National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

BUY CYBER-SECURE: IMPROVING CYBERSECURITY OF PROCURED COMBAT SYSTEMS

LCdr J.T.D.S. Turner

JCSP 42

Master of Defence Studies

PCEMI 42

Maîtrise en études de la défense

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

MASTER OF DEFENCE STUDIES – MAÎTRISE EN ÉTUDES DE LA DÉFENSE

BUY CYBER-SECURE: IMPROVING CYBERSECURITY OF PROCURED COMBAT SYSTEMS

LCdr J.T.D.S. Turner

Word Count: 17 153

Compte de mots: 17 153

TABLE OF CONTENTS

Table of Contents		i
Abstract		ii
Chapter		
1.	Introduction	1
2.	Literature Review	16
3.	Halifax Class Modernization: A Case Study	41
4.	General Analysis	62
5.	Recommendations and Conclusions	69
Bibliography		74

ABSTRACT

The pervasiveness of cyber-attacks continues to grow as does the complexity of the systems necessary for the Canadian Armed Forces to keep its technological fighting edge over its adversaries. These systems, heavily software-centric and increasingly built of commercial-off-the-shelf technology, inherit the vulnerabilities of their commercial counterparts/components and therefore are subject to an increasing threat of exploitation. The Department of National Defence and the Canadian Armed Forces must take action to ensure their mission critical combat and platform systems are defensible in the cyber domain. This research reviewed key literature discussing: security requirements engineering, risk management frameworks, certification programmes and system security engineering; with the aim of determining how to improve the cybersecurity of procured systems. The Halifax Class Modernization/Frigate Life Extension project was studied, relative to the aforementioned methods, as a recent and relevant case where a complex procurement attempted to address cybersecurity in modern combat systems. Additionally, this research analysed these methods in a general context, considering their applicability to procurement in the Department of National Defence. The case study and analysis yielded several findings and recommendations. The key finding was that a combination of the reviewed methods would be required in order to improve cyber-security of acquired combat and platform systems. This combined approach must be supported by a cyber-educated workforce and a holistic cybersecurity programme that integrates sound requirements engineering, system security engineering, internally and in industry, and risk management.

CHAPTER 1 – INTRODUCTION

The world is constantly changing and evolving which implies that the threat landscape is following suit. This combined with the increasingly rapid advance of technology means the Department of Defence (DND) and the Canadian Armed Forces (CAF) must attempt to keep pace. The adoption of new technology implies that the CAF benefits from being able to operate in more effective and efficient ways but its adversaries can also leverage innovative methods to attack and exploit new vulnerabilities. This is certainly the case with respect to cyberspace. As more advanced technology is used, the available attack surface is increased to potential symmetric and asymmetric threat actors. In order to improve cyber-security of acquired systems, DND and the CAF must educate its workforce, including key decision-makers, and develop a holistic cybersecurity programme that integrates sound requirements engineering, system security engineering, internally and in industry, and risk management. The CAF's effort to economically keep pace with technological advancement and keep the technological fighting edge have resulted in systems based on Commercial-Off-the-Shelf (COTS) hardware and software and along with that comes the new vulnerabilities and increased attack surfaces. Additionally, the drive to interconnect every system and to have access to vast amounts of data in order to make better and faster decisions also increases the CAF's exposure to threats. Employing advanced technology has become a double edged sword requiring the CAF to focus on ensuring the systems it uses are both effective and defensible in cyberspace.

The Ubiquity of Software

Every piece of modern technology contains software; cars, mobile phones, airplanes, televisions and even refrigerators are now becoming *smart* and as a result execute software to function. This fact extends to modern weapons, combat and platform systems employed by the

CAF.[1] In some cases, the military could be considered a very early adopter of computerized and software centric systems as it was one of the only organizations that could afford to acquire what was considered cutting edge technology. This can be seen as technology is inserted into systems that traditionally were purely organic, like the soldier, which is now planned to be augmented via the Integrated Soldier System Project (ISSP).[2] Additionally, systems that were purely mechanical and ballistic are experiencing technological insertion like the Defense Advanced Research Projects Agency's (DARPA) Extreme Accuracy Tasked Ordinance (EXACTO) project.[3]

The key challenge with a software centric system is the vulnerability of software itself. In 2005, the US President's Information Technology Advisory Committee stated "Software development is not yet a science or a rigorous discipline, and the development process by and large is not controlled to minimize the vulnerabilities that attackers exploit."[4] This fact persists today with little improvement from the broad software development industry noted in the SANS Institute's *2015 State of Application Security: Closing the Gap* which indicated that software developers and cyber-defenders are improving the coherence of their efforts but they still face significant challenges and are not completely synchronized.[5] Unfortunately, "information security engineers [do not] understand software development – and most software developers [do

---

[1] Roger Cyr, "Danger — Software Ahead!" *Maritime Engineering Journal* 3 (October, 1991), 23.; Doug Brown, "More Effective Software Management," *Maritime Engineering Journal* 3 (October, 1994), 11.

[2] "Integrated Soldier System Project (ISSP)," Department of National Defence, last modified December 3, 2013, http://www.forces.gc.ca/en/business-equipment/integrated-soldier-system-project.page. The website described the project as "a suite of military equipment that soldiers wear as part of their combat load. It includes weapon accessories and electronics that allow soldiers to stay connected with their teams after exiting vehicles on the battlefield. It also features a radio, a smartphone-like computer to run battle management software, a GPS, and a communications headset."

[3] "EXACTO Guided Bullet Demonstrates Repeatable Performance Against Moving Targets," Defense Advance Research Projects Agency, last modified April 27, 2015, http://www.darpa.mil/news-events/2015-04-27. The EXACTO project has demonstrated a .50 caliber bullet that is precision guided.

[4] President's Information Technology Advisory Committee, *Cyber Security: A Crisis of Prioritization* (Arlington, VA: National Coordination Office for Information Technology Research and Development, 2005), 3, accessed May 8, 2016, https://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.

[5] Jim Bird, Eric Johnson and Frank Kim, *2015 State of Application Security: Closing the Gap* (Bethesda, MD: SANS Institute,[2015])., 5-6, accessed May 8, 2016, https://www.sans.org/reading-room/whitepapers/analyst/2015-state-application-security-closing-gap-35942.

not] understand security."[6] These two groups have different motives and the organizations do not have a coherent approach to software (also called application) security.[7] In the book *Software Security Engineering*, Allen et al. note that "[s]oftware security matters because so many critical functions are completely dependent on software."[8] As a result of these facts, as the CAF embraces the available advanced technology in its pursuit of improving and modernizing its capabilities, without proper management and engineering, it is exposed to ever increasing risks with respect to software and software-centric systems.

The Growing Prevalence of Commercial-Off-the-Shelf

Militaries constantly strive to acquire better technology and to employ more efficient methods to procure those technologies. In the global arms race, modern military platforms and systems continuously increase in complexity and cost, and the price of maintaining the competitive technological edge over potential adversaries substantially increases as a result. As defence budgets in Canada are fully in the discretionary realm, increased scrutiny over how each dollar is spent drives a search for economies in acquisition of what are already considered expensive systems. Over the past several decades these stresses have inspired a number of changes in how the military procures advanced military systems. One of those key changes was the focus on procuring COTS based systems as opposed to Military Specification (MIL-SPEC) based systems[9]. This change is readily apparent when comparing the original build of the Halifax Class Frigates with the most recent mid-life refit and modernization project.[10]

---

[6] Ibid., 5.

[7] Ibid., 5-6.

[8] Julia Allen et al., *Software Security Engineering: A Guide for Project Managers* (Stoughton, MA: Pearson Education, Inc., 2008), 7.

[9] These systems were also based on Military Standards (MIL-STD) and a varied of other defence standards produced by the United States Department of Defense.

[10] As an example the original Canadian Patrol Frigate's Command and Control System (CCS) was made up of a distributed-federated network of Sperry UNIVAC AN/UYK-505 and AN/UYK-507 computers. Those computers were completely MIL-SPEC and not commercially available and the associated software was custom developed (in

The *Statement on Canadian Defence Policy* in 1992 specified that defence procurement should "avoid unique Canadian solutions that require expensive and risky research, development or modification of existing equipment."[11] This was followed up in the *1994 National Defence: Budget Impact* where it was stated that "in its acquisition strategy, the Department…will emphasize the purchase of equipment 'off the shelf', the use of commercial standard technologies, and unless absolutely necessary, the avoidance of military modifications."[12] Finally, the 1994 Defence White Paper stated,

> [t]he Department will increase the procurement of off-the-shelf commercial technology which meets essential military specifications and standards. Full military specifications or uniquely Canadian modifications will be adopted only where these are shown to be absolutely essential.[13]

In the same year, the United States (US) Department of Defense (DoD) was applying a similar approach which was outlined in a memorandum from Secretary of Defense William Perry. He went so far as to state that the use of military specifications and standards would be "…authorized as a last resort…." This memorandum initiated a new approach for US DoD acquisition and although Canada was already heading this direction, many of the US based vendors of military systems would soon only be delivering heavily COTS based products.

The primary drivers for this shift in approach were budget pressures and the high cost of military specific components. Beyond being expensive, it was well understood that MIL-SPEC

---

the CMS-2 programming language), from the Operating System (OS) called Standard Distributed Executive (SDX) to its application modules. There was a common software base share with the US military but again it was not available outside of controlled channels. MEJ 1990, Vol 1, 26. The modernized frigate's Combat Management System (CMS) is based on ruggedized server hardware that could be purchased globally and a standard version of the Red Hat Linux OS.

[11] Department of National Defence, *Candian Defence Policy* (Ottawa, ON: Canada Communications Group, 1992), 13.

[12] David Collenette, *National Defence: Budget Impact* (Ottawa, ON: Canada Communications Group, 1994), 14.

[13] Department of National Defence, *1994 Defence White Paper* (Ottawa, ON: Canada Communications Group, 1994), 41.

electronics were not able to keep pace, with respect to performance and functionality, with their commercial equivalents.[14] Development cycles for MIL-SPEC electronics were between five and seven years, whereas for development timelines for commercial products were less than a year and decreasing.[15] When considering this difference in development rate in the context of Moore's law, MIL-SPEC components were being outpaced in an exponential fashion.[16] Ultimately the broad use of MIL-SPEC components was "imped[ing] the rapid development and enhancement of military systems."[17] This issue was clearly recognized by some organizations, notably the US Air Force (USAF) and it needed "to achieve effects on the battlefield with technology today rather than yesterday's technology tomorrow."[18] The chosen solution was an increased use of COTS in military systems.

The Growing Threat in Cyberspace

Although, increased reliance on COTS technology provided distinct advantages in a number of areas, it had some undesired effects, namely exposure to a more broad set of cyber threats. The COTS software and hardware components used in modern systems would be present in a wide variety of industrial, commercial or personal use systems and products. This fact changes the landscape for a would-be attacker in that most of these COTS components would be

---

[14] John McHale, "Military Market One of Opportunity for Embedded COTS Suppliers," *Military Embedded Systems*, sec. Q&A, September 12, 2014, accessed May 8, 2016, http://mil-embedded.com/articles/military-one-opportunity-embedded-cots-suppliers/.; John Keller, "The Revenge of COTS: An Ageing Commercial Technology Base Complicates Military Supply Chain," *Military and Aerospace (Blog)* (November 19, 2013), accessed May 8, 2016, http://www.militaryaerospace.com/blogs/mil-aero-blog/2013/11/the-revenge-of-cots-an-ageing-commercial-technology-base-complicates-military-supply-chain.html.

[15] Thomas Kelly J., "The Shift to Standards-Based Hardware for Military Communications: What Role Will COTS Systems Play?" *Military Embedded Systems*, December 9, 2014, accessed May 8, 2016, http://mil-embedded.com/articles/the-cots-systems-play/.

[16] Carlo Kopp, "COTS – Revolution, Evolution Or Devolution?" *Defense Today*, June 2011, 30.

[17] *Cisco Systems, White Paper: Defense Agencies Meet Readiness Challenges with Commercial Off the Shelf (COTS)-Based Systems (San Jose, CA: Cisco Systems, Inc.,[2005])*, accessed May 8, 2016, http://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/space_COTS_v2.pdf.

[18] Headquarters United States Air Force, Future Concepts and Transformation Division, *The U.S. Air Force Transformation Flight Plan 2004* (Washington DC: Department of Defense, 2004), 23, accessed May 8, 2016, http://www.au.af.mil/au/awc/awcgate/af/af_trans_flightplan_nov03.pdf.

accessible for testing, experimentation or examination, allowing potential attackers to design and develop effective cyber-attacks. For example, the number of detected security incidents increased by 38% in 2015 in all industries, while they grew by 137% in public sector organizations.[19]

There are many forms of cyber-attack that rely on the exploitation of software (or firmware) flaws and vulnerabilities. These vulnerabilities can be attacked over the network or Internet but are also exploited by malicious software (malware). Some malware is analogous to fire-and-forget weapon systems and they autonomously navigate computer networks and systems leveraging vulnerabilities to self-propagate, escalate privilege and deliver specific payloads. The possible payload of the malware may vary depending on the desired effect of the attack but could range from providing persistent access to the system or network (e.g. Backdoors or Remote Administration Tool/Trojan (RAT)) to overloading the system (i.e. Denial of Service) to altering the operation of a machine controlled by a computer. In any of these cases, malware presents a clear danger and real risk to military operations by affecting combat systems and platforms.

Stuxnet – A game-changer

In 2010 the world was introduced to *Stuxnet*; a computer virus that was suspected of specifically targeting Iran's uranium refining operations.[20] This malware was a game-changer with respect to cyber-attacks and highlighted new technological developments that were of significance to military combat and platform systems as well as industries throughout the world. These important revelations were that:

---

[19] Pricewaterhouse Cooper, *Turnaround and Transformation in Cybersecurity: Key Findings from the Global State of Information Security® Survey 2016* (London, UK: Pricewaterhouse Cooper, [2015]), 2, accessed May 8, 2016, http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html.

[20] Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the most Menacing Malware in History." *Wired*, sec. Security, July 11, 2011, accessed November 14, 2015, http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.; Nicolas Falliere, Liam O. Murchu and Eric Chien, "W32. Stuxnet Dossier," *White Paper, Symantec Corp., Security Response* (2011), 4, accessed May 8, 2016, https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

- air-gapped systems, those not connected to the Internet, were not secure by default;
- malware could have physical effects; and
- nation states were willing to use cyberspace to attack others.

Beyond these new tenets, *Stuxnet* set a new standard in the complexity of malware that could be effectively employed.[21]

The *Stuxnet* virus likely found its way into an Iranian uranium enrichment facility on a Universal Serial Bus (USB) flash memory drive.[22] From this USB drive it may have first infected computers on a non-Internet connected network. The malware was designed to seek out two specific types of computers: one with an internet connection and containing very specific software called *Step 7*.[23] *Stuxnet* could spread both via USB device and by network using a number of zero-day exploits to infect all the computers on a given network. Once a computer was infected it would spread the virus to any USB memory devices that were connected to it in the future as well as any computer on the same network. The infection of other, previously clean USB drives would allow *Stuxnet* to spread to other networks in the facility including one that was connected to the Internet.[24]

---

[21] Two other key elements were that Stuxnet used two different stolen digitally signed drivers as well as four zero-day exploits. Digital Signatures are used to provide a user assurance that the software they are installing is actually from the manufacturer and has not been altered. This allows the user to "trust" the software in the same sense they would "trust" the manufacturer. The illegal use of a company's digital signatures represents a significant breach of trust and compromise of security. Further details and explanation provided in Randy Abrams, "Why Steal Digital Certificates?", *welivesecurity* (blog), July 22, 2010, accessed November, 14 2015, http://www.welivesecurity.com/2010/07/22/why-steal-digital-certificates/. Zero-day vulnerabilities are flaws in software that are still unknown to the developer and the general public. Software or code that leverages that vulnerability is known as a zero-day exploit. Since the vulnerability is still unknown to the software developer, they cannot attempt to repair it and since the exploit is still unknown to the general public, anti-virus companies cannot detect it (in the form of a virus, using traditional signature based detection techniques). This makes zero-day vulnerabilities and exploits extremely dangerous as well as being sought after by hackers with nefarious intentions. More details and explanation are provided in Kim Zetter, "Hacker Lexicon: What is a Zero Day?" *Wired*, sec. Security, November 11, 2014b, accessed November 14, 2015, http://www.wired.com/2014/11/what-is-a-zero-day/.

[22] Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York, NY: Crown Publishers, 2014a), 322-323.

[23] *Step 7* is software associated with Siemens Industrial Control Systems. Also involved was Siemen's software called WinCC. Falliere, Murchu and Chien, *W32. Stuxnet Dossier*, 3.

[24] Ibid., 25-32.

Once it found a computer connected to the Internet, *Stuxnet*, could communicate via a covert channel to send data and receive software updates.[25] It relied on USB drives to move across air-gaps but users, programmers or contractors likely facilitated this by moving files from one network to another using infected drives. The other target computer was one that was loaded with the *Step 7* software. This software was used to program and update Siemens programmable logic controllers (PLC), which were used by the Iranians to control their uranium enrichment centrifuges. Once the virus located this computer it would then load malware specifically designed for the centrifuge PLCs. Since the database of programs for the PLCs contained a variety of past and new versions the virus actually replaced them all with the malware.[26] This ensured that the next time a field programming laptop was loaded with new firmware for the PLCs it would be a malicious version. It was then, via this technician field programming laptop, that the virus would jump another air-gap and reach its final target.[27] Although there are many further insidious or ingenious details about this ground-breaking piece of malware it would then go on to destroy centrifuges and set the Iranian uranium enrichment programme back 18 months.[28] Given the complexity of the virus itself, the resources required to properly develop the malware, the resources required to get the initial infection started, the specificity of the targeting

[25] The covert channel was a Hyper-Text Transportation Protocol tunnel where the Stuxnet application would send web-requests with encoded or encrypted data to a specific set of web servers hosting fake websites. If visited the websites looked real to a human but if a properly encoded web-request was sent to them it would reply with commands or updated versions of the virus. If observed this network traffic would have initially looked like regular web-surfing. To strengthen the cover of these websites, they were setup to provide actual football scores which fit with the likely interests of the employees of the facility (i.e. It would not be considered unusual for employees to surf to websites providing football scores). Ibid., 21-22.

[26] Ibid., 33-35.

[27] Ibid., 36-49.

