National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

CONSIDERATIONS: CANADIAN FORCES' EFFORTS IN THE ELECTROMAGNETIC SPECTRUM AND CYBER OPERATING ENVIRONMENT

Lieutenant-Colonel J.C. Walkling

JCSP 39

Master of Defence Studies

PCEMI 39

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 39 – PCEMI 39
2012 – 2013

MASTER OF DEFENCE STUDIES – MAÎTRISE EN ÉTUDES DE LA DÉFENSE

CONSIDERATIONS: CANADIAN FORCES' EFFORTS IN THE ELECTROMAGNETIC SPECTRUM AND CYBER OPERATING ENVIRONMENT

By Lieutenant-Colonel J.C. Walkling
Par le lieutenant-colonel J.C. Walkling

Word Count: 19 731

Compte de mots : 19 731

TABLE OF CONTENTS

List of Figures

Abstract

This paper examines how the Canadian Forces will coordinate and conduct integrated effects in a combined electromagnetic spectrum and cyber operating environment, herein called the E/CE, on behalf of the Commander of the Canadian Joint Operation Command (CJOC) and other operational-level commanders at home and abroad.

With the growing number and sophistication of threats within the E/CE, this paper recommends that CJOC establish a subordinate organization dedicated to understanding current threats and anticipating emerging issues in order to directly coordinate and execute its operations in the E/CE. Moreover, CJOC needs to look beyond its current mandate of just defending its systems, but also towards deterrence and offensive operations.

To do this, this paper argues that CJOC needs to leverage all available expertise within the E/CE-related disciplines of Communications and Information Systems (CIS), Computer Network Operations (CNO), Electronic Warfare (EW) and Signals Intelligence (SIGINT), in addition to legal and other technical subject matter experts. Consequently, such a CJOC subordinate E/CE organization will require the support of other government actors that currently have mandates and missions that influence E/CE operations, in addition to remaining mindful of its allies' activities such that they remain capable of working together on coalition operations.

CHAPTER 1 - INTRODUCTION

Imagine a Canadian-led Joint Task Force (JTF) deployed half way around the world. In this expeditionary theatre of operations, the Canadian JTF is operating under a higher coalition headquarters comprised of allies from a combination of Five-Eyes, NATO, and other coalition partners, while subordinate JTF forces are from a subset of this coalition.[1] Meanwhile, the JTF Commander also reports to a national Canadian operational-level chain-of-command, to the Commander of the Canadian Joint Operational Command (CJOC) in Ottawa who is responsible for all of the CF operations at home and abroad on behalf of the Chief of Defence Staff and ultimately the Government of Canada (GC). Now, imagine that that this JTF Commander faces a particular targeting dilemma proposed from the theatre-level Joint Targeting Board, regarding how to "engage" a proposed target. Based on the campaign plan objectives, the recommendation from the effects-based analysis is to engage the target through a non-kinetic approach that both disrupts the target for a finite period and minimizes collateral damage to the local populace and infrastructure. At the Commander's disposal are several recommendations that the staff has put together in the targeting pack. They could engage the target physically, cognitively, spectrally or via cyberspace.[2] Physical (or kinetic)

---

[1] "Five-Eyes" states include United States, United Kingdom, Canada, Australia and New Zealand. NATO (North Atlantic Treaty Organization) involves the current member nations that currently form the Alliance; see http://www.nato.int/cps/en/SID-BA7F4A89-0FE374A1/natolive/nato_countries.htm.

[2] Through the targeting process, some non-kinetic measures include influencing the adversary without necessarily destroying infrastructure, equipment or harming personnel. These measures could involve information operations that seek to influence psychologically the adversary's will or ability to do something (cognitive influence). "Spectrally" refers to operations conducted within the electromagnetic spectrum (EMS) such as electronic warfare techniques (i.e. jamming) that deny the adversary's use of the radio frequency spectrum used for voice and/or data command and control, or for sensor equipment using other frequencies of the EMS. Examples of operations within cyberspace involve influencing the information resident within (i.e. operating systems or software programs) or affecting the actual hardware, software, cable/fibre/wireless transmissions or the embedded processors to cause a desired effect.

action is rather self-explanatory, while cognitive action involves influencing activities that attempt to change the adversary's will to fight or to do something they were not otherwise intending to do – and are the aim of military information operations activities.[3] It is rather the latter two effects ("spectrally" and "via cyberspace") – which focus on the medium, and not the message therein – that are the topic of this paper.

Ostensibly, the above scenario is a hypothetical situation. Conspicuously, it involves the planning for an offensive action, even though a similar defensive scenario involving a malicious computer virus that threatened to disable all CF networks would equally raise the same concerns over how to coordinate military action in the electromagnetic spectrum (EMS) and cyber operating environments. What is perhaps most bewildering about the offensive scenario is that many CF commanders would immediately dismiss the two non-kinetic options of spectral or cyber engagement as non-starter options. While it may be beyond the CF's current mandate to conduct offensive operations within cyberspace, the desired non-kinetic effect could likely be equally achieved through the EMS by the CF's own integral electronic warfare (EW) resources or through those of its coalition partners. Therefore, it is not that there is a lack of desire to conduct spectral or cyber engagement; there is just insufficient understanding of the interdependence of the EMS and cyber operating environments, of what the planning considerations are, and who the actors are within it. As the technical functionaries within the EMS and cyberspace, operational-level CF commanders have traditionally looked upon their "J6" or the commanders of their integral "Signals" or "EW" organization for

[3] Information Operations are "actions taken in support of national objectives which influence decision makers by affecting other's information while exploiting and protecting one's own information." Chief of Defence Staff, B-GG-005-004/AF-010, *CF Information Operations*. (Ottawa: Department of National Defence, 1998), 2.

possible answers; or, in some cases, the J2 for a signals intelligence (SIGINT) solution.[4] Despite their best efforts, the known staff branches are usually insufficient manned, or are simply unable, due to their own lack of experience to leverage the expertise and limited capacity that does exist throughout the CF and elsewhere in the Department of National Defence (DND).[5] Regardless of whether it is an offensive or defensive scenario, there is no single "go-to" organization or process to follow for Commander CJOC, or the hypothetical deployed JTF commander, when needed.

This is not necessarily the fault of a given commander or their staff. It is rather symptomatic of the extensive specialization that has occurred within the EMS and the cyber environments, and the fact that the CF has not yet organized itself adequately to address the issues as a combined EM/Cyber operating environment – hereinafter referred to as the E/CE. More importantly, this predicament has led to a significant gap in understanding the E/CE and how best to coordinate integrated effects within it.[6] As the future nature of conflict promises to involve many more actors, with varying motivations, there will be less emphasis on the physical and more on the informational aspects of

[4] The CF uses the continental staff system whereby the J6 staff branch is responsible for communications and information systems (CIS), while the J2 staff branch is responsible for the functional responsibilities of the various intelligence disciplines, which includes Signals Intelligence. Chapter 3discusses the various electromagnetic spectrum and cyber-related disciplines in greater detail.

[5] Current J6 staff branches in the CF typically have sufficient planners to cover the basic provision of CIS planning and coordination, but rarely have specialists or the expertise in each of the CNO, SIGINT, EW or JEMSO disciplines. The staff's depth of expertise relies on the CIS planners' previous postings or through rather haphazard cross-training. An example is expressed in Mark Gibbs, "SigInt in Afghanistan – Task Force Afghanistan 5-10" *C&E Branch Newsletter* 54 (1 December 2010): 31-32, http://www.commelec.forces.gc.ca/inf/new-bul/vol54/doc/newslett-bulletin-vol54-eng.pdf.

[6] Major-General S. Noonan, Deputy Commander (Operational Support) for the Canadian Joint Operational Command (CJOC), offered that although there is an emerging "whole of nation" policy effort, defence in cyberspace is "non-discretionary" and that the CF "cannot afford to not have a concerted Cyber Defence effort." MGen S. Noonan, "Preparedness at the Operational Level" (lecture, Canadian Forces College, Toronto, ON, January 17, 2013), with permission.

conflict.[7] Moreover, as the hypothetical introductory scenario suggests, a multinational coalition adds more planning and interoperability challenges for those operating in the E/CE, but it also provides significant opportunity to leverage capabilities that may not necessarily be available to all specific troop-contributing nations. These challenges and opportunities will increase many fold with the multitude of other joint, inter-agency, multinational and public (JIMP) actors that will work in future conflict as part of "whole of government" or "whole of nation" comprehensive approaches.[8] It is essential that an operational-level commander have the subordinate resources to work effectively with all of these actors whether it is at home or abroad to counter the increasing number and sophistication of threats in the E/CE.

The world is becoming increasingly more interconnected using commercial wireless, computer-based networks, and ubiquitous satellite communications. Rapid technological innovation has enabled modern networks to become faster, more agile, and possess ever-greater capacity.[9] The proliferation of networks has changed the manner in which people interact with one another, and have made governments and organizations dependent upon them for their everyday business. Likewise, these networks have also changed the face of CF military operations by continuously improving efficiency through virtual collaboration, providing near-instantaneous situational awareness, and flattening

---

[7] Jonathan E. Czarnecki, "Operational Command and Control in Age of Entropy" (Paper, Twelfth International Command and Control Research and Technology Symposium, Naval War College, 2007), 12, last accessed 2 April 2013, http://www.dtic.mil/dtic/tr/fulltext/u2/a481372.pdf.

[8] Canadian Forces Leadership Institute, *Broadsword or Rapier? The Canadian Forces' Involvement in 21st Century Coalition Operations* (Kingston, ON: Canadian Defence Academy, April 2008), 2.

[9] Next Generation Networks (NGNs) over fibre and high capacity wireless networks permits additional convergence of voice, data, and video packets. Organization for Economic Cooperation and Development, *Convergence and Next Generation Networks* (OECD Directorate for Science, Technology, and Industry Committee for Information, Computer and Communications Policy, 2008), 4-5, http://www.oecd.org/sti/40761101.pdf.

command and control hierarchies.[10] This has placed a significant reliance on the availability of these networks, and thus an importance on the people and organizations throughout the CF that are responsible to provide the networks. However, the people that provide the network systems are not necessarily the same as those that protect the systems from the multitude of threats challenging them each day.

The Royal Canadian Navy (RCN), Canadian Army (CA) and Royal Canadian Air Force (RCAF) and Special Operations Forces operating in the natural domains of air, land, and sea employ many different capabilities and tools within the EMS and cyberspace. Rational thinking would assume that the military disciplines in the E/CE, such as computer network operations (CNO), communications and information systems (CIS), EW, SIGINT, and electromagnetic spectrum operations (EMSO) would already have converged. However, this has not been the case. Even in today's complex operating environment, many of the CF's capabilities for EW, CNO, CIS, EMSO and SIGINT remain diffused throughout the CF at either the strategic or the tactical levels.[11] For the Commander CJOC, who is trying to employ the capabilities during actual operations, this complicates planning, coordinating and tasking these capabilities for operational-level effects.

