ensuring materiel readiness and successfully completing collective training events.[53] Of these three pillars of readiness, the one that is most relevant to quickly increasing the shipboard understanding of cyber dependencies is that of collective training.

The high-level requirements for collective training on board RCN ships are contained within *CFCD 129: Royal Canadian Navy Readiness and Sustainment Policy*. Of note, in the current version published in 2018, there is only one minor explicit reference to cybersecurity.[54] The complementary governing document for the execution

---

[51] Michael D. Pritchett, "Cyber Mission Assurance: A Guide to Reducing the Uncertainties of Operating in a Contested Cyber Environment," (Graduate Research Project, Air University, 2012), 1-3.; Panayotis A. Yannakogeorgos and John P. Geis II, *The Human Side of Cyber Conflict: Organizing, Training and Equipping the Air Force Cyber Workforce,* (Maxwell AFB: Air University Press, 2016), 148.

[52] Department of National Defence, *CFCD 129 Royal Canadian Navy Readiness and Sustainment Policy,* (Ottawa: Director Naval Force Readiness, 2018), 1.; Note that each of these readiness levels is further sub-divided.

[53] *Ibid*.,10-17.

[54] Department of National Defence, *CFCD 129…,* 99.

of collective training on board ships is *CFCD 102: Combat Readiness Requirements (CRRs).*[55] This document is broken down into specific activities that must be completed by ships' teams and the validity period for a successful qualification. There have been recent CRR additions that have an overt cybersecurity nexus, including the vulnerability testing discussed earlier in the paper regarding phishing attacks on crewmembers.[56]

Both of these documents offer a tremendous opportunity to both map network dependencies for operations and to raise awareness of the impacts of cyber effects among the shipboard personnel. These documents are continually reviewed and revised by the Director of Naval Force Readiness and the Commander Sea Training Group, and therefore can be modified within a relatively short timeframe. A specific section on cybersecurity readiness should be added to *CFCD 129*, followed by a revision of the *Halifax*-class readiness matrix that includes specific cybersecurity elements as part of the required capability requirements at each readiness level.[57] An argument could be presented that the cybersecurity requirements are already implicit in the requirements for warfare; however, this does not currently accomplish the effect of explicit dependency-mapping, and the resulting increase in operationalization of the cyber warfare domain.

More importantly, and flowing from the above updates to *CFCD 129*, every combat readiness requirement in *CFCD 102* should include a paragraph stating the network dependencies within the IT, OT and PT domains for each training activity. At this fidelity, the impacts on specific mission tasks would be clear to the ship's planning

---

[55] Department of National Defence, *CFCD 102(N) Royal Canadian Navy Readiness and Sustainment Policy,* (Ottawa: Commander Sea Training Group, 2018).

[56] *Ibid.*; There are three inter-related CRRs. The first is a cybersecurity lecture, followed by a table top discussion and culminating with the phishing email exercise described earlier in the paper.

[57] Department of National Defence, *CFCD 129…*, Annex A to Chapter 4.

staff and would serve as a catalyst for discussion and analysis with the command team and collective training validation staff.

It is important to note that this document is referred to on a routine basis by all leadership staff on board an RCN ship to plan, execute and evaluate exercises. By targeting *CFCD 102* for revision, an immediate impact will occur within the Canadian Fleet because of this routine engagement. In comparison, a new high-level strategy document, while important, will take much longer to filter down and will be unlikely to contain concrete steps to take at the tactical level, thereby limiting the short-term change on the overall organizational culture. Ultimately, at high-readiness levels, the network mapping information will enable training scenarios that include simulated cyber-contested environments in which networks are degraded or denied in order to test the crew during practical exercises. The Deputy Chief Information Security Officer for the USAF advocated for this type of cyber-contested training with the caveat that there is a "cost of proficiency and capability when the enemy does not contest the environment and all systems are working."[58] This is a valid concern that would have to be balanced by commanders. Having the tools and knowledge readily available, however, is undoubtedly better than not having a complete understanding of the dependencies within a ship.

