National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

NAVAL CYBER WARFARE CAPABILITY REQUIREMENT

LCdr J.M. Lanouette

JCSP 42	PCEMI 42
Service Paper	**Étude militaire**

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.

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 42 – PCEMI 42
2015 – 2016

JCSP SERVICE PAPER – PCEMI ÉTUDE MILITAIRE

NAVAL CYBER WARFARE CAPABILITY REQUIREMENT

LCdr J.M. Lanouette

Word Count: 2304

Compte de mots: 2304

NAVAL CYBER WARFARE CAPABILITY REQUIREMENT

AIM

1. The aim of this service paper is to identify the requirement for a cyber defence capability in the Royal Canadian Navy (RCN). Current initiatives within the Canadian Armed Forces (CAF) under Director General Cyber Force Development (DG Cyber FD) are studying the general cyber warfare requirements of DND and the government of Canada, however these are mostly focused on enterprise and land based networks. The naval environment, and more specifically, ships deployed at sea require a separate capability to deal with cyber threats.

INTRODUCTION

2. In recent years, reports of cyber attacks on government, defence contractor, industry and western military networks have been widely reported.[1] These attacks were targeting information, usually intellectual property or weapon system designs, to be exploited for either commercial or economic gains, or for military technical advantages. Attacks such as Stuxnet revealed that critical infrastructures and industrial control systems, such as power generation stations and nuclear refinement facilities, were not

[1] Mandiant Intelligence Center, "APT1: Exposing One of China's Cyber Espionage Units" (Mandiant, 2013); Ellen Nakashima, "Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyberspies - The Washington Post," accessed November 9, 2015, https://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html; Aditya K. Sood and Richard Enbody, "U.S. Military Defense Systems: The Anatomy of Cyber Espionage by Chinese Hackers | Georgetown Journal of International Affairs," accessed November 10, 2015, http://journal.georgetown.edu/u-s-military-defense-systems-the-anatomy-of-cyber-espionage-by-chinese-hackers/; Siobhan Gorman, "Electricity Grid in U.S. Penetrated By Spies," *Wall Street Journal*, April 9, 2009, sec. Tech, http://www.wsj.com/articles/SB123914805204099085; Richard Clarke, "China's Cyberassault on America," *Wall Street Journal*, June 15, 2011, sec. Opinion, http://www.wsj.com/articles/SB10001424052702304259304576373391101828876; Robert Windrem, "Exclusive: Secret NSA Map Shows China Cyber Attacks on U.S. Targets," *NBC News*, July 30, 2015, http://www.nbcnews.com/news/us-news/exclusive-secret-nsa-map-shows-china-cyber-attacks-us-targets-n401211.

immune to attacks simply because these infrastructures were “air gapped”[2] from the internet.[3] Further reporting highlights that critical infrastructure in the United States (US) are being attacked by China.[4]

3. These reports show that state-sponsored cyber attacks are occurring and are targeting military networks. While these attacks have been mostly limited to traditional information networks, large military platforms such as naval ships, which have several computer networks for communications, command and control, power generation, and control of propulsion systems, can be susceptible to cyber attacks. This paper will provide an analysis of the requirement for the RCN to develop its own cyber warriors to defend ships at sea from potential cyber attacks. It will present potential outcomes should a cyber attack be successful on a naval ship, without discussing actual vulnerabilities so as to keep this document unclassified. This paper will also provide supporting evidence that the US Navy is also considering the creation of a cyber warfare corps to be deployed with ships at sea. Finally, this paper will outline the requirements of an at sea cyber defence capability and provide a comparison with the current Emergency Response Team (ERT) organization and its means to maintain combat capability at sea as detailed in the RCN Emergency Response Team Manual.

DISCUSSION

4. The modernized HALIFAX class has been greatly enhanced by the incorporation of Commercial-Off-the-Shelf (COTS) equipment. While the use of COTS provides a

[2] An air gap is a physical separation of two or more networks that only allows the transfer of data via authorized scanning systems (computers) that are never connected to both networks at the same time.

[3] Kim Zetter, “An Unprecedented Look at Stuxnet, the World’s First Digital Weapon | WIRED,” accessed November 6, 2015, http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

[4] Gorman, “Electricity Grid in U.S. Penetrated By Spies”; Jian-Wei Wang and Li-Li Rong, “Cascade-Based Attack Vulnerability on the US Power Grid,” *Safety Science* 47, no. 10 (December 2009): 1332–36, doi:10.1016/j.ssci.2009.02.002.

lower barrier of entry for new trainees, it also increases the potential of malicious code (malware) being successful at corrupting data being passed over the communications networks, or disabling the ships communications. This also applies to the ship's command and control network which provides the ship's Common Operating Picture (COP) and means of controlling the ship's sensors and weapon systems as well as the ship's propulsion, power generation and damage control systems.