[28] David Albright, Paul Brannan and Christina Walrond, *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?* (Washington, DC: Institute for Science and International Security, 2010), 1, accessed May 8, 2016, http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/.

and the effect the virus had, it was evident this attack was state-sponsored and by a state highly skilled in the cyber domain.[29]

The Next Five Years

State-Sponsored Attacks. The five years that followed the discovery of *Stuxnet* continued to show advances in what could be considered cyber weapons that were used to attack a variety of industries and governments alike. A family of viruses were soon discovered and suspected to be relatives of *Stuxnet*. *Duqu*, *Gauss*, *Flame* and *mini-Flame* were the names of malware all built on the same framework as *Stuxnet*, although none of these viruses caused physical damage, all of them performed some form of reconnaissance or espionage.[30] One of the more complex of these family members was *Flame*, discovered in 2012. It was another complex and rich example of malware that had many modular functions from recording conversation via the computers microphone to acting as a Bluetooth hub to steal contact information from vulnerable mobile devices that passed within range.[31] This virus was found attacking Iranian oil industry computers and was investigated at the request of the United Nations (UN) International Telecommunication Union (ITU). This family of viruses were linked in the media to an US/Israeli operation called *Olympic Games*.[32] A key common thread was that all of these viruses spread via USB memory drive.

---

[29] David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *The New York Times*, sec. Middle East, June 1, 2012, accessed November 14, 2015, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

[30] Global Research and Analysis Team, "Full Analysis of Flame's Command & Control Servers," *SecureList* (Blog) (September 17, 2012) , accessed November 14, 2015, https://securelist.com/blog/incidents/34216/full-analysis-of-flames-command-control-servers-27/.

[31] A more complex piece of malware was being tracked an analysed, it was linked and reported on in 2014 based on documents leaked by Edward Snowden. A virus named *Reign* was used to infiltrate Middle-Eastern and European cellular telephone providers as well as the European Commission and a prominent Belgian Cryptographer. Kim Zetter, "Meet 'Flame,' the Massive Spy Malware Infiltrating Iranian Computers," *Wired*, sec. Security, May 28, 2012, accessed November 14, 2015, http://www.wired.com/2012/05/flame/.; Kim Zetter, "Researchers Uncover Government Spy Tool used to Hack Telecoms and Belgian Cryptographer," *Wired*, sec. Security, November 24, 2014c, accessed May 8, 2016, https://www.wired.com/2014/11/mysteries-of-the-malware-regin/.

[32] Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*

Firmware Viruses. In the year following the aforementioned viruses coming into public view, researchers introduced the concept of *BadUSB*.[33] This proof of concept demonstrated that the firmware of the USB drive's memory controller could be reprogrammed outside of the manufacturer's facilities. This concept was notable as malware was hidden in the USB devices firmware memory, which meant there was no practical method to detect the malware and it could hide some of the devices flash memory from the user (and computer) allowing it to hide data or larger malware. It was now theoretically possible to have an undetectable virus on a USB device that could hide another virus to reprogram USB devices (i.e. create more *BadUSB* devices) allowing it to propagate in a highly stealth manner. In 2014 and 2015 researchers demonstrated the *Thunderstrike* and *Thunderstrike 2* attacks on Apple computers, which were viruses that affected a computer's Unified Extensible Firmware Interface (UEFI) which is the modern form of the Basic Input Output System (BIOS).[34] The *Thunderstrike* demonstration proved that malware, specifically a root-kit also known as a boot-kit in this case, could be persistently installed and was undetectable (since it resides in the computers firmware) through the simple connection of a Thunderbolt (a computer peripheral interface standard) based device.[35] *Thunderstrike 2* demonstrated that this could be achieved remotely without the connection of the

[33] Karsten Nohl and Jakob Lell, "BadUSB — on Accessories that Turn Evil" (Presentation, Black Hat 2014, Las Vegas, NV, August 7, 2014) , accessed May 8, 2016, https://srlabs.de/blog/wp-content/uploads/2014/07/SRLabs-BadUSB-BlackHat-v1.pdf.; Karsten Nohl, Sascha Krißler and Jakob Lell, "BadUSB — on Accessories that Turn Evil" (Presentation, PacSec 2014, Tokyo, JP, November 12, 2014) , accessed May 8, 2016, https://srlabs.de/blog/wp-content/uploads/2014/11/SRLabs-BadUSB-Pacsec-v2.pdf.

[34] This concept was previously reported by security consultant Dragos Ruiu calling it BadBIOS in 2013. At the time of his report there was no he could not reproduce or find non-circumstantial evidence of the infection. At this time, it was considered a myth but potentially feasible attack. Thunderstrike and Thunderstrike 2 somewhat redeemed Dragos by demonstrating similar types of attacks as he describe in his reports of BadBIOS. It should also be noted that laboratory work had been done on BIOS attacks but none that demonstrated viable malware. Dan Goodin, "Meet 'badBIOS,' the Mysterious Mac and PC Malware that Jumps Airgaps," *Ars Technica* (October 31, 2013), accessed May 8, 2016, http://arstechnica.com/security/2013/10/meet-badbios-the-mysterious-mac-and-pc-malware-that-jumps-airgaps/.

[35] Trammel Hudson, "Thunderstrike: EFI Bootkits for Apple MacBooks" (Presentation, Schedule 31 Chaos Communications Congress, Hamburg, DE, December 29, 2014), accessed May 8, 2016, https://trmm.net/Thunderstrike_31c3.

device. Since these attacks take control of the system from the first instruction executed by the CPU, their power is almost limitless.[36] Additionally, given their location in the computer system and privileged nature the malware cannot be practically removed.

In 2015 revelations about attacks against hard drive controller firmware by the US National Security Agency (NSA) were released.[37] Again, this malware was able to hide in the firmware memory of the hard drive controller and survive computer hard disk formatting, OS reinstalled and anti-virus software actions. Once the computer was restored or repaired the malware was able to re-install itself from its hidden location and continue to operate or potentially downloading a new version of malware from the Internet. All of these attacks highlight that attack designers are finding new areas to hide malware from existing protections and maximizing persistence and stealth.

Embedded System Attacks. An embedded is defined as "a microprocessor-based system that is built to control a function or range of functions and is not designed to be programmed by the end user…."[38] The key of the definition is that these systems are not a general purpose computer, like a personal computer (PC), and are designed to perform very specific functions in specific environments. The end target for *Stuxnet* was an *embedded system* and much of our current world relies on these systems to function.[39] In 2014, Germany's Federal Office for

[36] Trammell Hudson, Corey Kallenberg and Xeno Kovah, "Thunderstrike 2: Sith Strike A MacBook Firmware Worm" (Presentation, Black Hat 2015, Las Vegas, NV, August 6, 2015), accessed May 8, 2016, http://legbacore.com/Research_files/ts2-blackhat.pdf.; It should also be noted that prior to conducting the Thunderstrike 2 research, Kallenberg and Kovah also developed a proof-of-concept attack called Lighteater, this method was foundational to Thunderstrike 2. Corey Kallenberg and Xeno Kovah, "How Many Million BIOSes would You Like to Infect?" (Presentation, CanSecWest 2015, Vancouver, BC, March 20, 2015), accessed May 8, 2016, http://www.legbacore.com/Research_files/HowManyMillionBIOSWouldYouLikeToInfect_Full2.pdf.

[37] Kim Zetter, "How the NSA's Firmware Hacking Works and Why It's so Unsettling," *Wired*, sec. Security, February 22, 2015, accessed May 8, 2016, https://www.wired.com/2015/02/nsa-firmware-hacking/.

[38] Steve Heath, *Embedded Systems Design*, 2nd ed. (Burlington, MA: Newnes, 2003), 2.

[39] *Embedded Systems* control everything from power plants and factories to modern automobiles. They could be as simple as the electronics that play a song in a greeting card or as complex as those that control the propulsion system on a warship.

Information Security disclosed a steel mill had suffered a cyber-attack.[40] This attack mirrored the *Stuxnet* attack by moving from an initial infection of an administrative network to the production network /industrial control system (ICS). This attack resulted in cascading failures in control system components and significant damage when the mill's blast furnaces could not be shut down in a controlled manner.

Another *embedded system* attack was demonstrated by security researchers in 2015 where the target was a 2014 Jeep Cherokee.[41] There had been previous work on hacking automobile systems dating back to 2010 but this demonstration had real effects and used a wireless and remote link to conduct the attack.[42] The researchers performed a live demo with *Wired* journalist Andy Greenberg behind the wheel showing that they could remotely control the entertainment system, climate control, engine control, brake system and in specific circumstances steering. Additionally, the researchers demonstrated that they could track vehicles, via onboard GPS, while gathering their vehicle identification number, make and model. The results of their previous work, this demonstration and presentation at *Black Hat 2015* were an introduction of automobile cyber-security bill in the US Senate and a recall of over one million Chrysler

---

[40] Federal Office for Information Security, *The State of IT Security in Germany 2014* (Bonn, DE: Federal Office for Information Security, 2014), 31, accessed May 8, 2016, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014.pdf.

[41] Charlie Miller and Chris Valasek, "Remote Exploitation of an Unaltered Passenger Vehicle" (Presentation, Black Hat 2015, Las Vegas, NV, August 5, 2015), accessed May 8, 2016, http://illmatics.com/Remote%20Car%20Hacking.pdf.

[42] In 2010, researchers examined the feasibility of attacking modern automobile through the Tire Pressure Monitoring System (TPMS). The tire pressure sensors in this system use an unsecure wireless radio communication link to communicate with the Engine Management System. In 2011, researchers examined a variety of attack surfaces in modern vehicles including the On Board Diagnostics (OBD) port, the CD player, Bluetooth, FM Radio Data Service and Cellular. Finally, in 2013 researchers performed a live demonstration of an attack via the OBD II port. Ishtiaq Rouf et al., "Security and Privacy Vulnerabilities of in-Car Wireless Networks: A Tire Pressure Monitoring System Case Study" (Washington, DC, USENIX Association, August 11-13, 2010) , accessed May 8, 2016, http://www.usenix.org/events/sec10/tech/full_papers/Rouf.pdf.; Stephen Checkoway et al., "Comprehensive Experimental Analyses of Automotive Attack Surfaces" (San Francisco, CA, USENIX Association, August 8-12, 2011), accessed May 8, 2016, http://www.autosec.org/pubs/cars-usenixsec2011.pdf.; Andy Greenberg, "Hackers Reveal Nasty New Car Attacks--with Me Behind the Wheel," *Forbes*, August 12, 2013, accessed May 8, 2016, www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/.

automobiles.[43] These attacks and demonstrations proved soundly that cyberspace can be used to have potentially lethal effects and *embedded systems* are not immune but are the high payoff targets in this respect.

Applicability to the Canadian Armed Forces

For sound reasons combat and platform systems are procured and they are composed of predominantly COTS software and hardware components but as the threat landscape has changed the CAF's procurement practices must adapt. It is challenging to deduce how vulnerable legacy MIL-SPEC based systems were but given the demonstrated cyber-attacks, whether research proofs-of-concept or real incidents, it is clear modern systems are at risk. Both industry and the CAF must take action to manage cyber risks in modern combat and platform systems. Without appropriate action, CAF combat and platform systems may be left indefensible and/or wide open to cyber-attack leaving military cyber-defenders at a distinct disadvantage. Although there are many approaches to managing this risk, a long purported approach is to build security into the system. Security is much like a system *'ilities* and systems engineering practice and theory state that these are best addressed in the design and implementation of the system as opposed to attempting to add them in after delivery.[44] The International Council On Systems Engineering defines the *'ilities* as "[t]he developmental, operational, and support requirements a program must address (e.g., availability, maintainability, vulnerability, reliability, supportability,

[43] Andy Greenberg, "Senate Bill Seeks Standards for Cars' Defenses from Hackers," *Wired*, sec. Security, July 21, 2015, accessed May 8, 2016, https://www.wired.com/2015/07/senate-bill-seeks-standards-cars-defenses-hackers/.; Aaron M. Kessler, "Fiat Chrysler Issues Recall Over Hacking," *The New York Times*, sec. Business Day, July 24, 2015, accessed May 8, 2016, http://www.nytimes.com/2015/07/25/business/fiat-chrysler-recalls-1-4-million-vehicles-to-fix-hacking-issue.html?_r=0.

[44] Security is included ISO-IEC 25010: 2011's product quality model (section 4.4). International Standards Organization, *ISO-IEC 25010: 2011 Systems and Software Engineering - Systems and Software Quality Requirements and Evaluation (SQuaRE) - System and Software Quality Models* (Geneva, CH: ISO, 2011), 34.

etc.)."[45] The systems engineering approach (i.e. considering the 'ilities in the design of a system) has been shown to have a positive return on investment.[46] It is unreasonable to expect system security to be any different.

The CAF is in the process of recapitalizing its naval fleet as well as planning for the procurement of a new fighter aircraft and the Joint Unmanned Surveillance and Targeting Acquisition System (JUSTAS).[47] These new ships, aircraft and other systems will be more interconnected via computer networks and be made up of more COTS hardware and software than ever before. Given the complexity of these *systems of systems*, retrofitting them to add security after they are delivered would very likely be unaffordable and infeasible for DND to manage. Additionally, attempting to manage or control the residual risks associated with security given the growing cyber threat may be a significant undertaking. Defending these systems in this case would also prove to be extremely challenging for the CAF cyber-defenders as it is still early in the development of that capability, which has been solely focused around traditional computer systems and networks.[48]

Based on these looming challenges, DND and the CAF must adapt their approach to acquiring systems such that cyber-security is a key consideration and it is designed into systems, validated and verified throughout the development, implementation and on final delivery. In order to improve cyber-security of acquired systems, DND and the CAF must educate its

---

[45] International Council On Systems Engineering, *INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*, ed. David D. Walden and others , 4th ed. (Hoboken, NJ: John Wiley and Sons, Inc., 2015), 261.

[46] Eric C. Honour, "Systems engineering return on investment" (PhD thesis, University of South Australia, 2013), 178, accessed May 8, 2016, http://www.hcode.com/seroi/documents/SE-ROI%20Thesis-distrib.pdf.

[47] "2015 Defence Acquisition Guide," Department of National Defence, last modified June 25, 2014, http://www.forces.gc.ca/en/business-defence-acquisition-guide-2015/index.page.

[48] Ibid. The Joint section of this guide lists a number of cyber related projects as well as their estimated timelines. A few examples are: the Computer Network Defence (CND) project enabling Defensive Cyber Operations (DCO) will be in Options Analysis (OA) in 2016 with an estimated Contract Award (CA) in 2021; the Computer Network Operations training project will be in OA in 2016 with an estimated CA in 2023; and the Cyber Security Architecture project again in OA in 2016 with an estimated CA in 2023.

workforce, including key decision-makers, and develop a holistic cybersecurity programme that integrates sound requirements engineering, system security engineering, internally and in industry, and risk management.

This paper is organized as follows: Chapter Two provides a review of relevant literature and examines potential approaches to ensuring cybersecurity in information systems, Chapter Three examines the Halifax Class Modernization as a case study where cybersecurity was an active element of focus in implementation of the project, Chapter Four analyses, in general, the approaches presented in Chapter Two in the context of DND/CAF major capital procurement and Chapter Five presents recommendations and conclusions for DND and the CAF to improve cybersecurity in future procurements.

CHAPTER 2 – LITERATURE REVIEW

The previous chapter demonstrated that both the increased use of COTS hardware and software as well as the ubiquity of software centric systems defines a vastly more threat rich environment for the CAF when acquiring combat and platform systems. Ultimately, the systems that are acquired must be resilient and defensible against modern threats and thus this research will examine what must be done to promote the acquisition of cyber-secure or cyber-resilient systems. In reviewing existing literature on developing secure systems there are several common themes: clearly define and elicit security requirements as well as integrate security, whether in the requirements form or as a consideration, as early as possible in the life-cycle of the system while continuing to pay attention to it throughout. In addition to those themes there was also strong evidence in support of security focused systems engineering. Specific focus on security requirements engineering has been given as it has the potential for high payoff whereas a holistic integration of security management or System Security Engineering throughout the system design life-cycle represents a more complete approach that may include some focus on requirements. In either case security must be considered early on in the process of development and acquisition.

Security Requirements Engineering

Security requirements engineering should be viewed as a root-cause approach to delivering cyber-secure systems. In systems engineering it is well accepted that failing at the requirements definition phase of a project will have a significantly negative impact on the success of a project.[49] This can be for a number of reasons including not delivering the functionality desired or poor implementation leading to low-quality. Dr. Nancy Mead, a senior researcher of Carnegie-Mellon University's Software Engineering Institute and its Computer

[49] Allen et al., *Software Security Engineering: A Guide for Project Managers*, 74.

Emergency Response Team (CERT) Division, has written extensively on security requirements engineering. Her specific focus was on software security requirements but when considering the near omnipresence of software in modern systems this work extends easily to generic systems engineering. In view of the conclusions she presented in various works, it can be seen that these would apply to systems generically without needing to be specific to software.

Dr. Mead stated that most attempts to write security requirements generally resulted in lists of security features.[50] Examples of these features are: anti-virus software, use of passwords, firewalls and encryption. She further argued that these features were "not security requirements at all but rather implementation mechanisms that [were] intended to satisfy unstated security requirements."[51] This approach resulted in the necessary security requirements specific to the systems needs for protections being left out. An additional element of focus Dr. Mead brought forward was the requirement to consider the attacker's perspective when defining security requirements. She argued that an attacker would not be interested in system features and functionality unless they were useful in conducting some form of attack. Her main argument was "that a systematic approach to security requirements engineering [would] help avoid the problem of generic lists of [security] features and to take into account the attacker perspective."[52]

In reviewing the importance of general requirements engineering, Dr. Mead, highlighted the relative cost between correcting defects in the early stages of a project, requirements development being the earliest, and in the maintenance phase (i.e. system operational). Seminal studies have shown that the repairing defects in the maintenance phase could cost between ten

[50] Nancy Mead, "Security Requirements Engineering," *Build Security In*, sec. Requirements, August 10, 2006, last modified July 14, 2010, https://buildsecurityin.us-cert.gov/articles/best-practices/requirements-engineering/security-requirements-engineering.
[51] Ibid.
[52] Ibid.

and 200 times more than if detected and rectified in the requirements phase.[53] She did also note that requirements problems lead projects to: be over budget, deliver late, suffer from significant scope reduction or cancellation, produce poor-quality applications and deliver products that are underutilized once delivered.[54] Further, she highlighted common problems in five areas of requirements engineering: requirements identification, requirements writing, requirements specifications, requirements analysis and modeling, and requirements management. The failure to include pertinent stakeholders when identifying requirements was noted. Logically, security stakeholders should contribute in ensuring key security requirements were included in a system but often this does not occur.[55] When writing security requirements, Dr. Mead noted that mainly architectural constraints or implementation mechanisms were described. These statements did not describe what the system must do and although this was focused on security this certainly extends to other areas. Stemming from poorly written requirements statements, requirements specifications were also determined to be problem areas. Key problems with the specifications were noted to be ambiguous language which could be seen as being related to infeasible or un-testable requirements. Also, due to stove piping requirements (i.e. keeping them in separate sections or not linking them) the overall specification could become inconsistent with change or not cohesive (i.e. functional requirements not being properly related to security or other quality requirements). She also noted that no requirements analysis or modeling was conducted and if it was, only a limited set of requirements were examined. The small amount of formal requirements analysis completed, was likely focused on "functional [and] end-user requirements,

[53] BW Boehm and Philip N. Papaccio, "Understanding and Controlling Software Costs," *Software Engineering, IEEE Transactions On* 14, no. 10 (1988), 1462-1477.; Steve McConnell, "From the Editor: An Ounce of Prevention," *IEEE Software* 18, no. 3 (May-June, 2001), 5-7.