---

[10] Information Age advocates contest that future conflict demands further "collaboration" over "control" that is inherent to present-day "command and control" mechanisms. David S. Alberts and Richard E. Hayes, *Power to the Edge: Command… Control… In the Information Age* (Washington, DC: Department of Defense C4ISR Cooperative Research Program, 2005), Chapter 11.

[11] "Tactical" CF capabilities in the E/CE are inherently the responsibility of the force generators of the RCN, CA, and RCAF, and Special Operations Forces to develop and maintain. "Joint" capabilities, such as the CF Joint Signal Regiment, are the responsibility of their force generator, the CF Joint Operational Support Group, a formation under CJOC. SIGINT and CNO capabilities are considered "strategic" capabilities under the CF Information Operations Group, under the NDHQ Level 1 responsibility of Assistant Deputy Minister (Information Management). See Chapter 4 for more details.

Returning to the introductory scenario as an example, a commander may be inclined to target an adversary's wireless capability such as wireless routers, microwave and satellite communication links that operate in the EMS. With its relative maturity and proven ability to limit collateral effects, the EW discipline enjoys intrinsically well-understood rules of engagement and inherently lower delegated authorization levels.[12] On the other hand, although an offensive cyber-attack option is currently constrained by many legal and policy limitations imposed by the Canadian government, CNO and SIGINT would still be required to gather the network intelligence, make appropriate risk assessments, provide appropriate recommendations as part of the planning process, and assist in post attack assessment and analysis. In essence, although it may be easier for a military commander to authorize the EW attack mission, he still must draw upon the specialist expertise that comes from the other disciplines of the E/CE community of interest. By understanding the threats and recognizing the military planning considerations related to a combined E/CE, this paper will determine that the CF requires a single operational-level commander and organization that is mandated to coordinate and conduct EMS/Cyber-related effects on behalf of the CF operational-level supported commander, Commander CJOC.

Even if it is just for self-preservation, the CF must invest heavily in transforming itself to integrate the effects required in the E/CE. However, this can only occur with the coherent desire from higher levels within the CF leadership and the Canadian government. Beyond the internal machinations, government officials still call into

[12] Association of Old Crows, "A (Pragmatic) Future for Joint Electronic Warfare: Does EW + CNO = Cyber?" *The Journal of Electronic Defense* (September 2008): 32.

question the role that the DND, and in particular the CF, has to play in cyberspace. The currently stated DND/CF role within *Canada's Cyber Security Strategy* is as follows:

> The Department of National Defence and the Canadian Forces will strengthen their capacity to defend their own networks, will work with other Government departments to identify threats and possible responses, and will continue to exchange information about cyber best practices with allied militaries.[13]

Proactively, the CF has been postured well ahead of other departments to defend itself within the E/CE – but only for force protection purposes. Even the *Canada First Defence Strategy* scarcely

[13] Government of Canada, *Canada's Cyber Security Strategy: For A Stronger and More Prosperous Canada* (Ottawa: Public Safety Canada, 2010), 10, last accessed 2 April 2013, http://www.publicsafety.gc.ca/prg/ns/cybr-scrty/ccss-scc-eng.aspx.

mentions "cyber" at all:

> Canada needs a modern, well-trained and well-equipped military with the core capabilities and flexibility required to successfully address both conventional and asymmetric threats, including terrorism, insurgencies and *cyber* attacks.[14]

This short-sightedness fails to confront the multitude of cyber-attacks already acknowledged within *Canada's Cyber Security Strategy*, let alone a potentially catastrophic event such as a "Cyber Pearl Harbour" or an "e-9/11" that could cause physical destruction and lives lost.[15] Should such a possibility occur, this lack of preparation will mean that the CF will be ill prepared to respond with appropriate offensive or even defensive contingencies.

To meet the impending challenges in the E/CE, this paper will undertake a comprehensive review of several pertinent issues relevant to the CF's operational-level commander, Commander CJOC. Chapter 2 lays out the current and future threats in the EMS and Cyber environments with a view to understanding the breadth of the known threats and outline trends related to the CF's contemplated future security environment. The increasing quantity and complexity of the threats within each of the EMS and the Cyber operating environments suggests that there needs to be a coherent CF approach at the operational level. This includes recognizing that there is sufficient convergence and interdependencies between both the EMS and "Cyber domain" that would justify

---

[14] Italicized emphasis added. Government of Canada, *Canada First Defence Strategy* (Ottawa: Department of National Defence, 2008), 7, last accessed 2 April 2013, http://www.forces.gc.ca/site/pri/first-premier/June18_0910_CFDS_english_low-res.pdf.

[15] US Secretary of Defense Leon E. Panetta (speech, Cybersecurity to the Business Executives for National Security, New York City, U.S.A., 11 October 2012), last accessed 2 April 2013, http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

referring to them as one combined EMS/Cyber environment – hence E/CE. Chapter 3 addresses the military characteristics of the E/CE that are pertinent to planning operations on behalf of operational-level commanders, with a view to demonstrating the need for a collective organization to conduct the planning and execution of operations in the E/CE. An analysis of the complexity of the legal and other planning considerations required in the E/CE indicate that there needs to be a comprehensive approach that brings together all of the expertise from the E/CE disciplines under one single functional authority for Commander CJOC. Chapter 4 reviews the mission and role of CJOC with a view to demonstrating that not only is there a task to protect DND/CF's portion of the E/CE, there are underlying implied supporting tasks that could see CJOC supporting other government departments and agencies as part of preventive measures or as post-event consequence management. A review of the DND/CF's current military and non-military actors demonstrates that there are many actors related to the various E/CE disciplines; however, their current roles, mandates or missions and their current organizational structures do not yet directly support CF operations under CJOC. Chapter 5 reviews the approaches taken by the US, NATO and the other three of the Five-Eyes nations, with a view to demonstrating that the CF is indeed on a similar path to its closest allies. Recognizing that the CF's contribution to the E/CE must be interoperable as a troop-contributing nation or as the potential lead nation in a coalition, CJOC should leverage potential lessons by participating in exchanges and/or liaising with such organizations as the NATO Cyber Incident Response Capability, the US Cyber Command or the UK Defence Cyber Operations Group. Finally, Chapter 6 will summarily conclude that the CF needs a single operational commander capable of stewarding EM/Cyber effects on

behalf of Commander CJOC. It will also recommend that there needs to be a similar classified assessment completed before proceeding further. To begin the discussion, the operational commander must first understand the threats confronting them in the E/CE.

CHAPTER 2 – THREATS AND THE ENVIRONMENT DEFINED

Strategically speaking, the CF's assessment is that the security environment is becoming increasingly more complex. In order to be "strategically relevant, operationally responsive, and tactically decisive," this complexity demands a comprehensive, integrated, adaptive, and networked approach to execute national intent.[16] Even with the impending reset of the *Canada First Defense Strategy (CFDS)*, it is unlikely that the CF's three roles will change:

- Defend Canada and Canadians;
- Defend North America; and
- Contribute to International Peace and Security.[17]

In particular, strategic alliances with the US, with NATO and with other multi-lateral security and defence partnerships have significantly enhanced Canada's position around the globe. This enhancement is due to the proliferation of information technology that has permitted virtual collaboration and enabled people and systems to interact. This technology has not only benefitted the CF with a substantial number of shared opportunities such as new concepts and doctrine to ponder, it has also enabled potential adversaries with new means and ways to attack Canada and its allies.[18]

---

[16] Chief of Force Development. A-FD-005-002/AF-001, *Integrated Capstone Concept.* (Winnipeg, MB: 17 Wing Winnipeg Publishing Office, 2009), 2, last accessed 2 April 2013, http://publications.gc.ca/collections/collection_2012/dn-nd/D2-265-2010-eng.pdf.

[17] Government of Canada, *Canada First Defence Strategy . . .*, 7-8.

[18] Angela Gendron and Martin Rudner, *Assessing Cyber Threats To Canadian Infrastructure: Report Prepared For The Canadian Security Intelligence Service* (Ottawa, ON: Canadian Security Intelligence Service, March 2012), 25, last accessed 2 April 2013, http://www.csis-scrs.gc.ca/pblctns/cdmctrch/20121001_ccsnlpprs-eng.asp#a.

Consequently, the CF needs to be cognisant of the multitude of known threats and the emerging trends that are shaping the potential future security environment, particularly in terms of how they will affect future military operations. In particular, the commonality of the threats within the EMS and Cyber environments suggests the need to recognize a single operating environment for the purpose of military operations - herein this chapter defined as the EM/Cyber environment (E/CE). The common threats and the inter-relationships of the E/CE actors also suggest that operational-level military commanders should adopt a coherent and unified approach to understanding the E/CE in order to confront the current threats and anticipate the emerging possibilities within it.

This chapter begins with an unclassified examination of the technologies that used to represent and transport today's information within the E/CE. In addition to improving the conduct of daily operations, these same technologies provide a multitude of ways in which potential adversaries can threaten Canadians and its military forces. The commonality of the threats from foreign military and intelligence agencies, terrorist networks, and criminal organizations suggest that military commanders should take a comprehensive, adaptive, integrated, and networked approach to conduct operations within these environments. A review of the assessed future security environment shows that the challenges within the E/CE will remain common to governments, militaries, and civilian populations alike. Finally, an examination of the contentious "Cyber domain" discussion will demonstrate that there is sufficient convergence and interdependencies between both the EMS and cyberspace that would justify referring to them as one combined E/CE. By recognizing a combined E/CE, the communities of interest and

practice may also be able to recognize their common inter-relationships in conducting the business of supporting the Commander CJOC.

Current Known Threats

Just as communications and information technologies have become essential to the individual Canadian way of life, they are critical to the functioning of the Canadian government and its economy. The DND/CF is equally dependent on the networks of communications and the information systems that connect commanders, staffs, sensors, weapons platforms and operators throughout the battlespace – the collective C4ISR.[19] Together this system of systems promises ubiquitous access to data and information that enhances overall situational awareness, but also has the potential to lead to shared understanding and to promote creativity.[20] However, there are threats to this informational plane. The threats that challenge everyday Canadians, businesses and government, also threaten to affect CF operations.

The proliferation of affordable technology has made it easy for individuals, non-state actors, and less-developed nation-states to acquire the means to exploit the E/CE. Looking solely at commercially available technologies, the sheer quantity of potential attack vectors in the E/CE becomes readily apparent. Point-and-click digital photography and videography, which permit easy editing, transmission, and data storage, also facilitate

[19] "C4ISR" is the collective system of systems encompassing Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance.