Formalizing Cyber Reporting in Existing Processes

The second recommendation is to add a specific cyber field to the NAVOPDEF message format. This field would be required in every message, recognizing the primacy of cyber assets across all warfare domains. This simple change would accomplish two

[58] William D. Bryant, "Surfing the Chaos: Warfighting in a Contested Cyberspace Environment." *Joint Force Quarterly* no. 88 (2018): 33.

goals. The first is that it would ensure that tactical level assessments of potential cyber impacts are being considered. By including the field in a message, the consideration would have to be consciously made by the technicians and officers who draft the messages. Given the extant culture on board RCN ships, NAVOPDEFs are reviewed and discussed in detail by the responsible technical officer, the operations officer and the commanding officer before they are approved for release to an operational authority. Including an overt *cyber considerations* paragraph, it would necessarily become part of the discussion.

The second goal that would be accomplished is that the tactical assessment of potential cyber issues and vulnerabilities would be captured such that when institutional level processes create the ability to conduct robust analytics on potential cyber vulnerabilities, they will have access to a historical record of these tactical assessments to build the data set. This is a potential task to be conducted by specialist Fleet Cyber Units that are being considered for each coastal Fleet.[59] The data set would also be useful to develop and prioritize collective training efforts in the cyber domain.

This recommendation is open to criticism that the personnel at the tactical level do not have the expertise to make cyber assessments. The consideration and discussion that would result from the small change, however, is a worthy goal in itself to build an awareness of the pervasiveness of the cyber domain throughout naval operations.

Creating a "Just Culture" for Cybersecurity

The final recommendation is to create a *just culture* in the context of cybersecurity on board ships modelled after the Royal Canadian Air Force's (RCAF)

[59] Department of National Defence*, Royal Canadian Cyber Strategy 2018-2025 version 1…*11.

successful Flight Safety Program.[60] This recommendation is more complex to implement than the first two, but is likely the most important for improving the RCN cybersecurity culture.

A holistic attempt to describe a complete cybersecurity program based on the Flight Safety Program is beyond the scope of this paper, but the critical theme that should be adopted is that "personnel are able to report occurrences, hazards or [security] concerns…without fear of sanction or embarrassment."[61] The idea of a *just culture* is one that agrees on acceptable and non-acceptable behaviour and only seeks punitive action for "negligence or wilful, deliberate deviations."[62]

The benefit that this culture would bring to the RCN is an increased willingness of personnel to self-report cybersecurity incidents, allowing for the development of a learning culture in which patterns of recurrent human errors in the cyber domain can be recognized and used as examples to enable policy changes, better individual and collective training and further build the awareness of the cyber domain.

By returning to the example of the simulated phishing attacks conducted against *Halifax*-class ships over the past year, the fact emerges that a large percentage of shipboard personnel were demonstrated to be vulnerable, even to unsophisticated attacks. Additional data from these exercises also showed that the majority of personnel did not report the suspicious emails, despite having been exposed to cybersecurity awareness

---

[60] Department of National Defence, A-GA-135-001/AA-001, *Flight Safety for the Canadian Armed Forces,* (Ottawa: Department of National Defence, 2018).

[61] *Ibid.,…*1-5/11.; the word "safety" in the original has been changed to "security" to fit the context.

[62] *Ibid.*

training. Of the 311 phishing emails sent, only 11 were reported to the Information Systems Security Officer.[63]

With the introduction of the IS2S system, and the resulting exponential increase in uncontrolled cyber access into the ship, it is inevitable that many human errors will be made, whether it is the inadvertent violation of operational security or a compromised PED being exposed to other technology domains on board the ship, it is therefore more urgent than ever to encourage personnel at all levels to self-report these errors so that corrective action can be taken to protect the cyber assets of the ship.

This recommendation could be criticized in that it would take a significant amount of time and work to implement, contrary to the criteria established at the beginning of this section, however, if approached in a phased implementation led by collective training teams and commanders, the initial benefits to the institution could be seen relatively quickly.

Summary

The three specific recommendations in this section were to map operational cyber dependencies into existing training and readiness documentation, add a cyber field to the NAVOPDEF message format and to make the initial steps toward creating a cybersecurity *just culture*. By implementing these efforts, a much more rapid positive impact to the shipboard cyber-resilience could be realized.

[63] MCC Cyber Ops and Plans and MARPAC N6 IPG, "CRR 3-15 Briefing: Cyber Security and Threat Awareness Brief," powerpoint presentation, last accessed 25 April 2019, http://halifax.mil.ca/SEA_TRG/pages/references.html

CONCLUSION

This paper argued that the current state of cyber resilience on board *Halifax*-class vessels is not sufficient to meet the existing threats due to a lack of effective cyber-awareness training and the relatively slow pace of implementing RCN-wide governance and formal training updates.