[54] Robert N. Charette, "Why Software Fails [Software Failure]," *Spectrum, IEEE* 42, no. 9 (2005), 42-49. in; Mead, *Security Requirements Engineering*

[55] There are a variety of reasons why a stakeholder may not be engaged in requirements identification but the applicable ones will be discussed further in the analysis chapter of this paper.

ignoring quality requirements… such as security….”[56] Finally, she presented common areas of weak requirements management mainly focusing on storing and relating requirements and their attributes and change management. The results of these failures were stated as being neglecting quality requirements: the ‘ilities[57], performance, safety and security from the requirements set. If any quality requirements would be included they would likely take the form of vague generalities about quality vice a set of atomic measurable requirements.

When considering why these failures and poor results occurred, Dr. Mead, implicated inattention to the importance of requirements engineering which was exacerbated by trying to drive costs down and meet aggressive schedules. She makes a key conclusion which sounds quite elementary when stated but apparently eludes many project managers: “[i]f security requirements are not effectively defined, the resulting system cannot be evaluated for success or failure prior to implementation.”[58] Alternatively stated, if you cannot measure, test, verify or validate security requirements you cannot be certain of an implementation based on those requirements. Finally, she recommended that security requirements engineering be an iterative activity that can match the dynamics of changing needs, that it focus attention on what the system should not do (i.e. instead of what the user functionality is, what functionality should not be present), ensure that implicit assumptions about security form requirements and that the attacker must be taken into consideration.[59]

Risk Management Frameworks

The previous section discussed a very specific and narrow aspect of developing or acquiring cyber-secure systems. It attempts to plant the seed of security in the actual design,

[56] Mead, *Security Requirements Engineering*
[57] Some of the ‘ilities are noted to be: security, usability, testability, maintainability, survivability, extensibility, scalability, etc.
[58] Ibid.
[59] Ibid.

development and implementation of a system but other approaches introduce a more broad and holistic approach. The US National Institute of Standards and Technology (NIST) was tasked by the Federal Information Security Management Act in 2002 "to develop standards and guidelines for improved agency management of secure information systems."[60] In 2010, NIST published revision one of special publication (SP) *800-37* giving it a risk management focus.[61] Although, NIST standards initially did not fully apply to the US DoD in 2014 they were adopted to replace their previous *certification* and *accreditation* (C&A) programme.[62] The core documents applicable to the Risk Management Framework (RMF) published by NIST resultant from the Joint Task Force Transformation Initiative Working Group[63] were:

- *SP 800-37 Revision 1 – Guide for Applying the Risk Management Framework to Federal Information Systems;*
- *SP 800-39 – Managing Information Security Risk: Organization, Mission and Information System View;*
- *SP 800-53 Revision 4 – Security and Privacy Controls for Federal Information Systems and Organizations;*
- *SP 800-53A Revision 4 – Assessing Security and Privacy Controls in Federal Information Systems and Organizations; and*
- *SP 800-137 – Information Security Continuous Monitoring (ISCM) for Federal Information Systems.*

---

[60] "ITL History Timeline: 1950-Present," Department of National Defence, last modified March 30, 2016, http://www.nist.gov/itl/history-timeline.cfm.

[61] National Institute of Standards and Technology, *Special Publication 800-37 Revision 1 - Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (Gaithersburg, MD: Department of Commerce, 2010), 102.

[62] Department of Defense Chief Information Officer, *Department of Defense Instruction 8510.01* (Washington, DC: Department of Defense, March 12, 2014), 47. DoD Instruction 8510.01 March 12, 2014 cancelled the DoD Information Assurance Certification and Accreditation Process (DIACAP) and adopted the RMF based on NIST standards and guidelines as well as the applicable Council for National Security Systems (CNSS) Instructions (which also adopted the RMF).

[63] National Institute of Standards and Technology, *Special Publication 800-37 Revision 1 - Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, 1. JTF Transformation was made up of the Department of Defense, Office of the Director of National Intelligence (ODNI), the Committee on National Security Systems (CNSS) and the National Institute of Standards and Technology (NIST).

In the context and scope of this chapter only the first two publications will be discussed as *SP 800-53 Revision 4* mainly provided a catalogue of the security controls, *SP 800-53A Revision 4* defined the method to assess the implementation of those controls and *SP 800-137* detailed the requirements of a continuous monitoring programme which occurs typically after system implementation.

SP 800-37 Revision 1 and *SP 800*-39 both highlighted that given the complex nature of system-related security risks; the management of those risks would need to be undertaken by the whole organization. Specifically, *SP 800-39* focussed on broadly describing the management of risk with respect to Information Security. It noted that

> [l]eaders must recognize that explicit, well-informed risk-based decisions are necessary in order to balance the benefits gained from the operation and use of these information systems with the risk of the same systems being vehicles through which purposeful attacks, environmental distruptions, or human errors cause mission…failure.[64]

The risk management approach presented uses a three tier approach to span the spectrum of risk between strategic and tactical risk. The tiers used were: the *organizational view*, *mission processes view* and *information systems view*.

The *organizational view* tier (tier one) set the governance, defined the risk executive[65], risk management strategy and investment strategies (specific to information security risk).[66] Although this level of risk management is out of the scope of this chapter, a key flow down output to tier two was the prioritization of mission processes. The *mission processes view* tier (tier two) highlighted the requirement to develop "*risk-aware mission processes* to support the

---

[64] National Institute of Standards and Technology, *Special Publication 800-39 - Managing Information Security Risk: Organization, Mission, and Information System View* (Gaithersburg, MD: Department of Commerce, 2011), 1.

[65] Ibid., 12. *SP 800-39* defined the risk executive as "a functional role established within organizations to provide a more comprehensive, organization-wide approach to risk management."

[66] Ibid., 11-15.

organizational mission functions."[67] *SP 800-39* also emphasizes the creation and employment of *enterprise architecture* and *information security architecture*. A key element of the *enterprise architecture* was stated as "establish[ing] a clear and unambiguous connection from investments (including information security investments) to measurable performance improvements…."[68] It was also noted to assist in standardizing information technology usage in the organization and "provid[ing] a common language for discussing risk management issues…."[69] Finally, *SP 800-39* argued that:

> [a] well-designed enterprise architecture implemented organization-wide, promotes more efficient, cost-effective, consistent, and interoperable information security capabilities to help organizations better protect missions…and ultimately more effectively manage risk.[70]

Flowing from the *Enterprise Architecture* was the *Information Security Architecture* which was to provide "a detailed roadmap that allows traceability from the highest-level strategic goals and objectives…through specific mission…protection needs, to specific information security solutions provided by people, processes and technologies."[71]

The final view presented was the *Information Systems View* (tier three). This view was the most applicable in the scope of this paper as it specifically dealt with the integration of risk management activities into the system development life cycle (SDLC). *SP 800-39* highlighted that risk management activities must occur in each of the phases of the SDLC.[72] Those activities were as follows:

- *Initiation* phase – early information security requirements definition driven by current threat information or assumed threats was deemed critical along with general requirements definition;

---

[67] Ibid., 17.
[68] Ibid., 18.
[69] Ibid.
[70] Ibid.
[71] Ibid., 19.
[72] The five phases of the system development life cycle are: *initiation, development/acquisition, implementation, operations/maintenance,* and *disposal.*

- *Development/Acquisition* phase – mitigation of "potential design-related vulnerabilities"[73] based on threat information or assumptions, addressing supply chain risks and selection of security controls;

- *Implementation* phase – testing the effectiveness of implemented security controls and alteration of planned system implementation in reaction to threat information changes;

- *Operations/Maintenance* phase – continuous monitoring of control effectiveness and measuring risk changes resulting from alterations to the system or threat environment; and

- *Disposal* phase – more limited risk management activities but dealt with removal of data or information that could cause adverse impacts if compromised.

This research will primarily focus on the first three phases but will also examine follow-on impacts and linkages to the last two phases. *SP 800-39* further delved into the concept of *trustworthiness* which impacts risk assessment, relationships with external organizations and selection of specific products for use in information systems.

SP 800-37 Revision 1 dealt with the integration of the RMF into the SDLC and noted that "[r]isk management tasks begin early in the [SDLC] and are important in shaping the security capabilities of the information system."[74] It also noted that "[t]he RMF operates primarily at Tier 3 in the risk management hierarchy but can also have interactions at Tiers 1 and 2…."[75] The document outlined the six steps of the RMF: *categorize*, *select*, *implement*, *assess*, *authorize*, and *monitor*.[76] These steps were focussed around security controls. The associated security controls were listed in *SP 800-53 Revision 4* and were defined as "fundamental safeguards and countermeasures necessary to protect information during processing, while in storage and during

[73] Ibid., 22.
[74] National Institute of Standards and Technology, *Special Publication 800-37 Revision 1 - Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, 7.
[75] Ibid.
[76] Ibid., 7-8.

transmission."[77] Notionally, security controls could be processes, actions by people or technology and through the selection and implementation a select set of controls the overall risk of operating the system will be reduced to an acceptable level for a given operational environment.[78]

The first step, *categorize*, required the determination of level of risk associated with the system as well as the information it processes, stores and/or transmits.[79] This categorization drives the next step, *select*, which chooses the initial set of security controls for the system. Based on the previous step's results this step could involve tailoring (removing controls from a given baseline set) or supplementing the baseline set.[80] Following the selection of security controls the *implement* step deals with the implementation of the controls as well as documenting how they will be employed to protect the system.[81] Once controls were implemented the *assess* step validates and verifies that they perform as required. The next steps, *authorize,* demarcates the transition from the acquisition of a project to in-service support. The *authorize* step aggregated and documented the residual risk in the system after all the security controls were assessed and presented that to the appropriate authority for risk acceptance. The *monitor* step was a component of the in-service support or *operations/maintenance* phase of a system's life. This step required continuous evaluation of security control effectiveness as well as ensuring

---

[77] National Institute of Standards and Technology, *Special Publication 800-53 Revision 4 - Security and Privacy Controls for Federal Information Systems and Organizations* (Gaithersburg, MD: Department of Commerce, 2013), B-21. FIPS 199 defines *Security Controls* as the management, operational and technical controls (i.e. safeguards and countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

[78] As mentioned when discussing *SP 800-37* risk management from the *organizational view* would set the risk tolerance which will determine what residual risk will be acceptable for a given system. Additionally, continuous monitoring will be required to ensure that threat environment (or just operational environment) changes do not alter the residual risk such that it exceeds the organizational risk tolerance.

[79] National Institute of Standards and Technology, *Special Publication 800-37 Revision 1 - Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, 7.

[80] Ibid. 800-53r4 also provides a set of baseline controls for given system categorizations. Systems are categorized based on the security objectives of: Confidentiality, Integrity and Availability.

[81] Ibid., 8. Documentation is critical as it will contribute greatly to security assessment.

potential residual risk changes due to system modification or changes in the operational or threat environment.[82]

SP 800-37 Revision 1 further iterated that requirement generation was critical to system development and should occur as early as possible in the life cycle. It noted that "[w]ithout the early integration of security requirements, significant expense may be incurred by the organization later in the life cycle to address security considerations that could have been included in the initial design."[83] Additionally, it reinforced that "[e]arly integration of information security requirements into the [SDLC was] the most cost-effective and efficient method for an organization to ensure that its protection strategy [was] implemented."[84] An additional important aspect covered by *SP 800-37 Revision 1* was the identification of system boundaries. It emphasised that when boundaries are too large the system would become too complex to protect or risk manage and when too narrow would unnecessarily increase overhead associated with implementing information system security. Finally, the document provided detailed guidance on each of the RMF steps and sub-steps as well as outlining milestone checkpoints to ensure the application of the process was on track.

The Government of Canada Approach

In 2012 the Communication Security Establishment (CSE) published *Information Technology Security Guidance (ITSG)-33, IT Security Risk Management: A Lifecycle Approach*. This was a 'Canadianization' of the NIST series of documents and followed *SP 800-37 Revision 1 and SP 800-53 Revision 3* very closely.[85] One of the major differences was that *ITSG-33* divided the risk management processes into two levels: *Departmental IT Security Risk*

[82] Ibid.
[83] Ibid., 9.
[84] Ibid.
[85] *SP 800-53 Revision 3* was published in 2010 therefore was the basis for the security control catalog included in *ITSG-33*.

Management and *Information Systems Security Risk Management* vice the three tiered construct of the NIST guidance.[86] It also included the security controls catalogue as well as baseline security control profiles as part of the guidance document.

The focus of *ITSG-33* at the departmental level split the tier one and two views of the NIST approach attempting to focus departmental risk management responsibilities of defining security needs and controls.[87] It also aimed to identify departmental security controls that require implementation and monitoring for all systems inside that level's purview.[88] Ultimately, it provided guidance to departments of the Government of Canada (GoC) to implement IT security risk management. The guidance indicated that the department must define its business needs for security and categorize the security of its business activities. In the context of DND and CAF this implied the definition of high level operational security needs as well as the enterprise level security needs. Overall the departments of the GoC must conduct departmental level IT security threat assessments (i.e. understand the threat environment for the department), determine security control objective, develop security control profiles that match the operational domains in the department, deploy the appropriate departmental level controls and assess those controls. Additionally, the departments must continuously monitor the effectiveness of the security controls deployed and update security controls based on changes to department operations (and the domains it operates in) and the threat environment it faces.[89] Further the guidance detailed the roles and responsibilities of departmental personnel involved in IT security

[86] Communications Security Establishment, "Overview," in *ITSG-33 - IT Security Risk Management: A Lifecycle Approach* (Ottawa, ON: Communications Security Establishment, 2012c), 4.
[87] Communications Security Establishment, "Departmental IT Security Risk Management Activities," in *ITSG-33 - IT Security Risk Management: A Lifecycle Approach* (Ottawa, ON: Communications Security Establishment, 2012a), 4.
[88] Ibid.
[89] Ibid., 7.

risk management as well as providing direction on categorizing departmental business or operations.

At the *Information System Security Risk Management* level, *ITSG-33* expanded on the SDLC and further defined the necessary IT security activities. It proposed an *Information System Security Implementation Process* (ISSIP) to "help IT projects implement security solutions in information systems that satisfy the security objectives…of the departmental business activities that [the] information system supports."[90] Sub-phases were described for each phase in the previously discussed SDLC[91] and they aligned with the steps of NIST's RMF. The *Initiation* phase included: *stakeholder engagement*, *concept*, *planning* and *requirements analysis*. These sub-phases align with the *categorize* and *select* steps of the RMF. The *Development/Acquisition* phase included: *high-level design*, *detailed design* and *development*. The *implement* and *assess* steps would be performed iteratively in these sub-phases. *ITSG-33* separates the *Integration* phase into *integration and testing*, and *installation*. Each of these phases would involve the *implementation* and *assess* steps of the RMF in testing and production environments. At the end of the *installation* sub-phase the *authorize* step would be completed for the system. Finally, in the *Operations/Maintenance* and *Disposal* phases the *assess* and *monitor* steps of the RMF would be performed. Much like *NIST 800-37 Revision 1*, *ITSG-33* provided a detailed description of each risk management activity in the *Information System Security Risk Management* level. Overall, *ITSG-33* provided further detail and alignment with GoC regulations from that of the NIST series of publication but aligns well with their broad concepts.[92]

---

[90] Communications Security Establishment, "Information System Security Risk Management Activities," in *ITSG-33 - IT Security Risk Management: A Lifecycle Approach* (Ottawa, ON: Communications Security Establishment, 2012b), 1.

[91] Ibid., 5. ITSG 33 refers to the phases of Initiation, Development/Acquisition, Integration, Operations/Maintenance and Disposal as the System Lifecyle (SLC) vice the SDLC. It defines the SDLC as the first three phases of the SLC with which it aligns the ISSIP.

[92] Ibid., 4-6.

DND's Implementation

Each department in the GoC was required to implement a departmental IT security risk management programme. In DND's case, this was to replace the existing Certification and Accreditation (C&A) programme with the Security Assessment and Authorization (SA&A) programme. This was completed through the release of several orders and directives as well as the Security Assessment and Authorization Guideline (SAAG).[93]

Based *ITSG-33, SP 800-53* and *SP 800-53a* the SAAG presented a condensed process of five activities:

- categorization of the information system;
- selection and tailoring of a DND/CAF based security control profile;
- assessment and acceptance of target residual risk;
- assessment of the security control implementation and residual risk acceptance; and
- continuous monitoring.[94]

The first activity, categorization, was a direct copy of that equivalent part of *ITSG-33* in the *Concept* phase in the SDLC which was in the *Initiation* phase of the SLC.[95] This activity set the security goals for *Confidentiality*, *Integrity* and *Availability* for the system.[96] The selection of the security control profile activity directed that the profile be selected based on the system

[93] Assistant Deputy Minister (Information Management), *Defence Administrative Order and Directive 6003-0, Information Technology Security* (Ottawa, ON: Department of National Defence, 2015a).; Assistant Deputy Minister (Information Management), *Defence Administrative Order and Directive 6003-1, Information Technology Security Programme* (Ottawa, ON: Department of National Defence, 2015b).; Assistant Deputy Minister (Information Management), *Defence Administrative Order and Directive 6003-2, Information Technology Security Risk Management* (Ottawa, ON: Department of National Defence, 2014). The 6003 series of Defence Administrative Order and Directives (DAOD) deal with IT security and in 2014 DND released *DAOD 6003-2 – IT Security Risk Management* which effectively implemented the new SA&A programme.

[94] Director Information Management Security, *Department of National Defence and Canadian Armed Forces Security Assessment and Authorization Guideline (SAAG)* (Ottawa, ON: Department of National Defence, 2014), 9-12.

[95] Communications Security Establishment, *Information System Security Risk Management Activities*, 25-26.

[96] Director Information Management Security, *Department of National Defence and Canadian Armed Forces Security Assessment and Authorization Guideline (SAAG)*, 9-10.

categorization.[97] This was done in reverse order relative to *ITSG-33* where a similar activity of selecting a *domain specific* (if available) security control profile was selected based on the business activities the system would support and the domain threat assessment.[98] In DND's case, only departmental security control profiles are currently available.[99] This activity included tailoring of the profile which was to determine controls and their enhancements that were not applicable, were not to be included in the system profile or determine compensating or alternative controls. The output of this activity was the information system security control profile. A similar activity exists in *ITSG-33* as part of *Requirement Analysis* phase of the SDLC and in the *Initiation* phase of the SLC.[100] The following activity, assessment and acceptance of target residual risk, examined the delta between the selected DND/CAF security control profile and the information system security control profile (i.e. tailored profile). The concept was based on the assertion that the DND/CAF security control profiles would provide low residual risk in each of the security goals if all of the profile's security controls were implemented to the required maturity level.[101] Maturity level was a concept introduced by the SAAG and it was a metric based on the Capability Maturity Model Integration version 1.3 with respect to the implementation of a given security control.[102] Each of the DND/CAF security control profiles, assigned a maturity level for each control and enhancement. Logically, based on this concept, not

---

[97] Ibid., 10-11.