[20] Melanie Bernier and Joanne Treurniet. "Understanding Cyber Operations in a Canadian Strategic Context: More Than C4ISR, More Than CNO," in *Conference on Cyber Conflict Proceedings 2010*, edited by C. Czosseck and K. Podins, 227-243 (Tallinn, Estonia: CCD COE Publications, 2010).

propaganda campaigns by distorting images.[21] High-definition compression techniques have made analog television almost obsolete, while both television and radio, traditionally broadcast over radio frequencies (RF), now extend over satellite frequency bands and via Internet Protocols (IP) to computers and personal handheld devices almost everywhere. Through wires (i.e. radio frequency over copper cable, or light transmitted over fibre optics), and wireless radio frequency protocols such as IEEE 802.1X, General Subscriber Mobile (GSM) and satellite links, adversaries have the potential to launch a cyber-based attack from just about anywhere around the globe.[22] Despite being illegal in most countries, it is relatively easily for a potential adversary to procure the hardware to locate and jam military command and control nodes or introduce malicious software into a wireless network.[23] Once considered solely as a proprietary domain, the Internet's "open architecture" has also permitted the creation of many different IP-based technologies embedded in home appliances and used for the remote control of lighting, security alarms, and heating/ventilation and air conditioning controls.[24] In addition to broadening the quantity and variety of IP-based attack targets, the increased quantity of devices has also led to problems with IP addressing protocols.[25] Mobile phones, which

---

[21] Brachman, Jerret and Lianne Kennedy Boudali. *The Islamic Imagery Project: Visual Motifs in Jihadi Internet Propaganda* (West Point, NY: The Combating Terrorist Centre, March 2006), 5-6.

[22] The Institute of Electrical and Electronics Engineers (IEEE) is the recognized global steward for various communications protocols such as 802.11 (WiFi, WiMax, etc). See http://www.ieee.org/index.html. General Subscriber Mobile (GSM) is a band of radio frequencies authorized by the International Telecommunications Union (ITU) for mobile phones. For more on the ITU and international standardization, see http://www.itu.int.

[23] Federal Communications Commission, "GPS, WiFi, and Cell Phone Jammers: Frequently Asked Questions (FAQs)," last accessed 2 April 2013, http://transition.fcc.gov/eb/jammerenforcement/jamfaq.pdf.

[24] Michael Chui, Markus Löffler, and Roger Roberts,"The Internet of Things," last accessed 2 April 2013, http://www.mckinseyquarterly.com/The_Internet_of_Things_2538.

[25] The 4.3 million IPv4 addresses managed by the Internet Assigned Number Authority (IANA) were officially depleted as of November 2011. The American Registry for Internet Numbers (ARIN), who distributes IP addresses for the US, Canada and most of the Caribbean, warned organizations to convert their infrastructure over to IPv6. The new coding provides greater security enhancements which will conflict with existing security protocols

use radio frequencies between the device and the cellular tower, have enabled wireless networks to proliferate throughout the developed and developing worlds. Moreover, the continued convergence of integrated technologies on mobile phones such as digital cameras, full computer processing with a multitude of easy-to-download software applications, and global positioning system (GPS) capabilities, offers a wide array of exploitation methods.[26] Unmarked or misidentified information storage media consisting of electromagnetic technologies such as compact or digital video disks, universal serial bus (USB) and secure digital (SD) cards offer attractive methods of introducing malicious software into networks by unsuspecting users.[27] Meanwhile, civilians and militaries also use the E/CE for various capabilities, including "positioning, navigation, and timing (PNT); sensing; command and control; attack; ranging; data transmission; and information storage and processing."[28] Although the aforementioned is by no means an exhaustive list, the key takeaway is that all of the consumer information technologies that operate within the E/CE are potentially vulnerable to those with malicious intent. More importantly, these aforementioned technologies could permit a potential adversary from attacking anyone and from anywhere around the world where connectivity permits. This makes it very difficult for Canadians, governments and militaries to anticipate potential vectors of attack. Moreover, as will be discussed in Chapter 3, it makes attribution to an attacker extremely difficult.

(firewalls, NAT, IDS, etc). Doug Howard and Kevin Prince, *Security 2020: Reduce Security Risks This Decade* (Indianapolis, IN: Wiley Publishing Inc., 2011), 67-68.

[26] Paul Ruggiero and Jon Foote, "Cyber Threats to Mobile Phones," in Report for the United States Computer Emergency Response Team. (Pittsburgh, PA: Carnegie Mellon University, 2011), 1-3, last accessed 2 April 2013, http://www.us-cert.gov/sites/default/files/publications/cyber_threats-to_mobile_phones.pdf.

[27] BBC News, "US plants hit by USB stick malware attack," 16 January 2013, last accessed 2 April 2013, http://www.bbc.co.uk/news/technology-21042378.

[28] US Department of Defense, JP 3-13.1, *Electronic Warfare* (Washington, DC: Department of Defense, 08 February 2012), I-1 last accessed 2 April 2013, http://info.publicintelligence.net/JCS-EW.pdf.

Not only are commercial systems vulnerable, so too are the systems that are critical to national security and economic prosperity. In essence, Canadian systems operating in the E/CE are an attractive target for potential adversarial militaries, intelligence services, criminals and terrorist groups.[29] Even cyber attackers with basic skills are able to gain access to computer files, deface websites and implant malicious software to crash systems and cause panic.[30] Appendix 2 describes a less-than-exhaustive list of specific cyber-based attack methods and potential adversary types.

Whether it is through phishing or other advanced persistent threats (APTs), adversaries can steal intellectual property, acquire national and industrial secrets, and obtain personal identify information such as banking or credit cards, social insurance numbers, or usernames and passwords.[31] Within the month of April 2012 alone, there was a record high of over 63,000 unique phishing sites detected by the Anti-Phishing Working Group.[32] Daily news testimonies also highlight the lacklustre information security and carelessness that compromises digital infrastructure and information in Canada and around the world. In 2011 and 2012, the Canadian Cyber Incident Response Centre (CCIRC) published 61 alerts, advisories, information notes and technical reports

---

[29] Gendron and Rudner. *Assessing Cyber Threats To Canadian Infrastructure: Report Prepared For The Canadian Security Intelligence Service . . .*, 21-30.

[30] Government of Canada, *Canada's Cyber Security Strategy . . .*, 1.

[31] "Phishing" is the attempt to gain access to an individual's personal details by masquerading as a trusted source, normally through fraudulent emails or websites. The word was added to the Oxford English dictionary in 1996. "Spear phishing" is phishing aimed at specific individuals or organizational entities. Additional cyber attack methods are described at Appendix 2. Peter Coogan, "Using Spam in Targeted Attacks," *Symantec* (blog) last accessed 2 April 2013, http://www.symantec.com/connect/blogs/using-spam-targeted-attacks; and Doug Howard and Kevin Prince, *Security 2020: Reduce Security Risks This Decade . . .*, 81.

[32] Anti-Phishing Working Group, "Phishing Activity Trends Report – 2nd Quarter 2012," last accessed 2 April 2013, http://docs.apwg.org/reports/apwg_trends_report_q2_2012.pdf.

for each year respectively.[33] Provided to the various government departments and industry sectors, the CCIRC reports describe the potential, imminent or actual threats, vulnerabilities or incidents within Canada's critical infrastructure. Consequently, DND/CF has also increased its internal messaging by promulgating security awareness bulletins and reminding users to remain vigilant to these potential threats.[34]

As shown in Figure 2.1, the continuum of national cyber risk varies from the most dangerous involving nation-state actors to the more nuisance variety involving hackers.[35] Due to the financing and labour resources required, the CF's most likely threats are those originating from nation-state foreign intelligence services and/or militaries who seek to gain political, economic, industrial or military advantage.[36] Some states such as Russia, Israel, China, India, France, South Korea and the United States have openly declared that EM/Cyber operations are core to their military strategy, integrated with other military and intelligence operations, to attack their adversary's military equipment and operations.[37] The cyber-attacks conducted against Iran and Georgia are likely indicators of the type of

---

[33] Public Safety Canada. "Cyber Security Publications," last accessed 2 April 2013, http://www.publicsafety.gc.ca/prg/em/ccirc/anre2012-eng.aspx.

[34] Khang Pham, "Cyber Security: Do your part!" *The Maple Leaf* 15, no.2 (February 2012). http://www.forces.gc.ca/site/tml/article-eng.asp?id=1&y=2012&m=02.

[35] Steven Bucci, "Joining Cybercrime and Cyberterrorism: A Likely Scenario," In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World,* ed. by Derek S. Reveron, 57-68 (Washington, D.C.: Georgetown University Press, 2012).

[36] Although the perspectives vary as to which poses the greatest threat, the most sophisticated attacks originate from national intelligence and military actors. Law enforcement agencies and many governments contest that terrorist threats to critical infrastructure likely pose the "most dangerous." Derek S. Reveron, *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World* (Washington, D.C.: Georgetown University Press, 2012), 13-15.

[37] Gvosdev, Nikolas K. "The Bear Goes Digital: Russia and Its Cyber Capabilities," and Nigel Inkster, "China in Cyberspace," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World,* ed. by Derek S. Reveron, 173-189 and 191-205 (Washington, D.C.: Georgetown University Press, 2012); Jamie Yap, "South Korea army, university to start cyberdefense major," last accessed 2 April 2013, http://www.zdnet.com/south-korea-army-university-to-start-cyberdefense-major-2062300991/; CBN News, "Israel Building 'Digital Iron Dome'," last accessed 2 April 2013, http://www.cbn.com/cbnnews/insideisrael/2012/October/Israel-Building-Digital-Iron-Dome/.

activity that is currently available to militaries and intelligence organizations.[38] Terrorist groups are consistently developing their cyber capabilities and doctrines with current activities within cyberspace focused on planning, recruitment, fundraising, and propaganda.[39] A number of groups, including Al-Qaeda and Hezbollah have indicated intentions to launch cyber-attacks against Western states.[40] The next most determined group within cyberspace are criminal organizations. By hiring "cyber mercenaries" these groups usually aim to steal identities, launder funds, extort their adversaries, and steal industrial secrets.[41]

The variety of the threats and the actors has caused much consternation for the Canadian government, particularly as it determines how best to posture to defend itself. As depicted in Figure 2.1, the boundaries often blur between what constitutes as defence missions (cyber warfare, cyber-terrorism) and what is security responsibility for law enforcement (cyber-crime, and online social activism).[42] The Canadian government's *Cyber Security Strategy* defines cyber-attacks in the following manner:

---

[38] The Stuxnet Worm, launched via an infected USB memory stick, is the first known malware that enabled the hijacking of programmable logic controllers at the Bushehr nuclear power plant in Iran. Holly Porteous, *The Stuxnet Worm: Just Another Computer Attack or a Game Changer?* (Ottawa: Library of Parliament, 7 October 2010), 1; As Russian forces attacked Georgian territory in 2008 accompanied by distributed denial of service (DDoS), website defacements and logic bombs against the Georgian Ministry of Defense. Georgia countered with DDoS disruptions to Russian Internet services. Brandon Valeriano and Ryan Maness, "Persistent Enemies and Cyberwar: Rivalry Relations in an Age of Information Warfare," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed.by Derek S. Reveron, 148-150 (Washington, D.C.: Georgetown University Press, 2012).