The slow pace can be attributed to several factors. The dispersion of technical responsibility for different technology domains across occupational groups and shore authorities necessitates a number of concurrent formal amendments to training regimes across the institution. There are weaknesses in the reporting process and data analysis for cyber threats and vulnerabilities, particularly in the realms of OT and PT. There is a very small cadre of personnel within the RCN structure who are specifically focused on cybersecurity, which creates a significant challenge to manage the massive array of considerations and activities required to sufficiently deal with the ever-changing and often anonymous threat.

Despite these issues, three specific recommendations were made to leverage existing frameworks within the RCN and the RCAF to catalyze awareness, discussion and a shift in culture at the tactical level in a more compressed timeframe and in a way that will complement the implementation of future institutional cyber initiatives. Once cybersecurity training is formally established throughout RCN occupational training programs, a preceding overall increase in cybersecurity awareness on board the ship will help close the gap for those with legacy training.

While human errors are one of the most significant contributors to cybersecurity incidents, a competent workforce can conversely be a tremendous firewall to prevent

these incidents when empowered by the learning culture that is demanded in this complex operational domain.

BIBLIOGRAPHY

Ablon, Lillian and Andy Bogart. *Zero Days, Thousands of Nights.* Santa Monica: RAND Corporation, 2017. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1751/RAND_RR1751.pdf

Blakely, Darlene. "Information as War." *Bits and Bytes: The Information Warrior's Newsletter* vol.1, no. 3. Ottawa: Royal Canadian Navy Directorate of Naval Information Warfare, October 2018.

Bryant, William D. "Surfing the Chaos: Warfighting in a Contested Cyberspace Environment." *Joint Force Quarterly* no. 88 (2018): 28-33.

Canada. Assistant Deputy Minister (Information Management). "IT Security Policies," DWAN website, last accessed 5 May 2019, http://admim-smagi.mil.ca/en/security/policies-standards/index.page.

———. Department of National Defence. A-GA-135-001/AA-001. *Flight Safety for the Canadian Armed Forces.* Ottawa: Department of National Defence, 2018.

———.Department of National Defence. *CFCD 102(N) Royal Canadian Navy Combat Readiness Requirements.* Ottawa: Commander Sea Training Group, 2018. http://halifax.mil.ca/SEA_TRG/pages/references.html

———. Department of National Defence. *CFCD 129 Royal Canadian Navy Readiness and Sustainment Policy.* Ottawa: Director Naval Force Readiness, 2018. http://halifax.mil.ca/SEA_TRG/pages/references.html

———. Department of National Defence. *High-Level Design Systems Security Risk Assessment Report for* Halifax-*Class Internet Services to Sailors System* 2183A-2100-02-10-02 (DNPS 9-4-2). Ottawa: Director Naval Propulsion Systems, 9 August 2018.

———. Department of National Defence. Maritime Component Commander Cyber Operations and Plans and Maritime Pacific Headquarters N6 IPG, "CRR 3-15 Briefing: Cyber Security and Threat Awareness Brief," powerpoint presentation, last accessed 25 April 2019, http://halifax.mil.ca/SEA_TRG/pages/references.html

———. Department of National Defence. *Naval Order 3250-7 Royal Canadian Navy Operational Deficiency Process*, (Ottawa: Royal Canadian Navy, 2016). http://rcn-mrc.mil.ca/assets/RCN_Intranet/docs/en/NAVORDs/3250-7-eng.pdf

———. Department of National Defence. *Royal Canadian Navy Cyber Strategy 2018-2025 version 1* RDIMS #426259 (Unapproved DRAFT). Ottawa: Director of Naval Information Warfare, n.d.

———. Department of National Defence. *Royal Canadian Navy Information Warfare Strategy Paper.* Ottawa: Royal Canadian Navy, September 2016.