[98] Communications Security Establishment, *Information System Security Risk Management Activities*, 22-24.

[99] DND has four departmental profiles: Protected B-Medium-Medium; Secret-Medium-Medium; Secret-High-High;Top Secret-High-High; "DND/CAF IT Security Control Profiles," Department of National Defence, last modified 29 September 2015, http://img.mil.ca/nls-snn/sec/saa-eas/cp-pc-eng.asp.

[100] Communications Security Establishment, *Information System Security Risk Management Activities*, i-104, 34-36.

[101] Director Information Management Security, *Department of National Defence and Canadian Armed Forces Security Assessment and Authorization Guideline (SAAG)*, 11.

[102] Ibid., 8-9.; "Entinex' CMMI FAQ," Entinex Inc., last modified January 26, 2014, http://www.cmmifaq.info/. Entinex, a global operations performance consulting company and CMMI Institute partner, defined CMMI as "a framework for business process improvement. In other words, it is a model for building process improvement systems. In the same way that models are used to guide thinking and analysis on how to build other things (algorithms, buildings, molecules), CMMI is used to build process improvement systems." The use of CMMI to assess security controls will be further discussed in Chapter Four.

implementing controls would increase the residual risk from low. Utilizing alternative or compensating controls could also have increased the residual risk based on the assessment. This activity was to produce a residual risk that if accepted by the system's Operational Authority would become the target residual risk. If the Operational Authority did not accept the assessed residual risk for the tailored profile, adjustments to that were to be made. The fourth activity was the final assessment of the controls as implemented. This focused on assessing the maturity level of each implemented control and determining the actual residual risk. Again the outputs of this activity would be the acceptance by the Operational Authority of the residual risk and the system being Authorized To Operate (ATO).[103] The final activity was continuous monitoring of the controls, threat environment, and configuration of the system.[104] Overall, the SAAG took a few of the *Information System Security Risk Management* level activities from *ITSG-33* and attempted to align them with DIM Secur's internal processes as well as the Project Approval process. [105]

Certification Programmes

In combination with risk management there is still a requirement to have assurance that a product will provide some level of security. In the early 1980s the US produced the *Orange Book* which was DoD's Trusted Computer System Evaluation Criteria. A variety of other likeminded nations also began producing certification standards for computer equipment to be used in their governments and militaries. The three main bodies of certification were the US, Europe and Canada. In the early 1990s those countries consolidated their standards into *Common Criteria*. These internationally recognized standards were then used to certify equipment and technology

[103] Director Information Management Security, *Department of National Defence and Canadian Armed Forces Security Assessment and Authorization Guideline (SAAG)*, 39, 11-12.

[104] Ibid., 12-13.

[105] The Project Approval process consists of: Identification, Options Analysis, Definition, Implementation and Close Out.

in certain configurations against set *protection profiles.* Standards like the *Common Criteria* programme provided a level of internationally accepted assurance for system components and remain an important and useful part of assessing the overall security of a system. [106]

US Navy's CYBERSAFE

As already stated the US DoD transitioned from DIACAP to the RMF based on NIST's publications. It layered the Committee on National Security Systems (CNSS) instructions and policies on top of those and finally added a reduced set of its own policies and standards to meet DoD specific requirements.[107] Further to DoD's approach the US Navy is in the process of implementing a new programme called CYBERSAFE. This programme was modelled on its submarine safety programme known as SUBSAFE which was designed "to provide maximum reasonable assurance of watertight integrity and recovery capability."[108] The stated purpose of the CYBERSAFE programme is:

> to provide maximum reasonable assurance of survivability and resiliency of critical warfighting IS and [Platform IT (PIT)]-Control System components and processes, achieved by material and software solutions plus procedural compliance, such that cyber incidents are adequately prevented, detected, analyzed, reported, responded to, and restored from without abruptly or unexpectedly impacting mission capability.[109]

---

[106] Kathryn Wallace, *Common Criteria and Protection Profiles: How to Evaluate Information Technology Security* (Bethesda, MD: SANS Institute,[2003])., 1, accessed May 8, 2016, https://www.sans.org/reading-room/whitepapers/standards/common-criteria-protection-profiles-evaluate-information-1078.

[107] Tim Denman, "Cybersecurity and the Risk Management Framework for DoD Information Technology" (Presentation, Feburary 4, 2015, Defense Acquisition University, Fort Belvoir, VA, 2015), accessed May 8, 2016, https://dap.dau.mil/cop/daullblog/DAU%20Lunch%20and%20Learn/DAU%20South%20Lunch%20And%20Learn%20-%20FY15%202nd%20Quarter/Cybersecurity%20RMF%20LnL%204%20Feb%202015.pdf.

[108] Paul E. Sullivan, "The SUBSAFE Program" (Statement of Rear Admiral Paul E. Sullivan, U.S. Navy Deputy Commander for Ship Design, Integration and Engineering Naval Sea Systems Command before the House Science Committee, October 29, STATEMENT OF REAR ADMIRAL PAUL E. SULLIVAN, U.S. NAVY DEPUTY COMMANDER FOR SHIP DESIGN, INTEGRATION AND ENGINEERING NAVAL SEA SYSTEMS COMMAND BEFORE THE HOUSE SCIENCE COMMITTEE, 2003), accessed May 8, 2016, http://www.navy.mil/navydata/testimony/safety/sullivan031029.txt.

[109] Secretary of the Navy, *SECNAV Instruction XXXX.XX - DEPARTMENT OF THE Navy CYBERSECURITY SAFETY (CYBERSAFE) PROGRAM Version 0.6* (Washington, DC: Department of Defense, April, 2015), 3.

The CYBERSAFE programme consists of three key elements: *Cyber Systems Levels (CSL),* CYBERSAFE *grades,* and *Cyber Conditions of Readiness*. It defines four levels of *cyber systems* or portions thereof and components which were summarised as: *Platform Safety (level one), Platform Combat (level two), Networked Combat (level three)* and *Sustained Combat (level four).*[110] In essence, these levels provided system or sub-system boundaries that corral risk and impact levels. This would allow prioritization of the application of safeguards as well as the appropriate level of rigour or robustness in those safeguards.

The *CYBERSAFE grades* were defined as: *Mission Critical (Grade A), Mission Essential (Grade B)* and *Non-Mission Essential (Material Grade C).* The assignment of a *grade* provides another level of granularity of identifying key components or systems. The draft instruction noted that assignment of a large number of components as *Mission Critical* may seem to increase security (and might) but will certainly affect the costs associated with implementing the more robust security controls and safeguards. This potentially could enable more efficient application of security in a given system though a concerted effort to understand where the key points of failure, vulnerability or attack exist in a given system.[111]

Finally, the *Cyber Conditions* were set as: *Fully Networked Capability (Condition X), Semi-Networked Capability (Condition Y)* and *No Networked Capability (Condition Z).* These *conditions* aligned directly with naval damage control conditions which are used safeguard ship's watertight integrity (i.e. control flooding) and smoke control based on risk of damage.[112] In the

[110] Brian Marsh, "CYBERSAFE Overview" (Presentation, AFCEA C4ISR Symposium, April 28, 2015), accessed May 8, 2016, http://sdsymposium.afceachapters.org/wp-content/uploads/2015/05/CYBERSAFE-AFCEA-Mr.-Marsh-FINAL.pptx.

[111] Secretary of the Navy, *SECNAV Instruction XXXX.XX - DEPARTMENT OF THE Navy CYBERSECURITY SAFETY (CYBERSAFE) PROGRAM Version 0.6*, 48, 7-11.

[112] In Damage Control Condition (DCC) X-Ray very few key watertight doors and hatches remain closed and secure. In this condition freedom of movement throughout the ship is almost unimpeded but if damage were taken water and smoke would propagate easily. Conversely, in DCC Zulu all watertight doors and hatches are closed and movement through the ship is significantly impeded. In this DCC any damage taken would be contained to a

context of CYBERSAFE, when exposed to a high threat or if an attack was underway in a specific sysem, it may be prudent to compartmentalize systems or isolate them from interconnection.[113]

In addition to these key concepts, the CYBERSAFE programme assigned security controls to different *CSL* and *grades.* Through the definition of system boundaries (or the parts of the system that are mission critical) and identification of key components CYBERSAFE aims to influence the system design and certify crucial system parts to provide resilience and maximize operational readiness in conjunction with appropriate operational procedures. The CYBERSAFE programme also aims to develop a new set of specifications and standards for the identified critical components. These standards already cover technologies such as Host Level Protection, Network Firewalls and Intrusion Detection Systems.[114] The combination of these standards, defining system and mission critical boundaries will "provide maximum reasonable assurance of a hardened subset of critical warfighting components."[115]

System Security Engineering

System Security Engineering (SSE) is a somewhat new and specialized facet of systems engineering.[116] Its focus is to deliver security and trustworthiness, as system qualities, as integral components of the system through a comprehensive systems engineering approach. NIST is in the process of producing an SP on SSE and released a draft called *SP 800-160 System Security*

---

minimum number of watertight sections. DCC Yankee is in between these two. The ship will adjust its DCC based on risk for example while underway at sea the ship will be in DCC Yankee, during combat it will be in DCC Z and while alongside in DCC X-Ray.

[113] Ibid., 11-14.

[114] Rear-Admiral Bryant Fuller, "Naval Sea Systems Command - Cyber Security Industry Day" (Presentation, October 30, 2015), 7-8, accessed May 8, 2016, www.navsea.navy.mil/Portals/103/Documents/SEA05_Final.pdf.

[115] Marsh, *CYBERSAFE Overview*, 5.

[116] Although the term was defined in MIL-HDBK-1785 in 1995 focus and effort in this field has only been vigorous recently.

Engineering: An Integrated Approach to Building Trustworthy Resilient Systems.[117] Additionally, SSE is an active research area for The Technical Cooperation Program (TTCP), a Five-Eyes organization.[118] Assistant Deputy Minister (Materiel) (ADM(Mat)) staff are playing a key role in this research and its production of guidance with respect to SSE.[119]

NIST *SP 800-160 draft* introduced four key concepts to SSE: *protection needs*, *security relevance, trustworthiness and assurance,* and *security risk management*.[120] Determining the *protection needs* takes inputs from three perspectives: stakeholder, system and trade-offs (referred to as the trades perspective). A sound understanding of threats and vulnerabilities was deemed essential as that would need to be considered with respect to each input. The outcomes of this determination were the security requirements and the security policy for the system and organization.[121] *Security relevance* was focussed on understanding the relationship between the functions of the system and how they contribute (or do not contribute while not interfering) to the overall protection of the system as a whole. *Security relevant* functions were said to contribute to meeting the overall security requirements of the system.[122] These functions must be validated and verified, in the formal sense, to ensure they met the system's security requirements. *Trustworthiness* and *Assurance* were used as broad terms that take a holistic view of a system and aggregate all the contributing attributes to make an assessment. *SP 800-160* stated that "[*trustworthiness*], from the security perspective, is an attribute that reflects

---

[117] National Institute of Standards and Technology, *Special Publication 800-160 Initial Public Draft - Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems* (Gaithersburg, MD: Department of Commerce, 2014), 121.

[118] "The Technical Cooperation Program: Overview," Department of Defense, last modified November 10, 2014, http://www.acq.osd.mil/ttcp/overview/. The TTCP has active participation from Australia, Canada, United Kingdom, United States and New Zealand.

[119] Mark Jennings, "Cybersecurity Requirements & System Security Engineering" (Presentation, INCOSE Canada Conference, November 21, 2015), accessed May 8, 2016, http://incosecanada.weebly.com/conference-2015.html.

[120] National Institute of Standards and Technology, *Special Publication 800-160 Initial Public Draft - Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems*, 121, 13.

[121] Ibid., 14.

[122] Ibid., 15-16.

confidence that a security-relevant entity warrants the trust that is placed on it relative to how that entity provides or contributes to a protection capability."[123] Also important was that "[t]he [*trustworthiness*] of the system [was] not achieved simply by composing [it of] individually trusted component parts."[124] *Security Risk Management* was described as continuously evaluating the threats, vulnerabilities, impacts and their correlation. It also, like generic risk management, examined severity and likelihood in the context of security breaches or system exploitation as well as prioritized security risks, selected those that require response and determined realistic approaches to address those risks. It highlights that *security risk management* was just one aspect of risk but must be fully integrated into all SSE activities performed throughout the system life cycle.

[123] Ibid., 21.
[124] Ibid., 20.

RAND Corporation's Report for the US Air Force (USAF)

In 2014 RAND Corporation published a report titled *Improving the Cybersecurity of U.S. Air Force Military Systems Throughout Their Life Cycles*. In this report, RAND researchers focused on USAF systems where, the Air Force had more control over the design and architecture as compared to purely COTS systems. They also provided a baseline of what they considered sound cybersecurity management principles and compared those to existing legislation and policy that governed USAF systems. In this report there was a consistent theme and focus on *mission assurance* vice just security the of systems or their components. This report argued that building a completely secure system was not feasible or likely, so understanding the residual risk in the context of *mission assurance* was of key value to the USAF. Further they defined the sought after outcomes of cybersecurity management as "limit[ing] adversary intelligence exploitation through cyberspace to an acceptable level and to maintain an acceptable operational functionality (survivability) even when attacked offensively through cyberspace."[125] Also of key import was that these outcomes must be attained throughout the whole life cycle of the system.[126] In line with their focus on *mission assurance*, it was noted that "overall operational risk reduction will come from a combination of system security engineering, assessment of how mission assurance is affected, and, because the cybersecurity environment is rapidly changing, adaptive solutions."[127] A principle element and outcome of solid and integrated SSE was stated to be a robust and resilient system design and architecture.[128]

[125] Don Snyder et al., *Improving the Cybersecurity of U.S. Air Force Military Systems Throughout their Life Cycles* (Santa Monica, CA: RAND Corporation,[2014]), vii, accessed May 8, 2016, http://www.rand.org/pubs/research_reports/RR1007.html.
[126] Ibid.
[127] Ibid.
[128] Ibid.

In further support to the employment of SSE it was noted that "[s]ystem security engineering is a critical component in achieving effective cybersecurity."[129] While arguing for improvements in the use of SSE, RAND researchers contested that the controls proposed by existing RMFs cannot be successful alone. To that end the report concludes "[s]ecurity controls enveloping a system poorly designed from a security standpoint [were] unlikely to be successful…[e]ffective cybersecurity management [was] most likely to be achieved through risk mitigation guided by mission assurance goals…."[130] Additionally, they noted that security control in combination with a secure design showed promise as well as that adaptive solutions to address cybersecurity risks must be "integrated into the design phase, rather than by prescribed rules."[131]

This report produced four key findings (or root causes) and twelve recommendations.[132] The first finding was that

> [t]he cybersecurity environment [was] complex, rapidly changing, and difficult to predict, but the policies governing cybersecurity [were] better suited to simple, stable, and predictable environments, leading to significant gaps in cybersecurity management.[133]

Four key consequences were noted from this finding. First, that prescribed solutions such as security controls were not adequately comprehensive when compared to the results of sound SSE.[134] Second, the controls prescribed by the RMFs were developed specifically for COTS IT system where the purchaser did not have great influence into design, architecture, protocols or interfaces.[135] Third, the existing approaches favoured compliance at the tactical level (i.e. with

---

[129] Ibid., 10.
[130] Ibid.
[131] Ibid.
[132] Specific recommendations will be discussed in Chapter Five based on their relevancy.
[133] Ibid., 41.
[134] Ibid.
[135] Ibid.

security controls) vice achieving the strategic aims of *mission assurance*.[136] Finally, the use of standardized and prescribed security controls sent a message to the organization that compliance was more important that achieving the outcomes stated above.[137]

The second finding was that

> [t]he implementation of cybersecurity [was] not continuously vigilant throughout the life cycle of a military system, but instead [was] triggered by acquisition events, mostly during procurement, resulting in incomplete coverage of cybersecurity issues by policy.[138]

This finding covered elements that are out of scope for this paper but some of the associated consequences were still relevant to the acquisition phase of managing cybersecurity risks. One of the relevant consequences associated with this finding was that the events that drive cybersecurity come late in the design process. The RAND researchers argued that the *categorize* step of the RMF was an indicator that the system already sufficiently designed to make this type of assessment and therefore too late to effectively influence the integration of cybersecurity.[139] Additionally, they argued that existing policies forced more focus on system vulnerabilities versus threats to *mission assurance* as well as noting that cross-system and cross-program vulnerabilities were not captured or managed well.[140]

The third finding was focused on organizational challenges and spoke to control of and accountability for the cybersecurity of systems. It was stated that "[c]ontrol of and accountability for military system cybersecurity [was] spread over numerous organizations and [was] poorly integrated, resulting in diminished accountability and diminished unity of command and control for cybersecurity."[141] The final finding was that "[m]onitoring and feedback for cybersecurity

---

[136] Ibid., 41-42.
[137] Ibid., 42.
[138] Ibid.
[139] Ibid., 43.
[140] Ibid.
[141] Ibid., 44.

[was] incomplete, uncoordinated, and insufficient for effective decision[-]making or accountability."[142] The consequences they noted were that many gaps in the feedback and monitoring existed and what did exist failed to completely survey all systems or examine operational impacts of cybersecurity weaknesses. Ultimately, the consequences of this finding were that decision-makers were not adequately informed of the risks they were accepting and individual accountability for cybersecurity shortcomings was not adequately instilled in the organization.

Of note, the authors discussed the lack of discussion on cybersecurity requirements indicating that "[r]equirements that [were] specific enough to be placed on contract and used as benchmarks for operational testing [were] unlikely to be sufficient."[143] They argued that sound SSE would have a better chance of producing the necessary cybersecurity solutions.[144] From the perspective of robustness and resiliency the authors indicated that the requirements would be similar to those for "robust power delivery in an aircraft."[145]

In summary, the authors indicated that "[n]o changes to policies will be effective without an adequately educated and trained workforce to implement them."[146] Early on in the report it was noted that cybersecurity was highly technical and changed rapidly so in order to be effective protective measures needed to be integrated into designs and architecture through SSE.[147] Essentially, the authors argue that a first principles approach to securing systems must be taken: building security, robustness and resilience in from the start. Additionally, the authors

[142] Ibid., 44-45.
[143] Ibid., 46.
[144] Ibid.
[145] Ibid.
[146] Ibid., 55.
[147] Ibid.

highlighted that engineers working to secure systems must be able to consider the attackers perspective without being restrained by the organizations view of how to defend.