[39] United States Army Training and Doctrine Command (TRADOC), *Cyber Operations and Cyber Terrorism*, DCSINT Handbook No. 1.02, (Fort Leavenworth, Kansas: Deputy Chief of Staff for Intelligence, 10 August 2006), VI-1 – VI-3, last accessed 2 April 2013, http://www.fas.org/irp/threat/terrorism/sup2.pdf.

[40] Infosecurity Magazine, "RSA 2011: Terrorist groups pose most dangerous cyber threat," last accessed 2 April 2013, http://www.infosecurity-magazine.com/view/16005/rsa-2011-terrorist-groups-pose-most-dangerous-cyber-threat/.

[41] The Economist, "Organized Crime Hackers Are The True Threat To American Infrastructure." March 11, 2013, last accessed 2 April 2013, http://www.businessinsider.com/organized-crime-hackers-are-the-true-threat-to-american-infrastructure-2013-3.

[42] US Army TRADOC, *Cyber Operations and Cyber Terrorism* . . ., VII-1.

Cyber attacks include the unintentional or unauthorized access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information. The severity of the cyber attack determines the appropriate level of response and/or mitigation measures. i.e. cyber security.[43]

The difficulty with such a generalized definition will be in determining which government agency will respond. As the force of last resort, the CF will need the expertise and the resources aligned in order to determine the difference between a hostile attack to the country's sovereignty, what constitutes as cyber reconnaissance or "exploitation," or that which is a crime under the purview of law enforcement agencies.

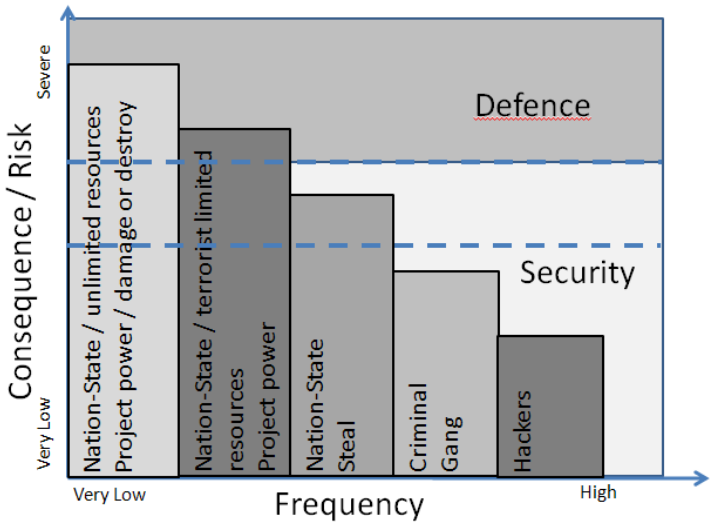


Figure 2.1 – National Cyber Risk Continuum

Source: Adapted from Andrew Cutts, "Warfare and the Continuum of Cyber Risks: A Policy Perspective," 72.[44]

[43] Government of Canada, *Canada's Cyber Security Strategy …,* 3.

[44] Andrew Cutts, "Warfare and the Continuum of Cyber Risks: A Policy Perspective." In *The Virtual Battlefield: Perspectives on Cyber Warfare*, edited by Christian Czosseck and Kenneth Geers, 66-76 (Fairfax, VA: IOS Press Inc., 2009).

The tools provided by technologies in the E/CE enhances Canadian livelihood, the government, and the CF's own operations. In addition to providing information for mutual gain, however, it also exposes Canadians and the CF to foreign military and intelligence agencies, terrorist networks, and criminal organizations that are all willing to exploit potential vulnerabilities. Although these current threats may appear bleak, the assessment of future trends indicates that these threats are likely to continue.

Future Threats

The only certainty about the future operating environment is its uncertainty. To understand the future E/CE issues, one must appreciate that an ever-expanding spectrum of complexity that will be present. Not only will globalization have continued to increase interconnectedness between people, it will have empowered a large number of non-state actors to levels commensurate with nation states, thereby changing the face of potential adversaries.[45] Technologies themselves will continue to evolve, particularly in the E/CE. Although no nation state can claim ownership over the global Internet, some have taken measures to restrict access to it from within their borders.[46] Others on the other hand will continue to extend access through national broadband plans that will expand capacity to more people.[47] Moreover, within an already congested EMS, additional wireless capacity

---

[45] US National Intelligence Council. *Global Trends 2025: A Transformed World* (Washington, DC: Director of National Intelligence, 2008), 84-85.

[46] OpenNet Initiative, "Country Profiles," last accessed 13 March 2013, https://opennet.net/country-profiles.

[47] Most of the Five-Eyes nations have identified individual national broadband plans that will increase the bandwidth capacity to the majority of their populations. For the US example, see US Federal Communications

demands from the telecommunications industry will also continue to impinge on the governments' reserved frequencies.[48] As the future becomes significantly more dynamic and uncertain, the CF must ensure that it is ready to respond to emerging threats and challenges. First, let us examine the general trends evident in the future security environment before looking at the issues more specifically.

General Trends

Looking first at the nature of future conflict, globalization will certainly intensify the trans-border movement of goods, people, technology, culture, crime and weapons, in addition to compressing traditional notions of time and space to instantaneous necessity. This will also continue to ensure that events in one part of the world will cause repercussions elsewhere. Although asymmetric attacks are the principal threat today, the potential for state-on-state conflict remains. Likewise, conflict is most likely to occur in failed or fragile states as they try to assert or re-assert power. Consequently, the DND/CF needs to be prepared to respond across the full continuum of conflict and do so in multilateral cooperation of "coalitions of the willing" over traditional NATO or UN alliances.[49] Particular anarchy in one country could create opportunity for extremists to

---

Commission, *Connecting America: The National Broadband Plan* (n.p., March 2010), last accessed 25 February 2013. http://www.broadband.gov/download-plan/.

[48] As an example, the previously reserved 700MHz block of frequencies is being solicited for auction by Industry Canada in order to increase competition and improve capacity in the mobile communications market. Industry Canada, *Policy and Technical Framework: Mobile Broadband Services (MBS) — 700 MHz Band, Broadband Radio Service (BRS) — 2500 MHz Band*. (Ottawa, ON: Industry Canada, March 2012), last accessed 2 April 2013, http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf10121.html#pA4.

[49] Chief of Force Development, *The Future Security Environment 2008-2030 – Part 1: Current and Emerging Trends* (Ottawa: Department of National Defence, 27 January 2009), 7 and 46, last accessed 2 April 2013, http://www.cfd-cdf.forces.gc.ca/documents/CFD%20FSE/Signed_Eng_FSE_10Jul09_eng.pdf.

operate from safe havens, thus making attribution of attacks more difficult as non-state actors hide amongst populations. Intensified globalization will also continue to provide these individuals and organizations with "off-the-shelf technology including global telecommunications, global positioning, information, intelligence, cryptography, imagery, and weapons"[50] In essence this could put adversaries on a relatively equal footing with Western state militaries and alliances such as NORAD and NATO. [51] This latter prospect has garnered much attention amongst alliance members who contemplate passive and active defence capabilities and proposals to pre-delegate authorities to the Secretary-General and/or NATO military leaders to respond during a cyber-attack.[52] Among many uncertainties associated with forecasting the future, NATO experts concede that the "world's increased reliance on potentially vulnerable information systems" could invoke action or reaction within the E/CE.[53]

Other scientific and technological developments in automation, customization and miniaturization will provide breakthroughs benefiting defence and security. The CF's assessment of the future security environment includes key developments in nanotechnology, micro-electromechanical systems, computing and networking, sensors, biotechnology and new energy/power technologies.[54] Developing applications in ultra-strong and ultra-light materials, new power sources, advanced non-lethal weapons and artificial intelligence each could potentially shock the existing E/CE. Finally, through the

---

[50] Chief of Force Development. *Integrated Capstone Concept . . .*, 21.

[51] North Atlantic Treaty Organization. *NATO 2020: Assured Security; Dynamic Engagement - Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO*, (Brussels: NATO Public Diplomacy Division, 17 May 2010), 14 and 45, last accessed 24 January 2013, http://www.nato.int/nato_static/assets/pdf/pdf_2010_05/20100517_100517_expertsreport.pdf.

[52] *Ibid*., 35.

[53] *Ibid*., 13.

[54] Chief of Force Development, *The Future Security Environment 2008-2030 – Part 1. . ., 71.*

continued commercialization of Space, many of the advanced satellite-based technologies such as GPS, imaging and communications will be available to adversaries for their own use, and alternatively as a means for denial, disruption or destruction.[55] As the NATO Experts Group concluded, "The most destructive periods of history tend to be those when the means of aggression have gained the upper hand in the art of waging war."[56] Therefore, the military must remain proactive and innovative in these areas, especially in terms of reviewing policies and regulating their application, particularly in reducing adversary access to these technologies.

Cyber-specific Trends

NATO's assessment of the future involves probable unconventional threats in the coming decade: a ballistic missile attack, international terrorist group attacks, and cyber-attacks.[57] For the Alliance, these cyber-attacks could come in the form of a full state cyber-attack such as witnessed in Estonia or Iran, or together in conjunction with kinetic assaults as was demonstrated by Russia against Georgia in 2008, or that demonstrated by

[55] *Ibid.*, 85-86.
[56] NATO. *NATO 2020: Assured Security; Dynamic Engagement . . .*, 15.

[57] *Ibid.*, 17.

Israel against Syria in 2007.[58] Nonetheless, the resource gap behind a state-sponsored attack and that available to current non-state actors appears to be closing.[59]

In addition to the continued progression of chipsets and memory under Moore's Law, the physical size of technology should shrink, thus providing new opportunities for applications within defence and security in the form of unattended sensors, robotics, mini-satellites, autonomous networks, smart weapons and military platforms, language translators, biometric technologies, and more seamless command and control.[60] Therefore, militaries and their adversaries should be able to acquire smaller, more portable devices that will converge with other sensors. However, this increase in E/CE footprint will provide even more information rich targets for any adversary to exploit.

Due to the anonymity and low risk of personal injury, adversaries are most likely to continue to target critical infrastructure, power distribution systems, banking, and other targets of political and economic consequence via cyberspace.[61] In addition, cyber-attacks conducted by these adversaries will continue to dominate the public media, inspiring others to copycat and continue the spiral development cycle to create attacks that are

---

[58] Erich Follath and Holger Stark, "The Story of 'Operation Orchard': How Israel Destroyed Syria's Al Kibar Nuclear Reactor," last modified 2 November 2009, http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html; and John Leyden, "Israel suspected of 'hacking' Syrian air defences," last modified 4 October 2007, http://www.theregister.co.uk/2007/10/04/radar_hack_raid/.