5. This new possible threat could impact a ship's capability to conduct its missions and even to support the three basic naval concepts: float, move and fight.[5] Float and move are supported by the ship's Integrated Platform Management System (IPMS). This system is similar to the industrial control systems used in the majority of power plants around the world as well as the system that controlled Iran's nuclear centrifuges in the Stuxnet attack.[6] Should similar malicious code to the Stuxnet example be targeted towards IPMS, it could have the potential of preventing the ship from sailing, as the system would not behave according to its fit, form and function. It could falsely report data to the operators while damaging equipment or disobeying commands given by the operators to the system.

6. Fight is supported by all the systems on the ships, for without float and move, there is no fight. As the IPMS has already been addressed, the other ships' systems, ie. the Combat Management System (CMS), the ships sensors (radars, sonars), the navigation equipment and the communications equipment all rely on various networks to provide

[5] Department of National Defence, "Securing Canada's Ocean Frontiers: Charting the Course from Leadmark" (Ottawa: Canada, 2005), 32.

[6] Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon | WIRED."

naval operators with the right information at the right time to conduct operations.[7] Should malware be introduced into the system, operators may make tactical or even operational decisions based on false information, or systems will not be available when they are most needed.

7. Significant effort has been made within the Halifax Class Modernization Project Management Office (HCM PMO) to secure the ships' systems.[8] The PMO followed the Communications Security Establishment's (CSE) Security Assessment and Authorization process outlined in the Information Technology Security Guidance 33 (ITSG-33) *IT Security Risk Management: A Lifecycle Approach* in order to determine its level of security and improve its configuration and software.[9] However, it is a certainty in the field of cyber security that any computer system or network always has security flaws, no matter the level of effort put into ensuring a secure design.[10] This means that malware can be introduced into the ship's systems and have an impact should the attackers know enough about the systems they are attacking.

8. The likelihood of malware being introduced into any of the ship's networks cannot be discussed in this document due to classification issues. However, given the sources presented in this paper that outline that cyber attacks are possible when state actors are involved in cyber campaigns, denying that the possibility of this type of attack could occur is akin to stating that Canadian warships will never be fired upon by anti-ship

[7] Nancy Brown, Danelle Barrett, and Jesse Castillo, "CREATING Cyber Warriors.," *U.S. Naval Institute Proceedings* 138, no. 10 (October 2012): 28–32.

[8] This is based on the author's previous work with the PMO as the Director of Naval Combat System's Systems Security Engineering Sub-Section Head.

[9] Communications Security Establishment, "IT Security Risk Management: A Lifecycle Approach," November 1, 2012, https://www.cse-cst.gc.ca/en/publication/itsg-33.

[10] National Institute of Standards and Technology and Department of Commerce, "NIST Special Publication 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems" (United States, September 1996), 9.

missiles (ASM), and thus do not require Electronic Support Measures (ESM) systems, tracking radars and surface-to-air missiles (SAM) to detect and prosecute incoming threats.

9. The US Navy has recognised this threat and is taking measures to face the future of naval cyber warfare. Former US Deputy Secretary of Defense, William J. Lynn III, wrote an article for the US Cyber Command Cyber Security newsletter titled *Defending a New Domain* which highlights the growing threat of cyber warfare to defence and critical infrastructure.[11] He notes that military networks are not impervious to attacks and that adversaries could introduce malware within the hardware components or the software that militaries purchase, providing “backdoors” and remote “kill switches” which could cause sudden malfunctions.[12] He argues that the US military must be able to deal with cyber attacks while they occur and be able to function with degraded systems. While operating with degraded systems is nothing new to the RCN – it is routinely practiced to simulate taking battle damage – doing so because the ship is subjected to a cyber attack brings a completely new dimension to the internal ship’s battle.

10. Vice Admiral (Retired) Nancy Brown, Captain Danelle Barrett and Lieutenant-Commander Jesse Castillo, US Navy specialists in information technology, presented a conference paper to the US Naval Institute Proceedings in October 2012 titled *Creating Cyber Warriors* in which they strongly argue that the US Navy must train a cyber warfare officer and enlisted corps that is part of the unrestricted-line, meaning that these cyber specialists would be treated as operators.[13] In this paper, they identify the requirement for

[11] William J. Lynn III, “Cybersecurity - Defending a New Domain,” *Cyber Security*, accessed February 1, 2016, http://archive.defense.gov/home/features/2010/0410_cybersec/lynn-article1.aspx.