Summary

Four different approaches (or key components of approaches) to system security were reviewed. Dr. Mead in her work on *Security Requirements Engineering* argued that getting the requirements correct early on in the development of a system will produce high payoffs in the future both in cost and system security. The RMF documents all provided the common theme of integrating security risk management as early as possible and ensure it that it would be done throughout the life cycle of the system. They also introduced the requirement to have the security risk management integrated into the organization especially to define the operation (or business) needs for security at a higher level than system-specific. The US Navy's CYBERSAFE programme introduced methods to view systems from the perspective of mission criticality and survivability. The RAND Corporation's work emphasised the reliance on SSE to ensure security was designed into the system from inception and argued that even the RMFs were not integrating security early enough. They also presented important findings as to why the existing US DoD was challenged to produce truly cyber-secure systems. Common to all three approaches was the notion that in order to have success developing or acquiring a cyber-secure system, security must be designed-in or built-in. This requires input from educated project staff to integrate requirements engineering, system security engineering, internally and in industry, and risk management. The RMF and SSE approaches, as they looked more broadly as the system life cycle, also emphasized the necessity of managing security risk from cradle to grave.

CHAPTER 3 – HALIFAX CLASS MODERNIZATION: A CASE STUDY

This case study was analyzed to illustrate the existing conditions in which the CAF, specifically ADM(Mat) on behalf of the Royal Canadian Navy, attempted to address cybersecurity in combat and platform systems. This study will primarily examine the initial requirements of the project related to security and discuss some of the outcomes of cybersecurity related activities. The Halifax Class Modernization\Frigate Life Extension (HCM\FELEX) project received preliminary project approval in June 2007. The primary objective of the project was to modernize the combat suite of the Halifax Class frigates, which were built in the early to mid-1990s.[148] In order to reduce overall integration risk, several individual system upgrade projects were consolidated into the original Frigate Life Extension (FELEX) project in 2006.[149] These projects were:

- the Halifax Class Modernized Command and Control System (HMCCS) project;
- the Halifax Class Radar Upgrade;
- the Identification Friend or Foe (IFF) Mode S/5 project; and
- the Multi-LINK project.

The project was then made up of three main components: ship enhancements and derived requirements, combat system enhancements, and combat systems integration and interfacing.[150] The ship enhancements and derived requirements included: improved degaussing, improved fuel efficiency, improved stability, Commander Task Group (CTG), operations room modifications and upper-deck modifications. The combat systems enhancements were: the command and

---

[148] Director Maritime Requirements Sea, *HALIFAX Class Modernization Statement of Operational Requirements Version 2.0* (Ottawa, ON: Department of National Defence, 2007a), 1-2.; Paul Daniel, "HCM, FELEX and HCM/FELEX Background" (Presentation, October 8, 2015, Department of National Defence, Ottawa, ON, 2015).

[149] Ibid.

[150] Director Maritime Requirements Sea, *HALIFAX Class Modernization/Frigate Equipment Life Extension Statement of Operational Requirements Version 2.0* (Ottawa, ON: Department of National Defence, 2007b), 6.

control system upgrade, radar suite replacement, IFF replacement, Multi-LINK replacement, electronic support measures (ESM) replacement, Internal Communications Systems enhancements and Harpoon Weapons System (HWS) upgrade. The combat systems integration and interfacing component included all of the integration and interfacing of sensors, command, control, communications, computers and intelligence (C4I) and countermeasures systems.[151] In addition to the aforementioned systems, many of the capitally funded standalone combat systems enhancements and the national procurement funded mid-life maintenance and sustainment activities required some level of integration or interfacing. Although some of the modernization elements were not combat suite related the bulk of the project was combat systems enhancements. All of these enhancements involved modern COTS hardware and software. A notable non-combat systems enhancement was the Integrated Platform Management System (IPMS) which also heavily leveraged COTS hardware and software.

Requirements

The requirements for the HCM/FELEX project flowed hierarchically from the HCM Statement of Operational Requirements.[152] This document provided broad requirements with respect to the whole modernization of the ship and described the high-level operational requirements. Subordinate to that document was the HCM/FELEX SOR which provided more detailed requirements, primarily with respect to integration and interfacing of systems as part of the modernization as well as an annex containing SORs for each of the systems to be upgraded, enhanced, or replaced as part of the project.[153] Those requirements then flowed into the Combat

[151] Ibid.

[152] Director Maritime Requirements Sea, *HALIFAX Class Modernization Statement of Operational Requirements Version 2.0*

[153] Director Maritime Requirements Sea, *HALIFAX Class Modernization/Frigate Equipment Life Extension Statement of Operational Requirements Version 2.0*

Systems Integration (CSI) Performance Specification (PS) or CSIPS.[154] This document focused on providing the performance based requirement that would enable the integration contract to design and build the systems.

The final artifact relevant to the context of this paper is the Design and Build (DAB) Statement of Work (SOW).[155] This document described the work that the integrator needed to perform during the implementation phase of the project as well as provided Data Item Deliverable (DID) descriptions for work products the contractor needed to provide to the Project Management Office (PMO).

Required Security and Analysis

Although in the HCM SOR's General Threat Overview did not capture the threat from cyber-attack, it did note that "the modernized Halifax Class shall defend itself against attack on information systems."[156] This single high-level operational requirement alone implied that the ship's information systems needed to be defensible in the cyber domain. It would be challenging to know if the broad cyber threat was envisioned or not, but the fundamental language existed as a requirement. The HCM SOR also referred directly to *Leadmark 2020* and the requirements to address *C4ISR* and *Self-Defence. Leadmark 2020*, stated the defining characteristics *C4ISR* and the cybersecurity relevant excerpts were: "ready access to military and civilian sources of…communication…[and] …interference resistant, multi-access and multi-level security

[154] Project Management Office Halifax Class Modernization/Frigate Life Extension, *Halifax Class Modernization/Frigate Life Extension Combat Systems Integration Performance Specification Version 10.0* (Ottawa, ON: Department of National Defence, 2007c).

[155] Project Management Office Halifax Class Modernization/Frigate Life Extension, *Halifax Class Modernization/Frigate Life Extension Combat Systems Integration Design and Build Statement of Work Version 15.4* (Ottawa, ON: Department of National Defence, 2015).

[156] Director Maritime Requirements Sea, *HALIFAX Class Modernization Statement of Operational Requirements Version 2.0*, 6.

systems."[157] It that case, those characteristics were extremely broad but described high-level capabilities that were required. Of note, *interference resistant* does imply resilience and integrity in the communications channel which gave some precision to what might be required. The reference to *multi-access and multi-level security systems* was more focused on capabilities but does imply some specific security requirements to enable these specific types of systems.[158] It should be noted that the capabilities of *multi-access* and *multi-level secure* systems were and are aspirational. The security requirements for *multi-access* and *multi-level secure* systems are not well defined or understood in the GoC.[159] With respect to *Self-Defence, Leadmark* did not note a threat from cyber-space but did include relevant characteristics. It stated the relevant defining characteristics as: "[c]apable of providing defence against kinetic, electronic, electro-optical, acoustic, EMP, nuclear, biological, chemical or information attacks…[and]…[p]rotection of information systems through encryption, anti-jam and anti-virus abilities."[160] It can be seen that attacks on information systems was being considered in 2001 (*Leadmark 2020*) and 2007 (HCM

[157] Director of Maritime Strategy, *LEADMARK: The Navy's Strategy for 2020* (Ottawa, ON: Department of National Defence, 2001), 132.

[158] Committee on National Security Systems, *Committee on National Security Systems (CNSS) Glossary: CNSS Instruction no. 4009* (Ft Meade, MD: National Security Agency, 2015), 84. CNSSI No. 4009 defines *multi-level security* as the "[c]oncept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances and denies access to users who lack authorizations." This was researched by the US DoD in the late 1960s and resulted in the Bell-LaPadula model which is considered seminal work on *multi-level security*. Most systems considered *multi-level secure* implement a form of that model. Currently, the term *Cross Domain System* (or *Solution*) has been used to describe systems that interconnect multiple security domains and therefore implement some form of *multi-level security*. *Cross Domain Systems* are broken down in to two types: access and transfer solutions. Access solutions allow the user to access multiple security domains but a prevented from transferring data between them. Transfer solutions allow data to be transferred between security domains. Given the risk that classified data could migrate to a system of lower classification through a CDS, these systems have very stringent requirements which are not always openly defined. The rigor and assurance required for national authorities to approve the use of a CDS is high. Work continues on implementing CDS in the GoC due to the potential operational and resource efficiency gains. In the case of the HCM project there was a strong desire to eliminate multiple laptops each connecting to a different network (read: security domain) from the Operations Room where space was at a premium.

[159] Communications Security Establishment, *ITSB-120 Cross Domain Security Primer* (Ottawa, ON: Communications Security Establishment, 2016), 3. This IT Security Bulletin indicated that only CSE –approved CDS should be used for information at security levels above Protected B (i.e. Protected C and classified systems).

[160] Director of Maritime Strategy, *LEADMARK: The Navy's Strategy for 2020*, 137.

SOR) but what was considered an information system may still have been too narrowly focused on traditional IT systems leaving out platform and combat systems.

The HCM/FELEX SOR dealt with integration and interfacing but did not discuss security requirements, nor did it address security requirements for integration or interfacing between systems. Further, the annexes addressing the operational requirements for each system provided extremely limited security relevant requirements. In the case of the Internal Communications System (ICS) the user terminal was required to have password and non-password based user authentication. The Electronic Support Measures (ESM) system required that the main emitter library was non-modifiable from the operator workstation and that once the tactical and main libraries were removed the system shall be deemed unclassified. The Command and Control System (CCS) requirements were limited to those surrounding the Isolated Auxiliary Information System. This system was to integrate systems with difference security classifications using government approved *multi-level security* solutions (also known as a *Cross Domain System* or *Solution* (CDS)) at the user workstation.[161] As discussed in Chapter Two, security was a component of system quality but in the sub-system annexes security was not mentioned in the quality sections. In those sections, the following systems were defined as mission critical: CCS, ESM, IFF and the Radar Suite. Although, the HCM/FELEX SOR provided more granularity, it did not address security in any real or valuable respects and focused mainly on system features, functionality and what and how systems should integrate into the overall Combat Suite.

[161] GoC approved CDS do not exist in general and did not exist in 2007 as demonstrated by the most recent ITSB-120. Again, this requirement was aspirational in that it expected that by the implementation phase an approved solution would be available. The current reality is that the RCN has a multi-caveat CDS access solution approved for use meaning at one security level multiple networks can be accessed of different releasability caveats. This system meets the bulk of the operational requirements for access CDS for the RCN today but does not fully meet the requirements set forth by the HCM/FELEX nor does it provide any transfer CDS capability.

The CSIPS main document included a few sections that were security relevant and common to all sub-systems. In this document the whole Combat Suite was referred to as the Combat System (CS) and the sub-systems that made up the CS and were being integrated as part of the CSI were called Combat System Integration Components (CSIC). In the section titled *System Management*, there were two security relevant sub-sections of requirements: *Access Management* and *System Security*. The *System Management* requirements were identified as common to all CSICs therefore these two sub-sections were meant to cover all aspects of security for the modernized Halifax Class CS.

The *Access Management* sub-section detailed that the systems were required to control access based on user identity and user roles.[162] Based on these identified users and roles, and if they were authorized, the CSICs were required to limit access to functions, sub-systems and information. This sub-section further detailed that the systems were required to manage user accounts, credentials, roles and authorizations as well as the relationship between users and roles.[163]

These access control requirements were a reasonable set of initial expectations of how the system would allow operators to use the system. Given the general nature of the requirements as stated there were no standards defined to which the mechanisms chosen by the implementer could be measured. This set of requirements lacked depth in defining the robustness or strength

[162] Specific user roles identified were: Commanding Officer, Warfare Officer, Operations Room Officer, Above Water Warfare Director, Track Supervisor, Air Raid Reporting Operator, Electronic Warfare Supervisor, Under Water Warfare Director, Anti-Submarine Plotting Operator, Sonar Control Supervisor, Sonobuoy Processing System Operator, Information Management Director, Shipboard Air Controller, Operations Room Supervisor, CCS Technician, Command Task Group Watch Officer, CCS Administrator, and CCS Shipboard Embedded Training Tool Controller.Director Maritime Requirements Sea, *HALIFAX Class Modernization/Frigate Equipment Life Extension Statement of Operational Requirements Version 2.0*, 8.; Project Management Office Halifax Class Modernization/Frigate Life Extension, "Appendix 1 Command and Control System," in *Halifax Class Modernization/Frigate Life Extension Combat Systems Integration Performance Specification Version 10.0* (Ottawa, ON: Department of National Defence, 2007a), 8.

[163] Project Management Office Halifax Class Modernization/Frigate Life Extension, *Halifax Class Modernization/Frigate Life Extension Combat Systems Integration Performance Specification Version 10.0*, 16-17.

needed. As a result, these requirements could have resulted in any particular method or mechanism with no measurable strength as the implementation was completely left to the designer. Although, these requirements were meant to performance based vice prescriptive, this case demonstrates that security performance was not considered. The high-level needs for access control were defined but there was no standard that the end implementation could be measured against and thus these requirements presented real risk that the desires of the HCM/FELEX project would not be effectively met. A metric for the measurement of success of the design should have been established prior to selection of the desired solution.

The *System Security* sub-section first described the requirement to exchange information in a careful and control fashion with allied units as part of a multi-national naval task force.[164] It also noted that the data and information would be classified at different levels and releaseability caveats.[165] The requirements stemming from these assertions were that the systems had to manage data in different communication domains (i.e. with other groups of allied nations) and they had to manage data at different security levels and caveats. These elements alone provided a broad description of a *multi-level secure* system. The notion of the PS requiring a *multi-level secure* system was further supported by the requirements provided in the *Information Exchange* Annex to the CCS Appendix.[166] This requirement implied specific security measures due to the risks and challenges associated with implementing a *multi-level secure* system. In line with this requirement the PS stated that the systems shall manage and control the distribution of data up to

[164] Ibid., 18-19.

[165] DND and the CAF use the following levels of classification: Unclassified, Confidential, Secret and Top Secret. Releasability caveats dictate specific groups that are authorized to access the information. These caveats are commonly used to indicate with which other nations the information can be shared (i.e. Secret CANUS indicates Secret level information that can be shared with US personnel holding the appropriate security clearance).

[166] Project Management Office Halifax Class Modernization/Frigate Life Extension, "Appendix 1 Command and Control System Annex 1.5 Information Services," in *Halifax Class Modernization/Frigate Life Extension Combat Systems Integration Performance Specification Version 10.0* (Ottawa, ON: Department of National Defence, 2007b).

and including the Secret level. Additionally, the systems were required to have services to protect the data according to its security level and caveat. Other key security requirements in this sub-section were that the CSICs shall be compliant with the National Defence Security Policies and Instructions (NDSP and NDSI) as well as the Operational Security Standard for Information Systems (OSSIS).[167] These requirements were reiterated in the *Information Exchange* Annex to the CCS Appendix of the PS. That annex also noted that due to *multi-level security* constraints the Secure Local Area Network (SECLAN) system could not be integrated into the CCS.[168] This statement seemed to be in conflict with the assertion that the CSICs would be a *multi-level secure* set of the systems by requirements in the CSIPS although not explicitly stated. Additionally, further detailed requirements were provided in this annex on the filtering and control of data and information flow. These requirements were predominantly focused on ensuring that the systems and users could manage and control the data flow such that undesired release of classified or sensitive data could be prevented. It also stated that CSIC hardware must be able to be rendered unclassified once classified data was removed from the system. The final security requirements were to do with emissions security (EMSEC) and TEMPEST.[169] In 2014,

[167] Director Information Technology Security. A-SJ-100-002/AS-001, *DND/CF Operational Security Standard for Information Systems* (Ottawa, ON: Department of National Defence, 1998).

[168] Project Management Office Halifax Class Modernization/Frigate Life Extension, *Appendix 1 Command and Control System Annex 1.5 Information Services*, 6.

[169] Jeffery Friedman, "TEMPEST: A Signal Problem," *National Security Agency Cryptologic Spectrum*, 1972, 26, accessed May 8, 2016, https://www.nsa.gov/news-features/declassified-documents/cryptologic-spectrum/assets/files/tempest.pdf.; Committee on National Security Systems, *Committee on National Security Systems (CNSS) Glossary: CNSS Instruction no. 4009*, 47. In Friedman's article it was noted that the covername TEMPEST was given to compromising radiation from information-processing equipment that was processing classified data. CNSSI No. 4009 defines EMSEC as "[t]he component of communications security [(COMSEC)] that results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from cryptoequipment and information systems. See TEMPEST."

the PS was changed through a contract change proposal to include that CCS equipment on the bridge would be TEMPEST Level 1 certified.[170]

This section of requirements in the CSIPS was focussed on four areas: *multi-level security*, rendering hardware unclassified, compliance with NDSP, NDSI and OSSIS, and EMSEC/TEMPEST. As has already been noted, *multi-level secure* systems or CDS were, and remain a challenging prospect. The approach of defining a number of requirements that implicitly point to providing a CDS but not explicitly requiring that solution must be questioned. The CCS was a central point of integration and interconnection between the various modernized and legacy combat systems. It was to take data and information from all of these systems and fuse it into a common picture that would enable rapid decision making and prosecution of threats to the ship. Not all of the systems providing data and information processed or stored classified data. This presented a new problem of how to keep the classified data contained in the CCS from leaking out into those unclassified systems. This problem could be rephrased as how to keep those unclassified systems from being contaminated with classified data from CCS. This second perspective considered the additional protections and restrictions associated with the design, construction and maintenance of classified systems. An additional conflicting consideration was that "[t]he *CCS* and *SECLAN* operate in different security domains, and thereby impose Multi-Level Security constraints that prevent *CCS* information and services from being integrated to *SECLAN* information and Services."[171] In that case, the authors of the requirement specification noted that CCS and SECLAN operated in different security domains, although both operated at

[170] Project Management Office Halifax Class Modernization/Frigate Life Extension, *Halifax Class Modernization/Frigate Life Extension Combat Systems Integration Performance Specification Version 11.4* (Ottawa, ON: Department of National Defence, 2014a), 20. TEMPEST Level 1 is the highest standard for EMSEC based on US (NSTISSAM TEMPEST/1-92), Canadian (CID/09/15A) and NATO (SDIP-27/1) testing standards. Depending on where classified information systems are to be used they require a different level of TEMPEST certification (Levels 1 through 3 (Canada/US) or A through C (NATO)).