[59] Steven Bucci, "Joining Cybercrime and Cyberterrorism: A Likely Scenario," In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World,* Ed.by Derek S. Reveron (Washington, D.C.: Georgetown University Press, 2012), 59-60.

[60] Chief of Force Development, *The Future Security Environment 2008-2030 – Part 1. . .,* 73.

[61] The cyber hacktivist group, Anonymous, launched 'Op Israel' in 2012 as a direct political statement. RT, "Erase Israel from the Internet': Anonymous plots massive cyber-attack," last accessed 2 April 2013, http://rt.com/news/anonymous-cyber-attack-israel-241/.

more dangerous.[62] With the expanding reach of modern media, it is likely that these actors will also employ public relations specialists to ensure that their message reaches a global audience.[63] Looking at the intended effects of cyber-attacks, these future effects will continue to fall into the following four categories:

- Loss of Integrity – unauthorized changes to the data or system itself; could lead to inaccuracy, fraud, or erroneous decisions; examples include web defacement and data corruption;
- Loss of Availability – inability of end-users to complete their mission using the system; loss of productive time, thus impeding the end users' performance;
- Loss of Confidentiality – unauthorized disclosure of information; could impact national security or personal privacy; and
- Physical Destruction – physical harm or destruction by using the system; examples include critical infrastructure supervisory control and data acquisition (SCADA) and industry control systems (ICS).[64]

Despite the significant level of ongoing disruptions, there are some considerable philosophical and operational considerations, as will be discussed Chapter 3, that need to be resolved for the CF to be engaged based on attacks originating in the E/CE. In addition to the above cyber-specific trends, the EMS presents some unique challenges for the future.

EMS–specific Trends

The overarching consensus at a 2010 Centre for Strategic and International Studies discussion held specifically on EMS-related concerns was that is time for consideration of the threats posed within and to the EMS to transition from a military to a

[62] Attack against a Saudi oil company is presumed to be the result of a copycat hacktivist group. InformationWeek, "Shamoon Malware Might Be Flame Copycat," last accessed 2 April 2013, http://www.informationweek.com/security/attacks/shamoon-malware-might-be-flame-copycat/240006014.

[63] NATO. *NATO 2020: Assured Security; Dynamic Engagement . . .*, 14.

[64] US Army TRADOC, *Cyber Operations and Cyber Terrorism . . .*, VII-3 to VII-4.

national issue.[65] Brigadier-General Kevin McLaughlin, Deputy J3 of US Strategic Command, opined that just as commanders had failed to appreciate the complexities of cyberspace, they are on the same path with the EMS, as they expect that it will be immediately available for their use in a new theatre of operations. Rather, as US Cyber Command's J3 Technical Director, Donald Boain, emphasized at the same forum is that militaries must fight for and defend their ability operate in theatre of operations where the EMS is degraded or denied.

The EMS environment faces challenges not only from foreign and domestic adversaries, but also from its shrinking availability. Although this may be nothing new to EMS specialists, it is of increasing concern to governments, law enforcement, and military commanders as they become aware of new challenges confronting commercial industry's and the military's use of the EMS at home and abroad. For instance, the US Department of Homeland Security (DHS), which deals with EMS-related security issues, indicates that there is an increasing domestic threat to domestic wind turbines, to electronic sensors employed along the border, and from electromagnetic pulse (EMP) capabilities to name several examples.[66] Another disturbing trend is the purchase of major wireless entities by European companies and the movement of wireless development to Europe and China.[67] Moreover, the foreign manufacture and assembly of

---

[65] David Sokolow, and Maren Leed, *Seizing the Wireless Advantage: Addressing an Increasingly Congested and Contested Electro-Magnetic Spectrum* (Washington, DC: Center for Strategic and International Studies, October 2010), 2, http://csis.org/files/publication/101018_seizing_wireless_advantage_final2.pdf.

[66] *Ibid.*, 2-3.

[67] A trend indicated by Dr. Vanu Bose, President and CEO of Vanu Inc. and Dr. Andrew Clegg, Director of the National Science Foundation's Enhancing Access to the Radio Spectrum program. Dr. Bose also indicated that India had discovered Chinese equipment that contained trap doors, and had subsequently banned Chinese telecommunications equipment from entering its borders. As cited in Sokolow and Leed, *Seizing the Wireless Advantage* . . ., 7, 11.

chipsets and wireless devices, such as the Apple iPhone in China, raises concerns for national security interests.[68] For spectrum regulators around the world, the increased EMS demand creates an economic challenge as they try to balance spectrum supply and demand.[69] The increasing move towards wireless networks has increased EMS demands, particularly in urban areas, and current processes take between 6-13 years to redistribute spectrum for approved use.[70] This will severely hamper broadband networks that are facing exponential growth in data use over voice service use, in addition to exponential growth in cellular subscriptions from approximate 5 billion in 2010 to 50 billion by 2020.[71] To keep their own military advantage in the EMS, US Department of Defense (DoD) advisors opine that new systems need to reduce fielding to months vice years, and that engineering efforts must develop more agile and adaptive open-systems architectures that can integrate commercial off-the-shelf capabilities.[72] Moreover, despite best efforts to leverage the "digital dividend" of converting old analog television "over the air" broadcast channels to digital terrestrial broadcasting, there remains insufficient spectrum for users around the world.[73] Although commercial industry complains that they have been unable to acquire spectrum successfully through the cumbersome government

---

[68] Sally Adee, "Hunt for the Kill Switch," *IEEE Spectrum* (May 2008): 34-39, http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch.

[69] International Telecommunications Union, *Exploring the Value and Economic Valuation of Spectrum: Broadband Series* (Geneva, Switzerland: International Telecommunication Union, April 2012), 2, last accessed 2 April 2013, http://www.itu.int/ITU-D/treg/broadband/ITU-BB-Reports_SpectrumValue.pdf.

[70] Blair Levin, a previous Executive Director to the US National Broadband Plan (NBP) as cited in Sokolow and Leed, *Seizing the Wireless Advantage . . .*, 3.

[71] Dr. Ali Khayrallah, the Director of Research at Ericsson, as cited in Sokolow and Leed, *Seizing the Wireless Advantage . . .*, 7.

[72] *Ibid*., 3-4.

[73] For the 119 member countries of the International Telecommunication Union – Radiocommunication GE06 Agreement, the cut-off date for the rights to use analog transmissions has been set as 17 June 2015 in the UHF band. The same date applies in the VHF band, with an extension to 17 June 2020 for a number of developing countries. See International Telecommunications Union, *Digital Dividend: Insights for Spectrum Decisions* (Geneva, Switzerland: International Telecommunication Union, August 2012), 1, last accessed 2 April 2013, http://www.itu.int/ITU-D/tech/digital_broadcasting/Reports/DigitalDividend.pdf.

processes, it appears that security and defense interests have the most to lose if spectrum is not available for their own use.[74]

Defining the EMS/Cyber Operating Environment

In 2009, the CF's Chief of Force Development (CFD) followed the US lead and proposed "cyber" as a new domain for the CF, in addition to "space" and "human" as part of its *Integrated Capstone Concept (ICC).*[75] The *ICC* implies that a "domain" is where military forces and adversaries can "exercise power and influence."[76] However, this only leaves the proposal fraught with controversy as the multitude of communities of interest fight for finite resources. Furthermore, the EMS has been a distinct operating environment ever since Guglielmo Marconi demonstrated its first use for wireless communications in 1895, although the *ICC* does not refer to it whatsoever. Fundamental to EMS practitioners, such as EW and cyber network operators, this naturally occurring physical environment is critical to military operations, and will remain so for the foreseeable future. Although the resolution of the "domain" versus "environment" debate is beyond the scope of this paper, it is essential that an operational military commander identify how they interpret the operating environments as they employ the capabilities delivered by force developers and force generators. There are sufficient unifying common elements between the EMS and the cyber operating environments to warrant a single

[74] FCC is the Federal Communications Commission, the US regulator for spectrum use. Sokolow and Leed, *Seizing the Wireless Advantage . . .*, 13.

[75] William J. Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (September/October 2010): 97-108, http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain; and Chief of Force Development. A-FD-005-002/AF-001. *Integrated Capstone Concept.* (Winnipeg, MB: 17 Wing Winnipeg Publishing Office, 2009), 28, http://publications.gc.ca/collections/collection_2012/dn-nd/D2-265-2010-eng.pdf.

[76] Chief of Force Development. A-FD-005-002/AF-001. *Integrated Capstone Concept. . .*, 28.

distinct operating environment – such as the EMS/Cyber Environment (E/CE) proposed here – in order to unify CF effort.

With recognition as an "environment" comes the responsibility by the related force development and force generator community to build capabilities by considering the associated PRICIE+G elements.[77] For force capability developers, any new distinctive additions to the traditional environments of land, air, space, and maritime must consider the tangible requirements of unique equipment, skill sets and training that differentiate operations within each.[78] For "Cyber," responsibility for "joint" force development is currently with Director-General Cyber (DG Cyber), under CFD. Meanwhile the RCN, CA, and RCAF have each kept the legacy responsibility for development of EMS capabilities within their respective organizations. With no strategic level or "joint" force developer responsible for the EMS, Commander CJOC is left to integrate the tactical EMS capabilities into the required "joint" force. Chapter 4 discusses this further in addition to describing in detail the organizations making up the DND/CF communities of practice in the E/CE.

While each of the newly proposed *ICC* "domains" transpose relatively well as "operational environments" for the purpose of military operations, it is not entirely evident what is included in "Cyber." Consider the Oxford English Dictionary definition of "environment" as "the setting or conditions in which a particular activity is carried

---

[77] CF capability development requires review of PRICIE+G components: People and Leadership; Research and Development and Operational Research, (plus Experimentation); Infrastructure, Environment, and Organization, Concepts and Doctrine; Information Management and Technology; Equipment and Support; and Generate.