———. Department of National Defence. *Royal Canadian Navy Strategic Plan 2017-2022*. Ottawa: Royal Canadian Navy, 2017. http://navy-marine.forces.gc.ca/assets/NAVY_Internet/docs/en/analysis/rcn_strategicplan_2017-2022_en-s.pdf

———. Department of National Defence. *Strong, Secure, Engaged: Canada's Defence Policy.* Ottawa: Department of National Defence, 2017. http://dgpaapp.forces.gc.ca/en/canada-defence-policy/docs/canada-defence-policy-report.pdf

C-SPAN. "Transcript of the Deputy Chief of Naval Operations testimony to the House Armed Services Committee." Website. Last modified 7 September 2017. https://www.c-span.org/video/?433297-1/admirals-testify-naval-warship-accidents&start=3641

European Union Agency for Network and Information Security. *Cyber Security Culture in Organizations.* Athens: European Union Agency for Network and Information Security, 2018. https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations/at_download/fullReport

Leenan, Louise and J.C. Jansen van Vuren. *Framework for the Cultivation of a Military Cybersecurity Culture*. Reading: Academic Conferences International, Ltd, 2019. https://search-proquest-com.cfc.idm.oclc.org/docview/2198530522?accountid=9867

Nakashima, Ellen and Paul Sonne. "China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare," *The Washington Post* 8 June 2018. Last accessed 20 April 2019. https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html?noredirect=on&utm_term=.3fa94462b933

Newman, Lily Hay. "The Elite Intel Team Still Fighting Meltdown and Spectre." *Wired Online* (3 January 2019). Last modified 3 January 2019. https://www.wired.com/story/intel-meltdown-spectre-storm/

Pritchett, Michael D., "Cyber Mission Assurance: A Guide to Reducing the Uncertainties of Operating in a Contested Cyber Environment." Graduate Research Project, Air University, 2012. https://apps.dtic.mil/dtic/tr/fulltext/u2/a563712.pdf

Turner, J.T.D.S. “Buy Cyber-Secure: Improving Cybersecurity of Procured Combat Systems.” Master of Defence Studies Directed Research Project, Canadian Forces College, 2016. https://www.cfc.forces.gc.ca/papers/csc/csc42/mds/turner.pdf

United States of America. Department of Justice. “Former Navy Nuclear System Administrator Charged with Hacking the United States Navy and National Geospatial-Intelligence Agency’s Computer Systems.” News Release.Last modified 5 May 2014. https://www.justice.gov/usao-ndok/pr/former-navy-nuclear-system-administrator-charged-hacking-united-states-navy-and

———. Department of the Navy. *Secretary of the Navy Cybersecurity Readiness Review.* Washington: Secretary of the Navy, March 2019. https://www.navy.mil/strategic/CyberSecurityReview.pdf

———. Department of the Navy. *Commander’s Cyber Security and Information Assurance Handbook* Revision 2 - COMNAVCYBERFORINST 5239.2A. Norfolk: Commander Navy Cyber Forces, 2013. https://www.cool.navy.mil/usn/ia_documents/5239_NCF_Cybersecurity_IA_HANDBOOK.pdf

———. Department of the Navy. *Commander’s Cybersecurity Manual* Version 4 – COMNAVIDFOR M-5239.2D. Norfolk: Commander Navy Information Dominance Forces, 2016. http://navybmr.com/study%20material/COMNAVCYBERFORINST%205239.2D.pdf

———. Deputy Chief of Naval Operations for Information Warfare. “The Cyber Threat is Real,” USN website. Last modified 2 October 2017. https://www.navy.mil/submit/display.asp?story_id=102685

———. Government Accountability Office. *Weapon Systems Cybersecurity: DoD Just Beginning to Grapple with Scale of Vulnerabilities*, Washington: US GAO, October 2018. https://www.gao.gov/products/GAO-19-128

Veiga, A. Da and J.H.P Eloff, “An Information Security Governance Framework,” *Information Systems* Management 24, no. 4 (2007): 361-372. https://search.proquest.com/docview/214123813?pq-origsite=summon

Waywell, Jennifer. “Cyber Security and the Halifax-Class Modernization.” *Maritime Engineering Journal* 82 (March 2017): 19-23.

Yannakogeorgos, Panayotis A. and John P. Geis II. *The Human Side of Cyber Conflict: Organizing, Training and Equipping the Air Force Cyber Workforce.* Maxwell AFB: Air University Press, 2016. https://www.airuniversity.af.edu/AUPress/Cyber-Power-Papers/