[171] Project Management Office Halifax Class Modernization/Frigate Life Extension, *Appendix 1 Command and Control System Annex 1.5 Information Services*, 6.

the same classification level and caveat, thus they could not be integrated. This logic did not persist when considering that some of the modernized sub-systems and legacy systems operated in a different security domain. It was more likely that those systems were initially considered to be in the same security domain as CCS. Ultimately, as will be further discussed later, this assumption was determined to be false. This resulted in a flawed view of the security domain(s) of the whole combat suite and ultimately would be reflected in the implementation of or lack thereof security between the CSICs.

From the perspective of the security goal of *Confidentiality* it would be very desirable to make hardware unclassified when classified data or software were removed. Beyond meeting the *Confidentiality* needs of the system it would be more cost effective and less effort to deal with unclassified components from a maintenance and logistics perspective. From strictly a *Confidentiality* perspective, before these components were loaded with classified operational software and/or data they could be stored in regular supply warehouses (i.e. not meeting the requirements to store and protect classified items from physical theft or damage), accessed and handled by personnel without higher level security clearances as might be the case for supply technicians. Additionally, these components would not require special shipping arrangements (i.e. bonded and security cleared couriers). From the maintenance and overhaul perspective, the contractors or personnel repairing the hardware would also not require higher security clearances. Unfortunately, it can be impractical to purge or sanitize classified data from certain types of computer memory.[172] Even if it were feasible to purge the all of the known memory

[172] Communications Security Establishment, *ITSG-06 Clearing and Declassifying Electronic Data Storage Devices* (Ottawa, ON: Communications Security Establishment, 2006), 5. ITSG-06 defines sanitization as "the process of erasing or destroying an EDSD in a manner that precludes any reasonable hope of recovery of the data – i.e., the risk of compromise following sanitization is low or non-existent. In addition to destroying the data, the sanitization process includes the manual removal of external indications that the device once contained sensitive data. EDSDs that have been sanitized may be declassified and disposed of as unclassified waste or as surplus equipment for sale or recycling." It also defines reasonable hope as "…a threat agent with opportunity, motivation

components in a given piece of hardware, an appropriate level of assurance (i.e. matched to the classification level) that there was not any hidden or unknown memory and that the purging method was effective, would be required. Given DND's outdated policies and the guidance provided by *ITSG-06 Clearing and Declassifying Electronic Data Storage Devices* this requirement was aspirational.[173] It would be possible to develop procedures to declassify hardware but would require departmental approval and possibly GoC approval by CSE but this represents a significant challenge. This requirement made sense as it would eliminate other risks and costs but the challenges was that it was impractical to implement and would be difficult for vendors to provide solutions with the appropriate amount of assurance. Additionally, it did not address the *Integrity* security goal in that if the hardware was declassified but the system required high *integrity*, no protections would be in place to ensure that component could not be impacted from that perspective.

The NDSP and NDSI have been replaced by the National Defence Security Orders and Directives (NDSODs). The original policies and instructions were in a few chapters but the main source was *Chapter 70 – Information Systems Security (ISSEC).* As this publication was made unavailable once the NDSODs were published it will not be analyzed. The NDSODs consolidated all IT security related orders and directives into its *Chapter 7* which mainly reiterates and supports the SAAG and associated DAODs.[174] The requirement to protect systems in accordance with the NDSI, NDSP and OSSIS hide large amounts of detail that would need to be analysed to determine the specific and relevant requirements. Although, this allowed a single

---

and capability [that] believes the presumed value of the data is worth the time and cost to attempt to recover it." DND uses the term *purge* as the equivalent of *sanitize*.

[173] A chapter of the NDSI/P did address purging magnetic media but due to its unavailability it cannot be further analysis regardless of the fact this direction was extremely dated (1990s).

[174] Director General Defence Security, "Information Technology Security," in *National Defence Security Orders and Directives* (Ottawa, ON: Department of National Defence, 2015).

requirement to cover a broad set of requirements it implied that bidding contractor would conduct a detailed analysis of policy and pick out relevant requirements. This requirements analysis, if performed solely by the contractor, could miss elements that were considered essential to the organizations operational needs for security and would exclude DND and CAF from important risk decisions about how the policy was interpreted. The use of broad policies and standards as security requirements needed to be more specific to ensure that the correct safeguards or protections were designed into the system. To successfully provide those requirements PMO staff must hold detailed knowledge of the policies and standards as well as the operational needs for security of the system. This component of the requirements, as written for HCM/FELEX, implied that detailed knowledge was lacking or unable to be properly articulated. Beyond challenges with the language used for this set of requirements, the protection standards being quoted were nearly ten years out of date (i.e. the OSSIS was published in 1998).[175] Overall, the protection requirements for the CSICs were both hard to measure and vague as well as not being current when the CSIPS was written and published in 2007.

There were only two EMSEC and TEMPEST requirements in the CSIPS.[176] Each of the requirements pointed to a particular policy with respect to compromising emanations. The challenge was the CSIPS did not identify to which level the systems and components would be certified. This required the contractor to determine the specific level of protection requirements for each system and its components. Although, the PMO was able to approve those decisions this left room for interpretation of system protection requirements and its categorization or needs for security. Eventually, in 2014, the CSIPS was amended to require some specific components

[175] Director Information Technology Security. A-SJ-100-002/AS-001, *DND/CF Operational Security Standard for Information Systems*

[176] Project Management Office Halifax Class Modernization/Frigate Life Extension, *Halifax Class Modernization/Frigate Life Extension Combat Systems Integration Performance Specification Version 11.4*, 20.

(CMS equipment on the ship's bridge), deemed by DND to be operating at the level of Secret releasable Canada and US (Secret CANUS), to meet TEMPEST Level 1 standards.[177] This was a late contract amendment and required retrofits as several ships had already completed their mid-life refits. Again, protection under existing standards and policies were required with insufficient specificity leaving risk decisions to the contractor which in this case turned out to be unacceptable.

The final source of security relevant requirements was the DAB SOW. In its description of the conduct of System Design Reviews (SDR), Preliminary Design Reviews (PDR) and Critical Design Reviews (CDR) it stated that security requirements and "the completeness of the CSIC security architecture"[178] would be reviewed. Following the release of *ITSG-33*, DND began to shift away from C&A to SA&A. The HCM/FELEX project was moved to SA&A in advance of the official release of the SAAG and associated DAODs. As a result the DAB SOW was changed in May of 2013 to include new requirements associated with the shift from C&A. A new section was added titled *Certification and Accreditation Risk Mitigation*. With this additional scope came an amendment of language with respect to C&A and it stated that "[t]he CCS, Trainers and [Combat Systems Training Centre (CSTC)] are considered to be Information System operating within the framework of DND Information management, security and infrastructure policies."[179] This statement explicitly moved these systems into the purview of DIM Secur and their approach to security. In addition, the new scope called for the contractor to:

- provide technical support to the PMO staff during the C&A process;
- provide new software tools specifically anti-virus and vulnerability scanners;

[177] Ibid.
[178] Project Management Office Halifax Class Modernization/Frigate Life Extension, *Halifax Class Modernization/Frigate Life Extension Combat Systems Integration Design and Build Statement of Work Version 15.4*, 22-25.
[179] Ibid., 47.

- provide Standard Operating Procedures (SOP) to deal with Foreign Nationals being onboard modernized frigates;[180]
- incorporate security into the software build and release process;
- conduct vulnerability scanning and address findings;
- upgrade the security classification of the Land Based Test Site (LBTS) to Secret CANUS;[181]
- investigate the feasibility of implementing unique Internet Protocol addressing schemes for each ship;
- update the security level and caveat for the final implementation of systems; and
- provide substantiation for non-classification of legacy subsystems as well as investigate port filtering solutions to allow those systems to retain their unclassified status.[182]

Although, these became contractual requirements they were reactionary in some part to the change or pending changes in the departmental approach to C&A (i.e. transitioning to SA&A based on *ITSG-33*). These also were indicative of a reaction to the lack of certain security features that were present in more traditional IT systems (e.g. anti-virus software). The amendments made to the DAB SOW represented an awakening of how combat systems were (and would be) viewed from a security perspective. These SOW requirements as well as the TEMPEST updated noted in a later version of the CSIPS were, effectively, bolting certain aspects of security on while requesting the necessary technical support to gather the detail documentation required by *ITSG-33* security controls. These arising SOW requirements also highlight some un-forecasted needs as the existing policies would not authorize specific aspects

[180] Based on the requirements for the CSICs, the information systems had been assigned a high-water mark level of classification of Secret CANUS. This meant personnel, civilian or military, who were not Canadian or US citizens holding a Secret security clearance could not have access to the systems. Given that several of the CSICs were delivered by non-Canadian or non-US vendors, this posed a significant challenge during implementation of those systems onboard modernized frigates.

[181] This site was the contractor owned development and test site. It was also used to conduct training for operators and maintainers.

[182] Ibid., 48-49.

of the implementation and testing effort to continue. The specific aspects were foreign nationals, sub-contractors who were working with the prime contractor to resolve integration issues, requiring access to system that were integrated with the CCS, now known as the Combat Management System (CMS). There was no policy at the time that allowed this to occur and therefore in order to enable the integration and testing efforts to continue the PMO was required to develop, and have approved by key stakeholders, risk mitigation strategies and procedures. Additionally, when the CMS was to be connected and interfaced to certain legacy systems that were deemed unclassified, it was desired that those systems did not taken on the high water mark level of classification of Secret CANUS. Again, the existing view dictated that systems that were physically connected together without specific guards or gateways (transfer CDS) they would be classified at the level of the system with the highest classification (i.e. high-water mark classification). The final key recognition made with these changes was that what may have been envisioned as the classification of systems delivered as part of HCM/FELEX would need to be revisited and reassessed. As has been previously stated, due to initially vague requirements the contractor was left, to some extent, to decide the classification level for each CSIC which was eventually adjusted well after design.

The security relevant requirements defined for the HCM/FELEX project can be summarized in six general statements, with the addition of the more detailed level of requirements provided in the DAB SOW. The general statements are:

- the modernized Halifax Class must be able to defend itself against attacks on its information systems;
- is systems must have some form of access control based on unique user identity and assigned roles;
- the CSICs must be able to control data and information internally and externally (inflows and outflows) at variously levels (up to Secret) and caveats; it should be noted that nowhere in the requirements documents does it state that the systems

should be *multi-level secure* systems but the requirements point to the functionality and control inherent to a system of that nature;

- the CSIC shall protect data and information in accordance with the NDSP/NDSI and OSSIS;
- it was also required that when specific classified data stores were removed from the CSICs the hardware would be deemed unclassified; and
- the systems must be protected against the exploitation of emissions through EMSEC and TEMPEST.

The DAB SOW requirements can be summarized as follows:

- provide technical support to the C&A efforts performed by the PMO;
- provide anti-virus and vulnerability scanning software;
- make the IP addressing scheme for each ship unique, if feasible;
- develop procedures to mitigate the risks associated with allowing foreign nationals to access Secret Canadian and US personnel only systems; and
- develop mitigations and justifications to interconnect (i.e. integrate or interface) the CSI and legacy combat systems but prevent the requirement to reclassify formerly unclassified systems.

It can been seen from this analysis that this set of security requirements failed to fully capture the operational needs for security for the modernized Halifax Class resulting in reactionary changes and significant un-forecasted effort to appropriately manage the risks. The HCM/FELEX project failed in several of the common problem areas of security requirements engineering noted by Dr. Nancy Mead and stated in Chapter Two.[183] These problems were with requirements identification, writing, specification and analysis.[184] In addition to those challenges some of the added security requirements were really lists of mechanisms meant to satisfy unstated security requirements (e.g. anti-virus software, vulnerability scanning tools and unique IP addressing

[183] Mead, *Security Requirements Engineering*

[184] Requirements management was not included as ADM(Mat) utilized the Dynamic Object-Oriented Requirements System (DOORS) which is an advanced requirements management tool and database.

schemes). Again, this issue was also noted as being common by Dr. Mead.[185] Finally, stakeholder engagement in the development of the HCM/FELEX security requirements was an issue. There were several reasons that contributed to this lack of engagement but were eventually addressed by the PMO. First, in 2007 it was unlikely that the CCS or combat systems were viewed as suffering from the vulnerabilities noted in traditional IT systems. Additionally, there was not a great deal of notable cyber-attacks that occurred prior to 2007.[186] At this point there were no cybersecurity engineers working in the PMO. DIM Secur staff was not yet engaged to support the C&A of the systems, although the expertise brought by that group would not have been well suited to address security requirements engineering issues. Overall, the problem of cybersecurity was still not a well understood challenge on the *radar screen* for ADM(Mat) project staff even though initial steps were made to address this new, to combat systems, issue.

The application of *ITSG-33* in the absence of the SAAG[187]

As shown in the 2013 amendment to the HCM/FELEX DAB SOW, the project transitioned from C&A to SA&A, although in advance of the publishing of the SAAG. Since the SAAG was still being drafted and the term SA&A had yet to be officially used, the only guidance publication available to the PMO was *ITSG-33*. The PMO was executing activities at the *Information Systems Security Risk Management* level while reacting to the output of the activities at the *Departmental IT Security Risk Management* level (the responsibilities of DIM

[185] Ibid.

[186] "Cyber Incident Timeline," Center for Strategic and International Studies, accessed May 6, 2016, http://www.csis-tech.org/cyber-incident-timeline/. This timeline only noted one attack against an Australian Supervisory Control and Data Acquisition (SCADA) system in 2000 then approximately 18 attacks against US government and military networks, European government networks and one purported cyber-warfare attack against Estonia between December 2005 and December 2007 (when the CSIPS was released to industry).

[187] The author was part of the PMO HCM/FELEX ISSEC team from 2013-2014 and was the ISSEC lead engineer from 2014-2015. During these two years, he worked closely with DIM Secur, Director General Maritime Equipment Program Management (DGMEPM) and Director Naval Requirements (DNR) staff to gain an initial ATO for the first operationally deployed modernized Halifax Class frigate (HMCS FREDERICTON which deployed in 2014). The details in this section of how the application of *ITSG-33* unfolded for the HCM/FELEX project are mainly based on that experience.

Secur). The key outputs from the Departmental level were the Departmental Security Control Profiles and the Departmental IT Threat Assessment Reports. Other outputs at this level were the deployment and monitoring of common Security Controls. Given that DND was still transitioning from C&A to the *ITSG-33* based SA&A some of the outputs were either not available or immature when HCM/FELEX was already in implementation. The Departmental Security Control Profiles were established and HCM/FELEX was using the Secret-High-High profile.[188] The Departmental IT Threat Assessment Reports were not available to PMO staff although they were used in the development of the Departmental Security Control Profiles. Additionally, common Security Controls at the Departmental level were still under development. The lack of these key outputs from the Departmental level (inputs to the Information Systems level) challenged efficient application of the Security Control Profile. Without the broad threat assessments there was no initial basis to tailor efforts against certain threats and effectively manage risk. This resulted in the requirement to attempt to address the full spectrum of threats and apply and document all of the controls in the Security Control Profile.[189] Overall, the efforts were not able to be effectively prioritized and the resulting scope of work was significant given the available resources to address IT security.[190]

At the time of the transition from C&A to SA&A (or the application of *ITSG-33*) the HCM/FELEX project already commenced the *Integration* and *Installation* phases of the SDLC as well as was fully in the implementation phase from the perspective of the project approval

[188] Each of the terms in the profile title was associated with the three security goals respectively: *Confidentiality, Integrity* and *Availability*. In the case of HCM/FELEX and specifically the CMS, the profile used was for protection of a Secret system requiring High *integrity* and High *availability*.

[189] Assistant Deputy Minister (Information Management), *DND/CAF IT Security Control Profiles*. DND's departmental Secret-High-High profile contains 670 individual security controls and control enhancements.

[190] Project Management Office Halifax Class Modernization/Frigate Life Extension, "HCM Oversight Committee" (Presentation, February 14, 2014, Department of National Defence, Ottawa, ON, 2014b)., 50-52.

process.[191] Although, the project was in the implementation phase, there was ongoing software development meaning that some aspects of the *Development* phase of the SDLC were addressed by the PMO. Based on entering the risk management process at a late stage, there was little ability to further influence the design as it was already set and being implemented in ships. Given that this went against the principle of integrating security as early as possible the focus of effort had to be assessing the existing security in the delivered systems, enhancing security where possible through procedures, policy or engineering changes (these were in addition to the existing project scope) and preparing the documentation necessary to attain ATO.

Certification Standards and SSE

There was no equivalent programme like the US Navy's CYBERSAFE before or during the execution of the HCM/FELEX project. In a few specific instances security related certification standards were used. As previously discussed the project added the requirement for CMS bridge equipment to be certified to TEMPEST Level 1. Other equipment was TEMPEST Level 3 certified to meet DND's EMSEC policy but this was not an explicit requirement. Additionally, some minor CMS components were certified to Common Criteria standards but, again, these were not explicit requirements.[192] Overall, there was limited use of existing certification programmes and no frameworks in place similar in spirit to CYBERSAFE.

Although ADM(Mat) staff had been involved in research on SSE for some time, its approach and principles were not applied in HCM/FELEX. It reality, SSE would have needed to be a more mature aspect of Systems Engineering early in the project's life (i.e. when

[191] Daniel, *HCM, FELEX and HCM/FELEX Background*, 17. The first frigate (HMCS HALIFAX) entered mid-life refit in 2010.

[192] Director Information Management Security, *DIR IM SECUR DIRECTIVE 01/07 - Approved use of Commerical-Off-the-Shelf Keyboard-Video-Mouse (KVM) Switch* (Ottawa, ON: Department of National Defence, 2007), 7. Keyboard, video and mouse switches that connect to systems at different security classifications are required to be Common Criteria EAL4 certified. Several of these switches were used through the CMS.

requirements were being initially developed) to have been effectively used. Applying SSE after a system was designed and implemented would require the ability to significantly retrofit or re-engineer the system and the prospect of these activities occurring in the midst of implement of a major capital project was unlikely. In examining the requirements for HCM/FELEX it was noted that there was no requirement for a standardized Systems Engineering process but simply that "[t]he contractor shall conduct the necessary Systems Engineering activities…."[193] Consistent with this approach to SOW requirements, it was also stated that "[f]or software development tasks, the Contractor shall follow an established and audited software development standard."[194] The key conclusion to be drawn from these requirements is that even though SSE could not realistically be applied, formal and assessable standards for Systems Engineering and Software Development were not demanded and therefore the design and engineering principles, upon which the CSIC were designed, were wholly in the hands of the contractor. It is understandable that not demanding specific Systems Engineering or Software Development standards gave the contractor flexibility but in the context of building or designing security into systems (and software) this approach removed the ability for the PMO to audit and understand key design and development decisions and their full impacts.[195]

Summary

The HCM/FELEX project faced significant challenges with respect to implementing cybersecurity. When the requirements for HCM/FELEX were being finalized, the world was just awakening to the reality of cyber-attacks and many organizations were not positioned well to

[193] Project Management Office Halifax Class Modernization/Frigate Life Extension, *Halifax Class Modernization/Frigate Life Extension Combat Systems Integration Design and Build Statement of Work Version 15.4*, 5.