[78] This "unique technology" requirement was offered by Mr. Regan Reshke, Chief of Staff Land Strategy Science Advisor, during Directorate of Land Concepts and Designs discussions in March 2010. As cited in Jim Gash, "Physical Operating Environments: How the Cyber-Electromagnetic Environment Fits," *Canadian Military Journal* 12, no. 3 (Summer 2012): 28.

on."[79] The physicality of the words "setting" and "conditions" would lead to the conclusion that land, air, maritime, space and EMS would best fit this description. However, as these words could equally apply to the "virtual" aspects of the information plane, some have offered the use of "cybered" as a modifier to describe all aspects of conflict or activity within cyberspace and the EMS – i.e. "cybered conflict."[80] The *ICC* refers to the "cyberspace domain" in the following manner:

> The cyberspace domain will be a mechanism for integrating all of the environmental domains at the strategic level resulting in one common operational picture of the mission environment. This functionality will be complemented by the facility of the cyberspace environmental domain to merge the strategic functional domains, producing integrated effects. Cyberspace may also be where the medium and the message are virtually inseparable.[81]

The final sentence implies that the technical and the social elements are intertwined. However, this is where current CF capabilities diverge in their approach to the E/CE. Information Operations specialists and Public Affairs experts use the E/CE to "virtually" access their intended audience for the purposes of influencing an adversary – their focus is the "message." For the technical E/CE disciplines (as will be described in Chapter 3 and 4) that create the networks, safeguard the EMS from adversarial threats, or exploit the infrastructure for the purposes of gathering or aiding information operations, the focus is on the physical "medium." To confuse this further, there is no clear consensus amongst the technical experts on whether the EMS subsumes the technical "Cyber" side or vice versa. As technologies in both continue to "converge", it is possible the EM

---

[79] See "Environment" - http://oxforddictionaries.com/definition/american_english/environment.

[80] Chris Demchak, "Cybered Conflict, Cyber Power, and Security Resilience as Strategy," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World,* ed.by Derek S. Reveron, 121-136, Washington, D.C.: Georgetown University Press, 2012).

[81] Chief of Force Development. A-FD-005-002/AF-001. *Integrated Capstone Concept. . .,* 30.

environment could subsume or become "wholly synonymous with the cyber environment."[82] This paper will continue to use the term E/CE as referring to the technical operating environments that encompasses the EMS and the physical hardware, software, infrastructure and embedded processors used for communications and information processing. For Commander CJOC, the recognition of this single distinct operating environment will help unify CF efforts at the operational level.

Chapter Summary

In addition to improving the conduct of daily operations, the inexpensive commercially available technologies of the E/CE also provide a multitude of ways for potential adversaries to threaten Canadians and its military forces. With the ability to launch an attack from anywhere around the world, it is extremely difficult for Canadians, the government, and the CF to prepare against threats from stealing personal information to destroying critical infrastructure. Based on the continuum of national cyber risk varying from the most dangerous involving nation-state foreign military and intelligence agencies, to transnational terrorist networks and criminal organizations, to individual hackers, it is suggested that Commander CJOC will need to take a comprehensive, integrated, adaptive, and networked approach to the E/CE that leverages all available capability.

---

[82] Jim Gash defines the "EM environment" as including electronic devices and their components (both hardware and software), the physical hardware and infrastructure connecting electronic devices, and the spectrum of electromagnetic energy itself, including all forms of radiation and EM particles – both elementary and atomic. Jim Gash, "Physical Operating Environments: How the Cyber-Electromagnetic Environment Fits," *Canadian Military Journal* 12, no. 3 (Summer 2012): 28.

Looking at the future, emerging trends indicate a greater complexity in terms of the quantity and quality of the various actors. Technological advances in miniaturization, automation, and customization, will vastly improve cyber and EM capabilities that will benefit both consumer and as well as potential adversaries. Future cyber-attacks are amongst the most likely methods of attack envisioned by NATO with effects involving one or a combination of loss of availability, loss of integrity, loss of confidentiality, and physical destruction. Trends also indicate that the issues related to the congested EMS will rise to a national level of significance on par with the buzz of "cyber." As the demand for spectrum continues to rise exponentially, regulators and innovators will be significantly challenged to find alternative methods of supply.

Finally, a joint "EM/Cyber environment" (E/CE) was proposed to recognize the convergence of technologies between both the EMS and the technical aspects of the "Cyber domain." By recognizing the E/CE in this manner, it should unify the focus of the force developers and force generators towards better support for the CF's principal force employer, Commander CJOC, to confront the multitude of presented threats.

CHAPTER 3 –
CONSIDERATIONS IN THE EMS/CYBER OPERATING ENVIRONMENT

Military officers undergo varying degrees of military socialization and indoctrination, professional training and advanced education. Depending on their chosen occupation, most begin their careers as specialists and as they advance up the career ladder, they tend to become generalists. Having become tactical specialists and commanders within the RCN, CA and RCAF, these senior officers have specific professional paradigms in how they approach the overall operating environment. Despite becoming generalists, they are equally capable of developing and mentoring junior members in tactical lessons and imparting their own experiences onto younger generations.

The same cannot be said for the E/CE. This is not to say that all of today's "generalist" commanders are E/CE neophytes. It just means that they may have more to learn regarding this specific operating environment. To do this, they will need to look to subject matter experts in CIS, CNO, EW, and SIGINT to help advise them on the environment's specific considerations and to coordinate and execute operations within it. For Commander CJOC, an appreciation of the E/CE also requires understanding the operational considerations in both the domestic and the continental context due to the actors involved. As a very complex environment, with very real threats (as discussed in the previous chapter), the E/CE requires a multi-disciplinary organization to advise Commander CJOC and to handle the multitude of unique operational level considerations that are inherent to it.

This chapter begins with a review of the "operational functions" used in military planning as they pertain to the E/CE. The importance of the E/CE to these "operational functions" demonstrates that it requires a dedicated organization to focus more attention it than what it currently gets. At this point, a review of the mutually supporting nature of the current E/CE disciplines will determine their relevance to a collective subordinate organization under Commander CJOC. The final section of this chapter will recommend that a new subordinate E/CE-focussed organization will need legal expertise and other experts to prepare collectively for the unique legal and other operational considerations of interoperability and use of force in the E/CE.

The Operational Functions and the E/CE

Today's CF commanders use the operational art to "[employ] forces to attain strategic and/or operational objectives through the design, organization, integration, and conduct of strategies, campaigns, major operations and battles."[83] To do this CF commanders and military planners break down the planning and execution of operations into the constitute parts known as the "operational functions" of Command, Sense, Act, Shield, and Sustain – as illustrated in Figure 3.1 and defined at Appendix 3.[84] As recognized in Chapter 2, the E/CE is distinct from the other physical environments (land, air, space, and sea), but at the same time the E/CE is vital in coordinating the tactical-level activities within them.[85] From an operational-level perspective, the E/CE is vital to each of these "operational functions" due to the information transmitted through or stored

---

[83] Chief of Force Development. A-FD-005-002/AF-001. *Integrated Capstone Concept . . .*, 39.

[84] Canadian Forces Warfare Centre. B-GJ-005-000/FP-001 *CFJP-01 - Canadian Military Doctrine*. Ottawa: DND, 2011), 2-7; and Chief of Force Development, B-GJ-005-500/FP-000, *CFJP 5.0 – The Canadian Forces Operational Planning Process (OPP), Change 2* (Ottawa: DND, 2008), 2-8 to 2-9.

[85] Chapter 4 describes the occupations and organizations that permit this function.

within it. The "operational function" of Command normally incorporates the E/CE.[86] The interrelationship of the "functions" around Command, as depicted in Figure 3.1, implies that it is absolutely critical for Commander CJOC to organize resources to not only extend the E/CE, but also to ensure its constant availability.[87] This interrelationship between the "functions" also implies that E/CE has at least two reciprocal considerations for each. Firstly, the E/CE enables the "function" by transmitting and storing vital information. Secondly, and what is more important here, is where the "function" enables the E/CE and activities within it. The complexity of these latter considerations should justify the creation of a dedicated subordinate organization under CJOC. Let us now examine these latter considerations for each "function."

Figure 3.1 – Inter-relationships of the Operational Functions

Source: Directorate of Land Concepts and Design, *Land Operations 2021*, 13.[88]

[86] The operational function "Command" (command and control) manifests itself in the commander, the headquarters staff, and an organization that provides the communications and information systems (i.e. a Signals unit) to allow command and control. Canadian Forces Warfare Centre. B-GJ-005-300/FP-001, *CFJP 3.0 – Joint Operations* (Ottawa: DND, 2011), 3-5.

[87] Other than the CF Joint Signal Regiment under the CJOC's CF Joint Operational Support Group (CFJOSG), which provides deployed extension of communications and information systems (CIS), there is no single organization under CJOC that is dedicated to E/CE provision and protection. See Chapter 4 for more details.

[88] Directorate of Land Concepts and Design. *Land Operations 2021: Adaptive Dispersed Operations: The Force Employment Concept for Canada's Army of Tomorrow* (Kingston, ON: Department of National Defence, 2007), 13.

As described above, most effort in the E/CE is to enable Command (and the other "functions") by providing the systems for virtual collaboration, shared situational awareness, but ultimately for the instantaneous and uninterrupted delivery of the commander's intent to an entire operational force.[89] Reciprocally, the Command function involves commanders that understand their environment, provide focus, assign priority of effort, and guide the solution of problems as they arise.[90] This requires a significant degree of training and experience, and the authority to make decisions quickly with a full understanding of known risks and consequences.[91] Although the J6 staff in a headquarters normally fulfills the staff role for planning and controlling purposes (on behalf a commander), it is tactical level entities that exercise the actual command authority to execute and operations in the E/CE. Chapter 4 elaborates how there are no standing operational-level entities that command the collective E/CE activities on behalf of Commander CJOC.

The Sense function requires a robust and secure E/CE enables to fuse the information from a variety of Intelligence, Surveillance and Reconnaissance (ISR) sensor apertures and transmit information to a multitude of decision-makers, operators, and intelligence analysts.[92] Conversely, the Sense function implies the planning and coordination of sensors and intelligence assets specifically for monitoring the E/CE

---

[89] Although "Command" is the name of the "operational function," the more commonly used terminology would be "Command and Control." Staff collaboration and situational awareness, as performed by the staff, are part of the "control" elements done on behalf of a commander. Canadian Forces Warfare Centre. B-GJ-005-300/FP-001. *CFJP 3.0 – Joint Operations . . .*, 1-5.

[90] Chief of Force Development. *Integrated Capstone Concept. . . .*, 40.

[91] Pigeau and McCann refer to a "competency" dimension developed through a commander's development. Ross Pigeau and Carol McCann, "Re-conceptualizing Command and Control," *Canadian Military Journal* 3, no. 1 (2002): 58.

[92] Canadian Forces Warfare Centre, B-GJ-005-200/FP-001. *CFJP 2-0 – Joint Intelligence* (Ottawa: Department of National Defence, 2011), 5-4.

against threats.[93] To be most responsive, the E/CE-specific "sensing" equipment (hardware and software) and the operators should be part of the organization they are supporting. This is not currently the case for CJOC.