[12] Ibid.

[13] Brown, Barrett, and Castillo, “CREATING Cyber Warriors.”

cyber warfare officers to be embarked on US Ships and should be included as a part of the operational planning process.

11. In order to deal with malware in ships' systems, there must be a capability onboard to deal with an attack. The US National Institute of Standards and Technology defines five core functions in its framework for conducting cyber security activities in critical infrastructure systems: identify, protect, detect, respond and recover.[14] Identify is the activity that determines your system's vulnerabilities. Protect is the activity that implements security safeguards to mitigate the vulnerabilities of the system, such as access control, data encryption, and security awareness training. The detect activity is the detection of malicious activity on your networks. The respond activity is the actions taken to deal with the intrusions. Finally, recover is the activity required to return the system to normal operations.[15] The first two activities are mostly conducted during the design and implementation phases of a ship project, but must be reviewed periodically to deal with new threats. The remaining activities are required on board ships to defend them from cyber attacks.

12. The detect activity requires that the ship's networks have intrusion detection systems (IDS) which will alert an operator of possible malicious activity. These systems can either alert the operator based on known malicious signatures (similar to how virus scanners work), or based on anomalous activities. Signatures require that the attack patterns have been discovered previously. The signatures must be built based on intelligence gathering of malicious actors' activities (known websites, known malicious

[14] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity" (United States, February 2014), 7, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[15] Ibid., 8–9.

files, etc). Anomaly based detections are done by previously determining the known good traffic patterns on your network and systems. Malicious activities would appear as a deviation from the known good and be flagged to the operator.[16] An example of this on a desktop personal computer would be for Microsoft Word to attempt to access an external website without interaction from the user. These systems cannot be trusted as fully automatic defence mechanisms as they are known to report false positives (falsely reporting normal activity as malicious) and false negatives (missing malicious activity and not reporting them). They must be monitored by operators who can interpret the reports and analyze the data to confirm the classifications of the activities.

13. Once a detection of malicious activity is discovered, a response would be required to deal with the attack. The attack would have to be contained or isolated while maintaining the ship's capabilities in-line with the command priority of the ship. The appropriate response would require the knowledge of which systems in the network are impacted, how those systems affect the ship's capabilities, and how to best isolate the malicious activities to limit the impact to the ship. This activity would require command decision in order to ensure that the ship retains its combat capability to the best of the ship's company's ability during a cyber attack.

14. Upon completion of the mission, or after securing action stations following an encounter, the ship's cyber defence operators would conduct the recover activities. This would entail determining the extent of the penetration of the cyber attack, any residual malware left behind, and returning the systems to full operational capability. It may require complete rebuilds of the affected systems or limited sanitization of the systems

[16] Edward Skoudis and Tom Liston, *Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses*, 2nd ed. (Prentice Hall, 2006), 320.

depending on what systems were attacked and whether they affect the ship's ability to float, move, and/or fight as well as how deeply they were infected or penetrated.

15. The RCN ERT Manual describes the doctrine for the ERT, its organization and its roles and responsibilities. The ERT exists to support the Damage Control (DC) efforts, to provide command with assessments on combat capabilities following damage to equipment, and to conduct battle damage repairs to maintain combat capabilities. These activities deal with physical damage to the combat systems of the ship as well as any structural damages or hazards (fires and floods) which impact the ship's ability to conduct the external battle.[17]

16. A cyber defence capability would mirror the ERT's activities for assessing the impact to the ship's combat capabilities. Cyber defence operators would monitor the ship's various networks, determine if they've been compromised, advise command on the impact of isolating the attack (essentially detailing to command of which war fighting capability would be lost during the isolation of infected systems), and restore services as quickly as possible. They would also advise the Executive Officer (XO) and the Engineering Officer (EO) of any impact to the ship's internal battle capabilities, such as a loss of the ability to use fitted fire systems remotely from IPMS, or to control the ship's stability. These same operators would also provide general health monitoring of the systems to ensure that they are operating at their peak efficiency.

17. A cyber defence team would have to be comprised of technical sailors who understand computer networking, software, hardware and also understand the systems that these networks are supporting, such as the radars, propulsion systems, weapons, etc.

[17] Department of National Defence, "B-GN-007-RCN/FP-002, CFCD 133 Royal Canadian Navy Emergency Response Team Manual" (Canada, July 1, 2015).