[194] Ibid., 42.

[195] Ibid., 22-25. It should be noted that the DAB SOW required security architecture and requirements to be reviewed in Preliminary Design Reviews and System Design Reviews but in the absence of principled application of Systems Engineering or Software Development as well as lacking capable and experienced Security Engineers designing security in, would still challenging.

deal with this burgeoning problem. As this field was somewhat new, especially to ADM(Mat), the limits of availability of cybersecurity expertise and experienced personnel certainly impacted the project's ability grapple with the importance of the cyber domain. The project fell into common missteps with respect to security requirements engineering and were forced to reference security policies and standards that were stale and dated. The lack of SSE or software assurance, in the form of formal software development processes, made it a challenge to build security in. Finally, the shift from C&A to SA&A part way through the implementation phase of the project introduced significant churn and un-forecasted scope. This was exacerbated by the fact that the Department was still in the process of developing and publishing guidance on this transition. Overall, the HCM/FELEX project faced a complex and growing challenge without significant policy, standards or framework support in addition to fighting the impact of inadequate cybersecurity requirements.

This case study examined the failures based on its requirements and application of a RMF which was in development. It also highlighted the lack of policies current enough to be effective in the modern cyber-threat environment. Even though this case study was RCN specific the general findings can be applied to RCAF or CA capital projects. When examining this case in hindsight, the failures were apparent but it should be noted that it is not necessarily simple to apply any of the approaches discussed in Chapter Two directly to major capital project. No single approach is likely to be a panacea for all applications and there will be adaptation required to meet the needs of complex capital procurement. This chapter examined the growing pains of a complex major capital project grappling with the realities of the new cyber-threat filled world but further analysis of the approaches and principles presented in Chapter Two is required.

CHAPTER 4 – GENERAL ANALYSIS

The previous chapter examined the HCM/FELEX project and its requirements focusing on how the methods and principles presented in Chapter Two were applied or not. It is important to understand what happened in the past to inform how methods can be applied in the future. Only time will tell if the friction points identified for HCM/FELEX will be addressed in the next major capital procurements. In order to inform future projects an examination of the techniques and principles from Chapter Two must be viewed through a feasibility lens to highlight what are the key components to their implementation in DND and the CAF, if implementation is feasible. Additionally, it is important to analyse existing DND and CAF approaches with respect to delivering cyber-secure systems.

Security Requirements Engineering

Based on Dr. Mead's and others' writing it is clear that improvements in requirements engineering provides a high payoff. Allen et al. stated that "…given these costs of poor security requirements, even a small improvement in this area would provide a high value."[196] Currently, there is no specific or standardized requirements engineering education or training available through the Materiel group.[197] Given, the potential payoffs formally educating both operations and engineering staff is a logically solution to address this challenge. The recent past, in the form of HCM/FELEX, demonstrated weakness in the security requirements and that the common mistakes documented by Dr. Mead and Allen et al. were still being made. The end result was analysed only with respect to the requirements as written but the challenges with respect to what

[196] Allen et al., *Software Security Engineering: A Guide for Project Managers*, 74.

[197] "Materiel Acquisition and Support (MA&S) Training," Department of National Defence, accessed May 6, 2016, http://dln-afiile-contentserver.mil.ca/production/cninv000000000129306/site_materiel%20acquisition%20and%20support%20training/mas_training_en.htm. No specific Requirements Engineering training is available based on the Materiel Group Training webpage. Requirements are listed as topics of study in two courses: Systems Engineering Awareness and Developing a Statement of Work and Evaluation Criteria. Neither of the courses' syllabus gave any indication that in depth requirements engineering would be studied.

was delivered are out of scope for this research. Overall, it is clear getting the requirements correct up front is essential to building in the correct security.[198] Producing sound security requirements and therefore getting cybersecurity built into systems can be further challenged by the lack of departmental vision, policy and direction in this domain. Ultimately, the organization's (department's) needs for security must be clearly established such that security requirements can be derived from them. In the case of the CAF and DND, each element must establish their domain specific needs for security and from those elicit proper cybersecurity requirements for systems.

Risk Management Frameworks

One of the first activities identified in *ITSG-33* at the *Departmental IT Security Risk Management* level was to "identify the business needs for security of departmental business activities."[199] In the context of defence, business needs translate into both business (corporate or enterprise like) and operational needs for security but conceptually these definitions are the same. With these needs defined, as stated above, valid and linked security requirements would be formulated. Additionally, these needs could be used to validate existing security policies and ensure alignment. This activity was only one of many outlined at the departmental level but in order to have success with applying the RMF these activities need to be conducted to form the proper foundation on which IT security risk management can be applied at the information systems level. The RMF approach makes sense and the Canadian specific *ITSG-33* is a grounded and applicable guideline but further work is required to ensure that DND's foundation at the

[198] "Build Security In," Department of Homeland Security, accessed May 6, 2016, https://buildsecurityin.us-cert.gov/.; Dan Ross, "Effective Continuous Monitoring," *FedTech*, Summer, 2012, 47. This is the key theme of the BSI website sponsored by the National Cyber Security Divisions of the US Department of Homeland Security and this was echoed by Dr. Ross from NIST where he stated a simple strategy to establish an effective security framework: "Build it right, then continuously monitor."

[199] Communications Security Establishment, *Departmental IT Security Risk Management Activities*, 8.

departmental level is properly established prior in support of activities at the information systems level.

Security Assessment and Authorization Guideline

The SAAG attempted to simplify the *Information System Security Risk Management* level of *ITSG-33* but washed away important concepts, activities and principles. *ITSG-33* detailed 31 activities at the information system level and the SAAG covers about 19 of them through its five defined activities or in steps of its workflow annex. One of the key activities not discussed in the SAAG was the definition of business needs for security that the system needed to address. Without this activity, the system would have to address all business needs for security. Additionally, understanding what business needs for security the system had to address would enable more efficient tailoring of control profiles and prioritize protection efforts. Another key activity not present in the SAAG was the concept of Security Assurance Level. It appears that the Security Assurance Level based on CSE's robustness model was replaced by DIM Secur's maturity level.[200] The CSE's robustness model was more complicated that DIM Secur's maturity level but was founded on existing best practices from the NSA.[201] Although, the use of CMMI to improve process based security controls could make sense, it is challenging to understand the logic and applicability of this model to assessing technology based security controls. The reason this is challenging to understand is the "CMMI is a framework for business process improvement."[202] Further to that definition, the CMMI Institute (the owner of the model) stated that "[t]he Capability Maturity Model Integration (CMMI®) is a capability improvement model that can be adapted to solve any performance issue at any level of the organization in any

[200] Communications Security Establishment, *Information System Security Risk Management Activities*, 77-87.
[201] Ibid., 77.
[202] Entinex Inc., *Entinex' CMMI FAQ*

industry."[203] The descriptions of each level of maturity described by CMMI could be construed as applying to the maturity of the implementation of controls but mainly for processes. It appears that DIM Secur staff did not fully comprehend the key concepts behind CMMI or how it could be applicable. Overall, this apparent mis-application of CMMI to assess security control implementation called into question the fundamental approach behind DND's SAAG.

Additionally, the SAAG called for DIM Secur's IT Security Advisors, assigned to projects, to evaluate the system design (high-level, detailed and final) from a security perspective.[204] These activities were directly in-line with *ITSG-33* and fits with the concepts in SSE. When facing projects as complex as HCM/FELEX where several systems were being designed, delivered and fully integrated, the volume of design review would be significant for a single advisors.[205] This issue mirrors the strain on project staff, specifically security engineers, in the overall capacity to ensure security requirements are properly integrated in the design.

Certification Programmes

The US Navy's draft CYBERSAFE instruction went beyond just certification of system components; it directed the zoning of systems (i.e. establishing system boundaries and scope), and identification of critical points of failure and vulnerability. Further it added guidance on how to manage systems and their interconnectivity in across the threat spectrum to maximize survivability and mission assurance through segregation. The RCN also has a SUBSAFE programme similar to the US Navy's therefore adoption of a CYBERSAFE-like programme

[203] "What is CMMI?" CMMI Institute, accessed May 6, 2016, http://cmmiinstitute.com/what-is-cmmi.

[204] Director Information Management Security, *Department of National Defence and Canadian Armed Forces Security Assessment and Authorization Guideline (SAAG)*, 20.

[205] Although the SAAG indicated at the advisor teams would be assigned, the author's experience with the HCM/FELEX project was that a single advisor was assigned and only a few assessors were assigned to support the project due to DIM Secur's own human resource constraints and other priority projects and activities.

would not be a significant hurdle for acceptance.[206] In a similar vein, the Royal Canadian Air Force (RCAF) may be able to integrate a CYBERSAFE-like programme into the existing flight safety programme. The Canadian Army (CA) may view this as too foreign or as a redundant to systems engineering but this would need to be further examined and is out of scope for this research. Overall, the draft CYBERSAFE instruction provided a method of viewing a system, systems of systems, and the interconnections of systems as well as identifying critical points of risk. The activities associated with a programme like this would be of value in any major capital procurement, even if only to inform decision makers about the systems and highlight their security architecture and vulnerabilities.

System Security Engineering

SSE truly embodies the concept of building security into a system and making part of the system from cradle to grave. It broadly supports mission assurance through the concept of making a system trustworthy with trustworthiness being a combination of safety, reliability, availability, resilience, and security.[207] It represents a more general approach to cybersecurity by attempting to make the aforementioned qualities inherent to the system itself.[208] SSE must occur in both DND/CAF as well as the vendors developing and implementing the system. The current challenges are a lack of SSE expertise and SSE personnel in the CAF and DND as well as determining how to motivate industry to employ SSE best practices.[209] The implementation of SSE for major capital procurement will take time and require some method to audit or a standard to demand of contractors. Without competent system security engineers on both sides of an

[206] "SUBSAFE Program," Department of National Defence, last modified October 26, 2004, http://www.forces.gc.ca/en/news/article.page?doc=subsafe-program/hnocfnn5.

[207] Jennings, *Cyber Security Requirements & Systems Security Engineering*, 5.

[208] Snyder et al., *Improving the Cybersecurity of U.S. Air Force Military Systems Throughout their Life Cycles*, 46.

[209] Jennings, *Cyber Security Requirements & Systems Security Engineering*, 13.

acquisition, cybersecurity will not be properly considered in design or development of systems.[210] At a minimum DND and the CAF must be able to properly articulate the SSE requirements and practices in project documentation such as SOWs. Additionally, subject matter expertise in SSE will be required to properly review designs and ensure cybersecurity is adequately addressed.

The RAND Corporation's conclusion from their research in improving cybersecurity of USAF weapons systems that security control compliance alone diminishes achieving mission assurance calls the RMF approach into question.[211] They also noted that it was unlikely that effective cybersecurity solutions would result from contract language and requirements whereas sound SSE would produce the desired outcomes.[212] This further reinforces the question of how to motivate or coerce industry in adopting SSE as a core set of principles with which they design and implement systems. Although, the RAND researchers challenge NIST's RMF, it was clear that there is a place for security controls and risk managed approaches but their emphasis was on a heavier weighting of SSE vice attempting to apply predetermined solutions (i.e. controls) to complex systems that may require more adaptation.

Summary

Overall, the methods and principles reviewed in Chapter Two are feasible and some have challenges in implementation and use. Security requirements engineering holds potential for high-payoff but requires great improvements in its application in DND/CAF based on the HCM/FELEX project. RMF provide a sound and standardized methodology to addressing cybersecurity in system development but must be fully integrated into the development and

---

[210] Snyder et al., *Improving the Cybersecurity of U.S. Air Force Military Systems Throughout their Life Cycles*, 55.

[211] Ibid., 44.

[212] Ibid., 46.

acquisition process. Additionally, DND's own implementation of a RMF attempted to provide an oversimplified process that still has some fundamental flaws and requires further analysis and improvement to be effective in the future. A programme like CYBERSAFE could be quickly adopted by the RCN due to its familiarity and appears to fit well with the RCAF's flight safety programme but may be too foreign for the CA to accept. Finally, SSE demonstrates promise from providing a general and inherent solution to cybersecurity but would require significant development of expertise as well as a method to ensure the same in industry. The next component of this research will be to address the completed analysis and present recommendations to improve DND and the CAF's approach to garnering cybersecurity in acquired systems.

CHAPTER 5 – RECOMMENDATIONS AND CONCLUSIONS

Recommendations

In order to address the growing issue of cybersecurity DND and the CAF must educate the workforce. The HCM/FELEX project demonstrated some of the issues that can occur when the requisite education and understanding is lacking early on in the process. As noted earlier, for a number of reasons decision-makers are not adequately informed of the risks they are accepting with respect to cybersecurity and education is one of the key factors. The personnel informing those decision-makers and the decision-makers themselves must be educated appropriately in order to effectively manage cybersecurity. This education must be fluid and updated regularly as technology and cybersecurity risks evolve. This is further supported by the statement from RAND researchers that simply updating policies will not be effective when the workforce is not properly educated to implement those new policies.[213] This played a role in the challenges in DND's implementation of *ITSG-33* but also its application to major capital projects as seen with HCM/FELEX. Beyond general education with respect to cybersecurity two key subject areas must be addressed: SSE and requirements engineering. Project staff must include educated and experienced engineers "who understand both SSE and the mindset and tactics of adversaries determined to attack through cyberspace."[214] . Additionally, system engineers and system lifecycle managers must be keenly aware of SSE considerations. Finally, personnel in ADM(Mat) as well as operational requirements developers must be formally educated in requirements engineering and specific to the subject of this research security requirements engineering. As already stated the cost of not addressing issues with requirements up front is far too high to accept in the operations and maintenance phase of a system's lifecycle.

[213] Ibid., 55.
[214] Ibid.

DND and the CAF must improve in requirements engineering and in order to support this it will require relevant and current cybersecurity policies and standards. In order to keep pace with the rapid developments in cyberspace, these policies and standards need to be flexible and adaptable. This may require significant effort and resources to keep current with the state of cyber-threats therefore DND and the CAF may need to look externally for these policies (i.e. to the expertise and experience of external consultants) and standards or focus on process and principles like SSE to develop cyber-secure solutions. Based on these standards and policies, requirements must be grounded in reality and have reasonable feasibility of being successfully delivered when the system is implemented. Again, education and subject matter expertise will be required to support this but it will avoid challenges as seen with HCM/FELEX such as the declassification of hardware or implementation of CDS. Additionally, the problem of generating requirements that were based on broad policies without performing the necessary analysis would be avoided. Sound general and security requirements engineering goes hand-in-hand with SSE and they represent high-payoff investments.

Although RAND researchers stated that requirements specific enough to be placed in a contract and operationally tested were unlikely to be successful with respect to cybersecurity solutions, major capital projects will still have contracts and requirements documents.[215] A combination of sound security requirements and SSE will be required to succeed. The key challenge, presently, is how to ensure the contractor embraces SSE in their process. One method would be to demand compliance with a standard such as *ISO/IEC 15288:2015 Systems and Software Engineering – System Lifecycle Processes*. Beyond demanding compliance, auditing may also be required to ensure that as schedule and resource pressure increase best-practices or standard processes are not shed. It is therefore recommended that DND and the CAF invest

[215] Ibid., 46.

heavily in SSE as well as investigate methods to ensure that it is used by contractors so as to enable security to be designed into systems.

As can be seen there are a number of issues to address and the rapid pace of change in this field requires agility as well as a support framework. A formalized cybersecurity programme like the US Navy's CYBERSAFE does a number of things to manage the risks in this domain. First, it creates an institutional culture where cybersecurity is everyone's responsibility. This aspect is further supported by properly educating the workforce so that all personnel have some understanding of cybersecurity. Second, it focussed and prioritizes efforts to survivability then mission assurance. This fits well with the RCN's *float, move, fight* damage control doctrine. Through the lens of survivability and mission assurance a broader perspective of the systems are taken and they included the mission as well as critical points of failure between systems. In addition to what a programme like CYBERSAFE would bring SSE and RMFs view the cybersecurity problem space to include people, process and technology. This was already highlighted in the statement that trustworthiness is not just the sum of trusted components.[216] The challenge of cybersecurity will not be solved with one single method or one perspective but a holistic view of system security. In DND's specific case this will require review and improvements to its own IT security RMF and determining the adaptations required to synchronize it with the acquisition process. DND and the CAF must develop a broad cybersecurity programme focussed on managing the specific risks with respect to acquisition of platform and combat systems.

In summary, it is recommended that DND and the CAF:

- educate the whole workforce in cybersecurity;

[216] Ibid., 20.

- formally educate requirements engineering for project staff and operational requirements developers;
- invest heavily in SSE, specifically through education, as well as investigate methods to ensure that it is used by contractors, such as auditing, so as to enable security to be designed into systems; and
- develop a holistic cybersecurity programme for acquisition that includes an improved RMF and fully integrates SSE.

Conclusions

The challenge of procuring cyber-secure and cyber-resilient systems is manageable. In order to improve cyber-security of acquired systems, DND and the CAF must educate its workforce, including key decision-makers, and develop a holistic cybersecurity programme that integrates sound requirements engineering, system security engineering, internally and in industry, and risk management. The cyber domain is a complex and rapidly changing environment where only adaptability and sound first principles will enable success. The days of security by obscurity have passed and the increasing complexity and use of COTS technology in modern software-centric combat and platform systems continues to expand the avenues of attack through this new domain. There are many approaches to address this growing problem and logically no single or static approaches are likely to succeed. This problem must be addressed at the core of the system or systems by integrating cyber-resilience and cybersecurity, as inherent qualities, into the system(s) design. The principle of designing or building security in will avoid the failings of past procurements where security was an after-thought or initially misguided. Education, awareness and a broad view of the problem space, which includes the mission, CAF personnel and the adversary's perspective, are required to succeed in defending some of Canada's most critical systems in cyberspace. Based on the analysis presented in this research it is clear that action must be taken to ensure DND and the CAF's combat and platform systems are defensible from an inevitable cyber-attack in the future. Through preparation and education,

DND and the CAF can prevent a cyber-attack from wreaking havoc on their mission critical systems.

BIBLIOGRAPHY

Albright, David, Paul Brannan, and Christina Walrond. *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?*. Washington, DC: Institute for Science and International Security, 2010. Accessed May 8, 2016. http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/.

Allen, Julia, Sean Barnum, Robert J. Ellison, Gary McGraw, and Nancy R. Mead. *Software Security Engineering: A Guide for Project Managers*. Stoughton, MA: Pearson Education, Inc., 2008.

Canada. Assistant Deputy Minister (Information Management). *Defence Administrative Order and Directive 6003-0, Information Technology Security*. Ottawa, ON: Department of National Defence, 2015a.

Canada. ———. *Defence Administrative Order and Directive 6003-1, Information Technology Security Programme*. Ottawa, ON: Department of National Defence, 2015b.