As previously indicated, the E/CE provides the medium in which the majority of Act activities in the land, air, and maritime domains are planned and controlled. Conversely, Information Operations (IO) conducted within the E/CE will seek to attain "information dominance" on the informational plane, and will often conduct specific E/CE-related Act activities to deliver the majority of the requested effects.[94] However, before they are able to exploit the information within, they must "act" to acquire the necessary freedom of manoeuvre within the E/CE.[95] When authorized by rules of engagement, EW, CNO and SIGINT can conduct the full continuum of defensive, exploitative, and offensive actions. Currently, these disciplines independently plan and execute their own operations without any operational-level integration of effects.[96]

As discussed in Chapter 2, the Shield function must consider some unique and complex threats in the E/CE, and therefore the E/CE factors heavily into the operational commander's force protection plan. As much of the military E/CE intertwines with the civilian E/CE, a multilayered Shield function integrates CF force protection with effort

---

[93] These E/CE-specific sensors would include specialized hardware and software (such as intrusion detection systems, spectrum scanners, etc.) and the operators to analyze and react accordingly.

[94] Information Operations (IO) are actions taken in support of national objectives which influence decision makers by affecting other's information while exploiting and protecting one's own information. IO will employ electronic warfare (EW), intelligence, computer network attack (CNA), in addition to other IO disciplines psychological operations (PSYOPs), deception (OPDEC), and special information operations (SIO). DND, B-GG-005-004/AF-010. *CF Information Operations* . . ., 1-2.

[95] While commanders may demand "dominance" of the E/CE some experts contest that it is more likely based on the resources available to expect a lesser "control." Association of Old Crows, "A (Pragmatic) Future for Joint Electronic Warfare: Does EW + CNO = Cyber?". . ., 34.

[96] Discussed in greater detail at Chapter 4.

from other government departments, industry and allies.[97] Normally, soft procedural Shield measures reinforce the technological security measures.[98] Moreover, Shield effects from various E/CE capabilities can protect ship and aircraft platforms from physical threats, in addition to land vehicles and individuals from threats such as remote-controlled improvised explosive devices.[99] This requires that CIS, CNO, EW and SIGINT disciplines must work together in order to mitigate the risk to their portion of the E/CE as well as protect the physical forces using their unique capabilities.

Finally, the E/CE enables the Sustain function, and reciprocally needs to be sustained. At the operational level, the Sustain has only considered CIS capabilities as part of the initial activation of a theatre of operations in order to establish host nation liaison and build or extend necessary telecommunications infrastructure for a deploying force.[100] By neglecting the other E/CE disciplines until later deployment stages, operations in the E/CE are considerably disadvantaged.[101] Conversely, due to the rapid change in technologies, the E/CE requires the Sustain function to responsively and efficiently acquire, repair or replace hardware/software components when required. The

---

[97] To overcome this reliance on civilian telecommunications, the CF is acquiring its own dedicated military controlled satellite links with the delivery of three DG Space projects (Protected Military SATCOM, Mercury Global Wideband SATCOM, and Tactical Narrowband SATCOM). DND, "DND/CF Space Operations: To The Future and Beyond," *The Maple Leaf* 15, Issue 5 (May 2012): 8-9, last accessed 2 April 2013, http://www.forces.gc.ca/site/tml/article-eng.asp?id=1&y=2012&m=05.

[98] IT Security (ITSEC) encompasses the sub-set of Emissions Security, Computer security, Cryptographic Security, Transmission Security and Network Security. CF Provost Marshall, "Information Systems (IS) Security," Chapter 70 in A-SJ-100-001/AS-000. National Defence Security Instructions (Ottawa: DND, 1999), 3-4.

[99] For example, various vehicle and portable Counter Remote Control-Improvised Explosive Device (RC-IED) capabilities have been developed and employed in theatres for force protection purposes. Glenn Goodman, "Dismounted Counter-IED: Size, Weight and Power Limits," *Soldier Mod* 2 (January 2009): 38-39. http://soldiermod.com/volume-2/pdfs/articles/dismounted-jamming.pdf.

[100] John Nethercott, "Op ATTENTION Theatre Activation Team Puts It All Together — Literally," last accessed 2 April 2013, http://www.afghanistan.gc.ca/canada-afghanistan/stories-reportages/2011_06_07.aspx?lang=eng&view=d.

[101] Deploying EW, CNO and/or SIGINT resources at later stages is satisfactory in a permissive or already mature theatre with other coalition nations on the ground. However, it significantly disadvantages the deploying CF force if it is deploying into a theatre without these E/CE disciplines.

discovery of counterfeit electronic components onboard CC-130J Hercules aircraft demonstrates that the security of the supply chain for E/CE technologies warrants considerable attention to avoid impact to operations.[102] With a collective organization involved in the operational-level E/CE, these Sustain functions can acquire more focus.

Not only does the E/CE influence upon all the various operational functions, they reciprocally influence it. The common denominator from this review of the "operational functions" is that Commander CJOC would benefit from a dedicated organization that can continuously consider these "operational functions" in the planning and execution of CJOC operations in the E/CE.

The Mutually Supporting Disciplines in the E/CE

Now that we have examined the E/CE in terms of its generic threats and the "operational function" considerations that are vital to military planning, it is important to review the relative E/CE disciplines in order to determine how they might mutually contribute to collective subordinate organization under CJOC. Appendix 3 shows how each of the disciplines relates to a single or to multiple "operational functions." However, it also shows that none of the disciplines individually covers all of the "functions" that are deemed vital to operations in the E/CE.

[102] Greg Weston, "Fake parts in Hercules aircraft called a genuine risk." (CBC News, 9 January 2013), last accessed on 2 April 2013, http://www.cbc.ca/news/canada/story/2013/01/09/f-vp-weston-hercules-counterfeit-chinese-parts.html.

Once described only as a subset of IO doctrine, CNO has since gained prominence as its own discipline deserving of its own doctrine.[103] Encompassing the trifecta of computer network attack (CNA), computer network defence (CND) and computer network exploitation (CNE) depicted in Figure 3.2, CNO includes actions to confront threats to the E/CE, less activities conducted explicitly by EW assets.[104] CND involves passive surveillance, active monitoring and reacting to threats to maintain the integrity of the computer network and their underlying infrastructure.[105] The offensive nature of both CNA and CNE, are particularly significant due to the advanced education and training and the considerable legal and policy aspects that govern these areas.[106]As shown in figure 3.2, CNE could include pursuing an adversary who is manipulating friendly information networks in order to determine their location, or to probe an adversary's defences prior to conducting CNA. CNA goes beyond CNE by causing an effect against an adversary's own network, systems, or information found within. When authorized, CNA could go so far as to degrade or destroy the adversary's own network or

[103] CNO used to be described as C2W within IO doctrine. Within current US joint doctrine "computer network operations" has been replaced by "cyberspace operations." US JP 3-12, *Cyberspace Operations* (classified) was recently published. Status last modified 29 March 2013, http://www.dtic.mil/doctrine/doctrine/status.pdf.

[104] There is no unclassified CNO policy or doctrine. The only reference to CNO is in IO doctrine. CNO elements of CND, CNE and CNE are reflected in CF School of Communications and Electronics, *Transforming the Network Fight: Unique Skills, Unique Tactics, Unique Effects – CFSCE Campaign Plan* (Kingston: CFSCE Publication Development, 27 June 2008), 17.

[105] "CND focuses on managing the vulnerabilities and risk that are inherent in all computer networks." Luc Beaudoin, Michael Froh, Marc Gregoire, and Julie Lefebvre, "Computer Network Defence Situational Awareness Information Requirements," last accessed on 2 April 2013, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4086552.

[106] CNE is a form of active reconnaissance that goes beyond the confines of the outer defenses to extract information from an adversary without their knowing. Advanced training in CNO focuses on privacy laws and other SIGINT-type policies that are overseen by Communications Security Establishment Canada (CSEC). Discussed further in Chapter 4.

the connected systems.[107] Due to their complementary activities in the E/CE, there is increasing recognition to leverage synergies between CNO and EW.[108]

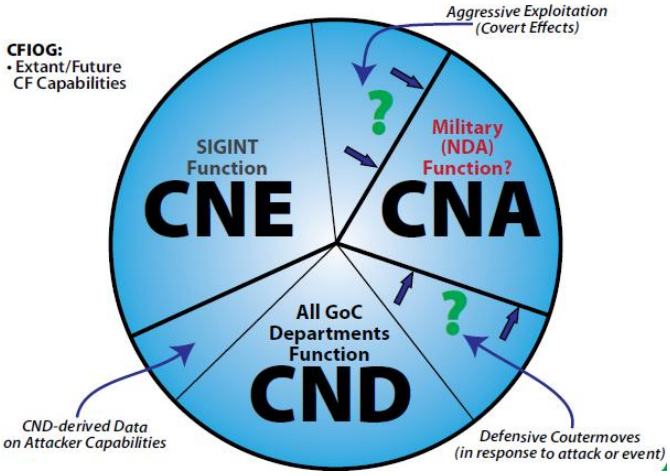


Figure 3.2 – Components of Computer Network Operations

Source: CF School of Communications and Electronics, *Transforming the Network Fight: Unique Skills, Unique Tactics, Unique Effects – CFSCE Campaign Plan*, 17.

EW is "a military action involving the use of electromagnetic [EM] energy and directed energy to control the EMS or to attack the enemy."[109] Shown at Figure 3.3, it consists of three sub-components: and electronic warfare support (ES), electronic attack (EA), and electronic protection (EP).[110] ES involves actions to search for, intercept,

---

[107] The Stuxnet Worm is the most common example that demonstrates the destruction capacity of CNA. Gary D. Brown, "Why Iran Didn't Admit Stuxnet Was an Attack," *Joint Forces Quarterly* 63 (4th Quarter 2011): 70-73.

[108] Zachary Friar-Biggs, "DoD Looking to 'Jump the Gap' Into Adversaries' Closed Networks," last accessed 19 March 2013, http://www.defensenews.com/apps/pbcs.dll/article?AID=2013301150010; and Zachary Fryer-Biggs, "Navy Looking to Use EW as Part of Cyber," last accessed 19 March 2013, http://blogs.defensenews.com/intercepts/2013/03/navy-looking-to-use-ew-as-part-of-cyber/.; and Ron Smith and Scott Knight, "Applying Electronic Warfare Solutions to Network Security," *Canadian Military Journal* 6, no. 3 (Autumn 2005): 49-58.