Because of the advanced knowledge, education and training required to be proficient in naval cyber defence, personnel would likely have to be hand picked from the current Weapons Engineering Technician (WENG Tech) and Naval Combat Systems Engineering Officer (NCS ENG) occupations, with some cyber defence operators also coming from the Maritime Surface Officer (MARS), Naval Communicators (NAV COM), Marine Systems Engineering Officer (MS ENG), Marine Electrician (MAR ELEC) and Marine Engineer (MAR ENG) occupations who demonstrate the requisite skill sets. The cyber operators could be placed within the Combat Systems Engineering Department and form part of the ERT.

CONCLUSION

18. This paper outlined the requirement for the RCN to build a cyber defence capability that can be deployed onboard ship and form part of the ship's company. The modernized fleet has become completely dependant on information technology to float, move and fight. The systems that support these three naval concepts on the RCN's warships are vulnerable to well-planned cyber attacks. A cyber defence capability must therefore provide real-time support to the ship's commander for the detection of cyber attacks, responding to the attacks and restoring the combat capability of the ship.

19. The US Navy has recognized this requirement and is investing heavily in cyber warriors. Such a capability in the RCN would assist the existing ERT in maintaining a ship's combat capability throughout an engagement and should be created from hand-picked individuals within the technical and operator communities of the navy.

RECOMMENDATION

20. It is recommended that the RCN conduct a study to determine which occupations could feed into a naval cyber defence operator. Included in this study should be the

identification of which tasks are no longer required to be performed by sailors due to the automation provided by the latest technology found in today's warships. This would alleviate the physical limitations of space and bunking on the ship. The study should also include training and education requirements, possibly leveraging existing training through the Canadian Forces Network Operations Centre.

BIBLIOGRAPHY

Brown, Nancy, Danelle Barrett, and Jesse Castillo. “CREATING Cyber Warriors.” *U.S. Naval Institute Proceedings* 138, no. 10 (October 2012): 28–32.

Canada. Communications Security Establishment, Web Experience. “IT Security Risk Management: A Lifecycle Approach,” November 1, 2012. https://www.cse-cst.gc.ca/en/publication/itsg-33.

Canada. Department of National Defence. “B-GN-007-RCN/FP-002, CFCD 133 Royal Canadian Navy Emergency Response Team Manual.” July 1, 2015.

Canada. Department of National Defence. “Securing Canada’s Ocean Frontiers: Charting the Course from Leadmark.” Ottawa: 2005.

Center, Mandiant Intelligence. “APT1: Exposing One of China’s Cyber Espionage Units.” Mandiant, 2013.

Clarke, Richard. “China’s Cyberassault on America.” *Wall Street Journal*, June 15, 2011, sec. Opinion. http://www.wsj.com/articles/SB10001424052702304259304576373391101828876.

Gorman, Siobhan. “Electricity Grid in U.S. Penetrated By Spies.” *Wall Street Journal,* April 9, 2009, sec. Tech. http://www.wsj.com/articles/SB123914805204099085.

Lynn, William J., III. “Cybersecurity - Defending a New Domain.” *Cyber Security*. Accessed February 1, 2016. http://archive.defense.gov/home/features/2010/0410_cybersec/lynn-article1.aspx.

Nakashima, Ellen. “Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyberspies - The Washington Post.” Accessed November 9, 2015. https://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html.

Skoudis, Edward, and Tom Liston. *Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses*. 2nd ed. Prentice Hall, 2006.

Sood, Aditya K., and Richard Enbody. “U.S. Military Defense Systems: The Anatomy of Cyber Espionage by Chinese Hackers | Georgetown Journal of International Affairs.” Accessed November 10, 2015. http://journal.georgetown.edu/u-s-military-defense-systems-the-anatomy-of-cyber-espionage-by-chinese-hackers/.

United States. National Institute of Standards and Technology. “Framework for Improving Critical Infrastructure Cybersecurity.” February 2014.

http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

United States. National Institute of Standards and Technology, and Department of Commerce. "NIST Special Publication 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems." September 1996.

Wang, Jian-Wei, and Li-Li Rong. "Cascade-Based Attack Vulnerability on the US Power Grid." *Safety Science* 47, no. 10 (December 2009): 1332–36. doi:10.1016/j.ssci.2009.02.002.

Windrem, Robert. "Exclusive: Secret NSA Map Shows China Cyber Attacks on U.S. Targets." *NBC News*, July 30, 2015. http://www.nbcnews.com/news/us-news/exclusive-secret-nsa-map-shows-china-cyber-attacks-us-targets-n401211.

Zetter, Kim. "An Unprecedented Look at Stuxnet, the World's First Digital Weapon | WIRED." Accessed November 6, 2015. http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.