Canada. ———. *Defence Administrative Order and Directive 6003-2, Information Technology Security Risk Management*. Ottawa, ON: Department of National Defence, 2014.

———. "DND/CAF IT Security Control Profiles." Department of National Defence. Last modified 29 September 2015. http://img.mil.ca/nls-snn/sec/saa-eas/cp-pc-eng.asp.

Assistant Deputy Minister (Materiel). "Materiel Acquisition and Support (MA&S) Training." Department of National Defence. Accessed May 6, 2016. http://dln-afiile-contentserver.mil.ca/production/cninv000000000129306/site_materiel%20acquisition%20and%20support%20training/mas_training_en.htm.

Bird, Jim, Eric Johnson, and Frank Kim. *2015 State of Application Security: Closing the Gap*. Bethesda, MD: SANS Institute, 2015. Accessed May 8, 2016. https://www.sans.org/reading-room/whitepapers/analyst/2015-state-application-security-closing-gap-35942.

Boehm, BW and Philip N. Papaccio. "Understanding and Controlling Software Costs." *Software Engineering, IEEE Transactions On* 14, no. 10 (1988): 1462-1477.

Brown, Doug. "More Effective Software Management." *Maritime Engineering Journal* 3, (October, 1994): 11-14.

Center for Strategic and International Studies. "Cyber Incident Timeline." Center for Strategic and International Studies. Accessed May 6, 2016. http://www.csis-tech.org/cyber-incident-timeline/.

Charette, Robert N. "Why Software Fails [Software Failure]." *Spectrum, IEEE* 42, no. 9 (2005): 42-49.

Checkoway, Stephen, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage. "Comprehensive Experimental Analyses of Automotive Attack Surfaces." San Francisco, CA, USENIX Association, August 8-12, 2011. Accessed May 8, 2016. http://www.autosec.org/pubs/cars-usenixsec2011.pdf.

Cisco Systems. *White Paper: Defense Agencies Meet Readiness Challenges with Commercial Off the Shelf (COTS)-Based Systems*. San Jose, CA: Cisco Systems, Inc., 2005. Accessed May 8, 2016. http://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/space_COTS_v2.pdf.

CMMI Institute. "What is CMMI?" CMMI Institute. Accessed May 6, 2016. http://cmmiinstitute.com/what-is-cmmi.

Canada. Collenette, David. *National Defence: Budget Impact*. Ottawa, ON: Canada Communications Group, 1994.

United States of America. Committee on National Security Systems. *Committee on National Security Systems (CNSS) Glossary: CNSS Instruction no. 4009*. Ft Meade, MD: National Security Agency, 2015.

Canada. Communications Security Establishment. "Departmental IT Security Risk Management Activities." Annex 1, In *ITSG-33 - IT Security Risk Management: A Lifecycle Approach*, i-48. Ottawa, ON: Communications Security Establishment, 2012a.

Canada. ———. "Information System Security Risk Management Activities." Annex 2, In *ITSG-33 - IT Security Risk Management: A Lifecycle Approach*, i-104. Ottawa, ON: Communications Security Establishment, 2012b.

Canada. ———. *ITSB-120 Cross Domain Security Primer*. Ottawa, ON: Communications Security Establishment, 2016.

Canada. ———. *ITSG-06 Clearing and Declassifying Electronic Data Storage Devices*. Ottawa, ON: Communications Security Establishment, 2006.

Canada. ———. "Overview." In *ITSG-33 - IT Security Risk Management: A Lifecycle Approach*, i-10. Ottawa, ON: Communications Security Establishment, 2012c.

Cyr, Roger. "Danger — Software Ahead!" *Maritime Engineering Journal* 3, (October, 1991): 21-23.

Daniel, Paul. "HCM, FELEX and HCM/FELEX Background." Presentation, October 8, 2015, Department of National Defence, Ottawa, ON.

Defense Advance Research Projects Agency. "EXACTO Guided Bullet Demonstrates Repeatable Performance Against Moving Targets." Defense Advance Research Projects Agency. Last modified April 27,2015. http://www.darpa.mil/news-events/2015-04-27.

Denman, Tim. "Cybersecurity and the Risk Management Framework for DoD Information Technology." Presentation, Feburary 4, 2015, Defense Acquisition University, Fort Belvoir, VA. Accessed May 8, 2016. https://dap.dau.mil/cop/daullblog/DAU%20Lunch%20and%20Learn/DAU%20South%20Lunch%20And%20Learn%20-%20FY15%202nd%20Quarter/Cybersecurity%20RMF%20LnL%204%20Feb%202015.pdf.

United States of America. Department of Defense Chief Information Officer. *Department of Defense Instruction 8510.01*. Washington, DC: Department of Defense, March 12, 2014.

Canada. Department of National Defence. *1994 Defence White Paper*. Ottawa, ON: Canada Communications Group, 1994.

———. "2015 Defence Acquisition Guide." Department of National Defence. Last modified June 25,2014. Last modified June 25, 2014. http://www.forces.gc.ca/en/business-defence-acquisition-guide-2015/index.page.

Canada. ———. *Candian Defence Policy*. Ottawa, ON: Canada Communications Group, 1992.

———. "Integrated Soldier System Project (ISSP)." Department of National Defence. Last modified December 3,2013. http://www.forces.gc.ca/en/business-equipment/integrated-soldier-system-project.page.

———. "SUBSAFE Program." Department of National Defence.Last modified October 26,2004. http://www.forces.gc.ca/en/news/article.page?doc=subsafe-program/hnocfnn5.

Canada. Director General Defence Security. "Information Technology Security." Chap. 7, In *National Defence Security Orders and Directives*. Ottawa, ON: Department of National Defence, 2015.

Canada. Director Information Management Security. *Department of National Defence and Canadian Armed Forces Security Assessment and Authorization Guideline (SAAG)*. Ottawa, ON: Department of National Defence, 2014.

Canada. ———. *DIR IM SECUR DIRECTIVE 01/07 - Approved use of Commerical-Off-the-Shelf Keyboard-Video-Mouse (KVM) Switch*. Ottawa, ON: Department of National Defence, 2007.

Canada. Director Information Technology Security. A-SJ-100-002/AS-001. *DND/CF Operational Security Standard for Information Systems*. Ottawa, ON: Department of National Defence, 1998.

Canada. Director Maritime Requirements Sea. *HALIFAX Class Modernization Statement of Operational Requirements Version 2.0*. Ottawa, ON: Department of National Defence, 2007a.

Canada. ———. *HALIFAX Class Modernization/Frigate Equipment Life Extension Statement of Operational Requirements Version 2.0*. Ottawa, ON: Department of National Defence, 2007b.

Canada. Director of Maritime Strategy. *LEADMARK: The Navy's Strategy for 2020*. Ottawa, ON: Department of National Defence, 2001.

Entinex Inc. "Entinex' CMMI FAQ." Entinex Inc. Last modified January 26,2014. http://www.cmmifaq.info/.

Falliere, Nicolas, Liam O. Murchu, and Eric Chien. "W32. Stuxnet Dossier." *White Paper, Symantec Corp., Security Response* (2011). Accessed May 8, 2016. https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

Germany. Federal Office for Information Security. *The State of IT Security in Germany 2014*. Bonn, DE: Federal Office for Information Security, 2014. Accessed May 8, 2016. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014.pdf.

Friedman, Jeffery. "TEMPEST: A Signal Problem." *National Security Agency Cryptologic Spectrum* 2, no. 3 (1972): 26-30. Accessed May 8, 2016. https://www.nsa.gov/news-features/declassified-documents/cryptologic-spectrum/assets/files/tempest.pdf.

Fuller, Rear-Admiral Bryant. "Naval Sea Systems Command - Cyber Security Industry Day." Presentation, October 30, 2015. Accessed May 8, 2016. www.navsea.navy.mil/Portals/103/Documents/SEA05_Final.pdf.

Goodin, Dan. "Meet 'badBIOS,' the Mysterious Mac and PC Malware that Jumps Airgaps." *Ars Technica* (October 31, 2013). Accessed May 8, 2016. http://arstechnica.com/security/2013/10/meet-badbios-the-mysterious-mac-and-pc-malware-that-jumps-airgaps/.

Greenberg, Andy. "Hackers Reveal Nasty New Car Attacks--with Me Behind the Wheel." *Forbes* (August 12, 2013). Accessed May 8, 2016. www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/.

———. "Senate Bill Seeks Standards for Cars' Defenses from Hackers." *Wired*, July 21, 2015, sec. Security. Accessed May 8, 2016. https://www.wired.com/2015/07/senate-bill-seeks-standards-cars-defenses-hackers/.

United States. Headquarters United States Air Force, Future Concepts and Transformation Division. *The U.S. Air Force Transformation Flight Plan 2004*. Washington DC: Department of Defense, 2004. Accessed May 8, 2016. http://www.au.af.mil/au/awc/awcgate/af/af_trans_flightplan_nov03.pdf.

Honour, Eric C. “Systems engineering return on investment,” PhD thesis, University of South Australia, 2013. Accessed May 8, 2016. http://www.hcode.com/seroi/documents/SE-ROI%20Thesis-distrib.pdf.

Hudson, Trammel. "Thunderstrike: EFI Bootkits for Apple MacBooks." Presentation, Schedule 31 Chaos Communications Congress, Hamburg, DE, December 29, 2014. Accessed May 8, 2016. https://trmm.net/Thunderstrike_31c3.

Hudson, Trammell, Corey Kallenberg, and Xeno Kovah. "Thunderstrike 2: Sith Strike A MacBook Firmware Worm." Presentation, Black Hat 2015, Las Vegas, NV, August 6, 2015. Accessed May 8, 2016. http://legbacore.com/Research_files/ts2-blackhat.pdf.

International Council On Systems Engineering. *INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*, edited by Walden, David D., Garry J. Roeldler, Kevin J. Forsberg, R. Douglas Hamelin and Thomas M. Shortell. 4th ed. Hoboken, NJ: John Wiley and Sons, Inc., 2015.

International Standards Organization. *ISO-IEC 25010: 2011 Systems and Software Engineering - Systems and Software Quality Requirements and Evaluation (SQuaRE) - System and Software Quality Models*. Geneva, CH: ISO, 2011.

Jennings, Mark. "Cyber Security Requirements & Systems Security Engineering." Presentation at the International Council of Systems Engineering Canada Conference, November 21, 2015. Accessed May 8, 2016. http://incosecanada.weebly.com/conference-2015.html.

Kallenberg, Corey and Xeno Kovah. "How Many Million BIOSes would You Like to Infect?" Presentation, CanSecWest 2015, Vancouver, BC, March 20, 2015. Accessed May 8, 2016. http://www.legbacore.com/Research_files/HowManyMillionBIOSWouldYouLikeToInfect_Full2.pdf.

Kelly, Thomas, J. "The Shift to Standards-Based Hardware for Military Communications: What Role Will COTS Systems Play?" *Military Embedded Systems* (December 9, 2014). Accessed May 8, 2016. http://mil-embedded.com/articles/the-cots-systems-play/.

Kopp, Carlo. "COTS – Revolution, Evolution Or Devolution?" *Defense Today* 9, no. 1 (June, 2011): 30-33.

Marsh, Brian. "CYBERSAFE Overview." Presentation, AFCEA C4ISR Symposium, April 28, 2015. Accessed May 8, 2016. http://sdsymposium.afceachapters.org/wp-content/uploads/2015/05/CYBERSAFE-AFCEA-Mr.-Marsh-FINAL.pptx.

McConnell, Steve. "From the Editor: An Ounce of Prevention." *IEEE Software* 18, no. 3 (May-June, 2001): 5-7.

McHale, John. "Military Market One of Opportunity for Embedded COTS Suppliers." *Military Embedded Systems,* September 12, 2014, sec. Q&A. Accessed May 8, 2016. http://mil-embedded.com/articles/military-one-opportunity-embedded-cots-suppliers/.

Mead, Nancy. "Security Requirements Engineering." *Build Security In,* August 10, 2006, sec. Requirements. Last modified July 14, 2010. https://buildsecurityin.us-cert.gov/articles/best-practices/requirements-engineering/security-requirements-engineering.

Miller, Charlie and Chris Valasek. "Remote Exploitation of an Unaltered Passenger Vehicle." Presentation, Black Hat 2015, Las Vegas, NV, August 5, 2015. Accessed May 8, 2016. http://illmatics.com/Remote%20Car%20Hacking.pdf.

National Institute of Standards and Technology. "ITL History Timeline: 1950-Present." Department of National Defence.Last modified March 30,2016. http://www.nist.gov/itl/history-timeline.cfm.

United States. ———. *Special Publication 800-160 Initial Public Draft - Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems*. Gaithersburg, MD: Department of Commerce, 2014.

United States. ———. *Special Publication 800-37 Revision 1 - Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*. Gaithersburg, MD: Department of Commerce, 2010.

United States. ———. *Special Publication 800-39 - Managing Information Security Risk: Organization, Mission, and Information System View*. Gaithersburg, MD: Department of Commerce, 2011.

United States. ———. *Special Publication 800-53 Revision 4 - Security and Privacy Controls for Federal Information Systems and Organizations*. Gaithersburg, MD: Department of Commerce, 2013.

Nohl, Karsten, Sascha Krißler, and Jakob Lell. "BadUSB — on Accessories that Turn Evil." Presentation, PacSec 2014, Tokyo, JP, November 12, 2014. Accessed May 8, 2016. https://srlabs.de/blog/wp-content/uploads/2014/11/SRLabs-BadUSB-Pacsec-v2.pdf.

Nohl, Karsten and Jakob Lell. "BadUSB — on Accessories that Turn Evil." Presentation, Black Hat 2014, Las Vegas, NV, August 7, 2014. Accessed May 8, 2016. https://srlabs.de/blog/wp-content/uploads/2014/07/SRLabs-BadUSB-BlackHat-v1.pdf.

United States of America. President's Information Technology Advisory Committee. *Cyber Security: A Crisis of Prioritization*. Arlington, VA: National Coordination Office for Information Technology Research and Development, 2005. Accessed May 8, 2016. https://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.

Pricewaterhouse Cooper. *Turnaround and Transformation in Cybersecurity: Key Findings from the Global State of Information Security® Survey 2016*. London, UK: Pricewaterhouse Cooper, 2015. Accessed May 8, 2016. http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html.

Canada. Project Management Office Halifax Class Modernization/Frigate Life Extension. "Appendix 1 Command and Control System." Chap. Appendix 1, In *Halifax Class Modernization/Frigate Life Extension Combat Systems Integration Performance Specification Version 10.0*. Ottawa, ON: Department of National Defence, 2007a.

Canada. ———. "Appendix 1 Command and Control System Annex 1.5 Information Services." Chap. Appendix 1 Annex 1.5, In *Halifax Class Modernization/Frigate Life Extension Combat Systems Integration Performance Specification Version 10.0*. Ottawa, ON: Department of National Defence, 2007b.

Canada. ———. *Halifax Class Modernization/Frigate Life Extension Combat Systems Integration Design and Build Statement of Work Version 15.4*. Ottawa, ON: Department of National Defence, 2015.

Canada. ———. *Halifax Class Modernization/Frigate Life Extension Combat Systems Integration Performance Specification Version 10.0*. Ottawa, ON: Department of National Defence, 2007c.

Canada. ———. *Halifax Class Modernization/Frigate Life Extension Combat Systems Integration Performance Specification Version 11.4*. Ottawa, ON: Department of National Defence, 2014a.

———. "HCM Oversight Committee." Presentation, February 14, 2014, Department of National Defence, Ottawa, ON.

Ross, Dan. "Effective Continuous Monitoring." *FedTech* (Summer, 2012): 47.

Rouf, Ishtiaq, Rob Miller, Hossen Mustafa, Travis Taylor, Sangho Oh, Wenyuan Xu, Marco Gruteser, Wade Trappe, and Ivan Seskar. "Security and Privacy Vulnerabilities of in-Car Wireless Networks: A Tire Pressure Monitoring System Case Study." Washington, DC, USENIX Association, August 11-13, 2010. Accessed May 8, 2016, http://www.usenix.org/events/sec10/tech/full_papers/Rouf.pdf.

United States of America. Secretary of the Navy. *SECNAV Instruction XXXX.XX - DEPARTMENT OF THE Navy CYBERSECURITY SAFETY (CYBERSAFE) PROGRAM Version 0.6*. Washington, DC: Department of Defense, April, 2015.

Snyder, Don, James D. Powers, Elizabeth Bodine-Baron, Bernard Fox, Lauren Kendrick, and Michael H. Powell. *Improving the Cybersecurity of U.S. Air Force Military Systems Throughout their Life Cycles*. Santa Monica, CA: RAND Corporation, 2014. Accessed May 8, 2016. http://www.rand.org/pubs/research_reports/RR1007.html.

Strategic Initiatives Branch of the National Cyber Security Division. "Build Security In." Department of Homeland Security. Accessed May 6, 2016. https://buildsecurityin.us-cert.gov/

Sullivan, Paul E. "The SUBSAFE Program." Statement of Rear Admiral Paul E. Sullivan, U.S. Navy Deputy Commander for Ship Design, Integration and Engineering Naval Sea Systems Command before the House Science Committee, October 29, 2003. Accessed May 8, 2016. http://www.navy.mil/navydata/testimony/safety/sullivan031029.txt.

The Technical Cooperation Program. "The Technical Cooperation Program: Overview." Department of Defense. Last modified November 10, 2014. http://www.acq.osd.mil/ttcp/overview/.

Wallace, Kathryn. *Common Criteria and Protection Profiles: How to Evaluate Information Technology Security*. Bethesda, MD: SANS Institute, 2003. Accessed May 8, 2016. https://www.sans.org/reading-room/whitepapers/standards/common-criteria-protection-profiles-evaluate-information-1078.

Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York, NY: Crown Publishers, 2014a.

———. "Hacker Lexicon: What is a Zero Day?" *Wired*, November 11, 2014b, sec. Security. Accessed November 14, 2015. http://www.wired.com/2014/11/what-is-a-zero-day/.

———. "How Digital Detectives Deciphered Stuxnet, the most Menacing Malware in History." *Wired*, July 11, 2011, sec. Security. Accessed November 14, 2015. http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.

———. "How the NSA’s Firmware Hacking Works and Why It’s so Unsettling." *Wired*, February 22, 2015, sec. Security. Accessed May 8, 2016. https://www.wired.com/2015/02/nsa-firmware-hacking/.

———. "Meet 'Flame,' the Massive Spy Malware Infiltrating Iranian Computers." *Wired*, May 28, 2012, sec. Security. Accessed November 14, 2015. http://www.wired.com/2012/05/flame/.

———. "Researchers Uncover Government Spy Tool used to Hack Telecoms and Belgian Cryptographer." *Wired*, November 24, 2014c, sec. Security. Accessed May 8, 2016. https://www.wired.com/2014/11/mysteries-of-the-malware-regin/.