[109] US DoD, JP 3-13.1, *Electronic Warfare* (Washington, DC: Department of Defense, 08 February 2012), I-4 to I-6, last accessed 2 April 2013, http://info.publicintelligence.net/JCS-EW.pdf

[110] There is no CF joint or operational-level doctrine for EW. Only the CA and the RCAF have published tactical doctrine. Chief of the Air Staff, B-GA-403-002/FP-001, *Aerospace Electronic Warfare Doctrine*, 1st Ed

identify and locate sources of intentional and unintentional radiated EM energy for the purpose of immediate threat recognition, targeting, and conduct of operations.[111] Doctrinally speaking, ES overlaps with SIGINT by providing targeting information for electronic or physical attack. EA intends to prevent or reduce an enemy's effective use of the EMS by either active or passive jamming.[112] Offensive EA suppresses a threat for a limited time, while defensive EA protects personnel, facilities, capabilities and equipment. EP is the component of EW that protects personnel, facilities, and equipment from any effects of friendly, neutral, or adversarial use of the EMS.[113] It also serves to protect against naturally occurring phenomena such as sunspots, lightning, and precipitation static, as well as EM radiation hazards to personnel, ordnance, and volatile materials.[114] EP tends to overlap with the CIS discipline when it deals with spectrum management processes, frequency coordination, and emission control, amongst other procedures.[115] Considering this ovelap, the US adopted the term Joint EM Spectrum Operations (JEMSO) in their doctrine as an umbrella term to encompass EW together

---

(Ottawa: DND, March 2011); and Chief of Land Staff, B-GL-351-003/FP-003, *Signals in Support of Land Operations – Volume 3: Tactical Electronic Warfare and Signals Intelligence* (Ottawa: DND, 28 March 2011).

[111] ES also "synchronizes and integrates the planning and operational use of sensors, assets, and processes within a specific battle space to reduce uncertainties concerning the enemy, environment, time, and terrain." US DoD, JP 3-13.1, *Electronic Warfare* . . ., I-6.

[112] Active jamming includes using EM energy or DE weapons such as lasers, electro-optical (EO), infrared (IR), and radio frequency (RF) or an electromagnetic pulse (EMP) to disrupt, degrade, deny, deceive, or destroy, while on the other hand, passive jamming involves non-radiating or re-radiating chaff, flares, towed decoys, etc. US DoD, JP 3-13.1, *Electronic Warfare* . . ., I-4 to I-5.

[113] Chief of Land Staff, *Signals in Support of Land Operations – Volume 3: Tactical Electronic Warfare and Signals Intelligence* . . ., 4-1.

[114] So as not to confuse, EP protects from the effects of friendly and/or adversary EA or EM interference, while defensive EA protects against lethal attacks by denying adversary use of the EMS to target, guide, and/or trigger their weapons. *Ibid.*

[115] Specifically, EW collaborates with CIS discipline in the management of the joint restricted frequency list (JRFL), and emission control (EMCON) procedures, and other EM spectrum management functions. *Ibid*., 7-3 to 7-4, and 5A-1.

with a management function of the EM operating environment.[116] While EW focuses on combat effects for a tactical level commander, JEMSO (as shown at Figure 3.4 below) encompasses a broader scope of EMS activities including host-nation spectrum coordination, spectrum interference resolution, frequency management and spectrum management to control neutral (i.e. civilians') and friendly forces' use of the EMS on behalf of an operational-level commander.[117]

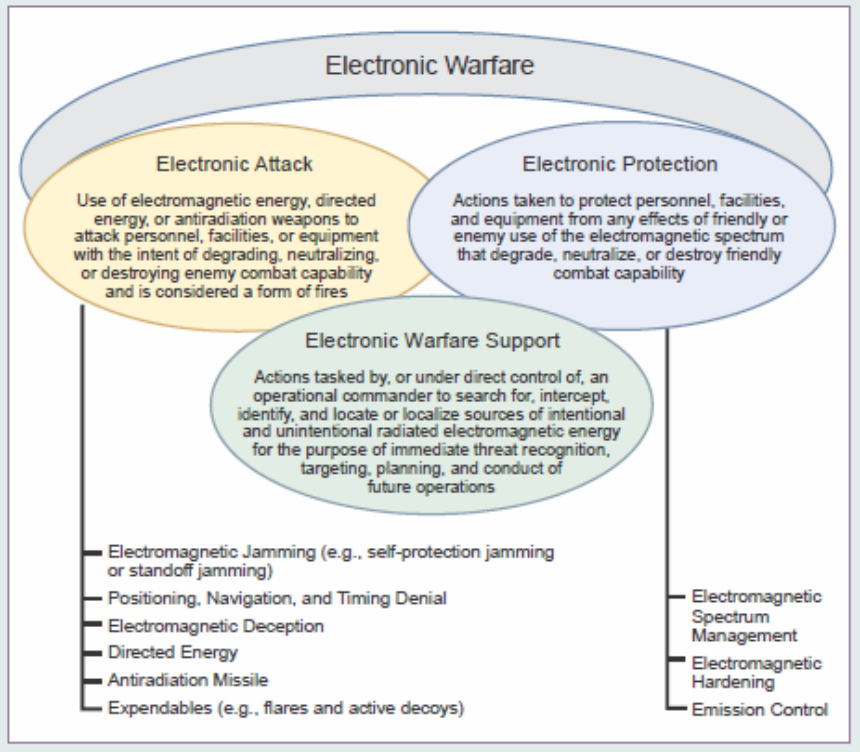


Figure 3.3 - Overview of Electronic Warfare

Source: US DoD, JP 3.13-1, *Electronic Warfare*, I-5.

[116]The Joint Electromagnetic Spectrum Operations (JEMSO) function in the CF is practically divided between the EW and CIS practitioners, but is not reflected in any CF doctrine. The US tends to take lead nation responsibility for coalition JEMSO operations through their combatant command joint EM support elements JEMSEs. US Department of Defense, JP 6-1, *Joint Electromagnetic Spectrum Management Operations* (Washington, DC: Department of Defense, 20 March 2012), I-5, http://www.dtic.mil/doctrine/new_pubs/jp6_01.pdf.

[117] As an example, JEMSO must consider that the International Telecommunication Union's (ITU) allocations for civil and military spectrum use in North and South America are different from those used in the Middle East and Asia.

For example, recent operations in Iraq and Afghanistan concluded a critical need for aligning military spectrum operations policies and procedures amongst the multinational partners, particularly early on in the deployment and deterrence phases – see Figure 3.5 below.[118]

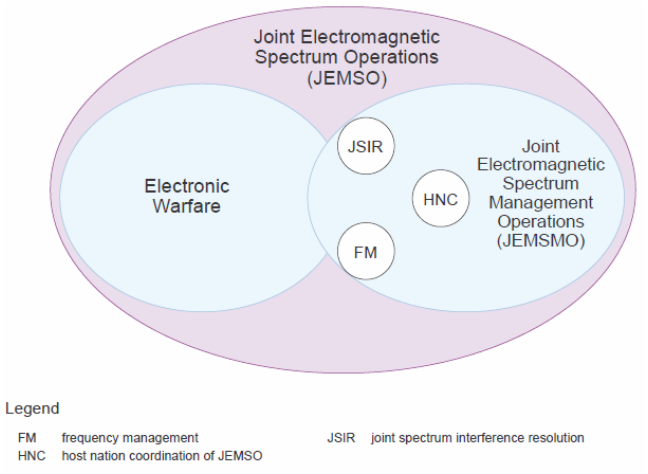


Figure 3.4 - Joint Electromagnetic Spectrum Operations (JEMSO)

Source: US DoD, JP 6-1, *Joint Electromagnetic Spectrum Operations*, I-5.

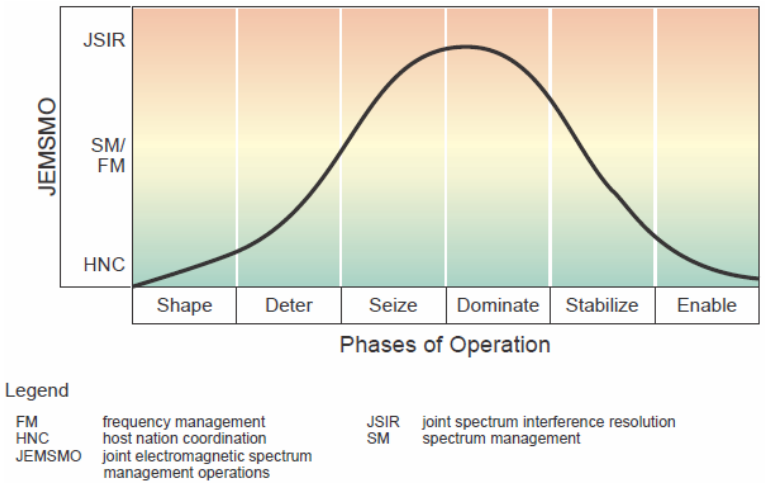


Figure 3.5 - JEMSO Activities across Notional Phases of Operation

Source: US DoD, JP 6-1, *Joint Electromagnetic Spectrum Operations*, VI-3.

[118] US DoD, JP 6-1, *Joint Electromagnetic Spectrum Management Operations . . .* , VII-1.

SIGINT is intelligence derived from communications, electronic, and/or foreign instrumentation signals.[119] A highly controlled discipline that involves considerable policy oversight and strict control over its activities, SIGINT is normally controlled as a strategic capability under the auspices of the national authority, such as Communications Security Establishment Canada (CSEC).[120] Within Canadian doctrine, SIGINT divides into two principle components: communications intelligence (COMINT), and electronic intelligence (ELINT).[121] Due to the sensitivity of SIGINT tradecraft, there are no unclassified lessons learned or operational recommendations from which to elaborate here. However, as has been already discussed, SIGINT doctrinally overlaps with ES (under EW) and with CNE (under CNO).

The discipline of CIS provides robust and secure communications system for the commander "to assimilate information and to exercise authority and direct forces over large geographic areas and a wide range of conditions."[122] Referred also as C4, C2IS, C3I and other derivatives, the responsibility of CIS is the management of end-to-end communications system for military operations en route to a theatre, inter-theatre (from

---

[119] Chief of Land Staff, B-GL-351-003/FP-003, *Signals in Support of Land Operations – Volume 3: Tactical Electronic Warfare and Signals Intelligence . . .*, 6-2.

[120] Treasury Board of Canada Secretariat, "*Policy on Government Security*", updated 1 April 2012, last accessed 2 April 2013, http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578&section=text.

[121] Obtained from intercepting communications and data links, COMINT derives its intelligence "from electromagnetic communications and communications systems, by those who are not the intended recipients of the information." ELINT derives its intelligence from the technical assessment of electromagnetic non-communications emissions produced by equipment such as radars, missile guidance systems, lasers, infrared devices, and any other equipment that produces emissions in the EMS compared with emission parameters of equipment signatures held in databases. Canadian Forces Warfare Centre. B-GJ-005-200/FP-001 *CFJP 2-0 – Joint Intelligence* (Ottawa: DND, 2011), 2-8.

[122] The CF has not published any joint CIS doctrine. See US DoD, JP 6-0, *Joint Communications System* (Washington, DC: Department of Defense, 10 June 2010), I-3 to I-4, http://www.dtic.mil/doctrine/new_pubs/jp6_0.pdf.

Canada to a theatre of operations) and intra-theatre (within an operational theatre between Canadian units, coalition forces, and the local communications infrastructure).[123] CIS expertise encompasses the full gamut of voice and data information exchange technologies, hardware and software maintenance, and information assurance responsibilities.[124]

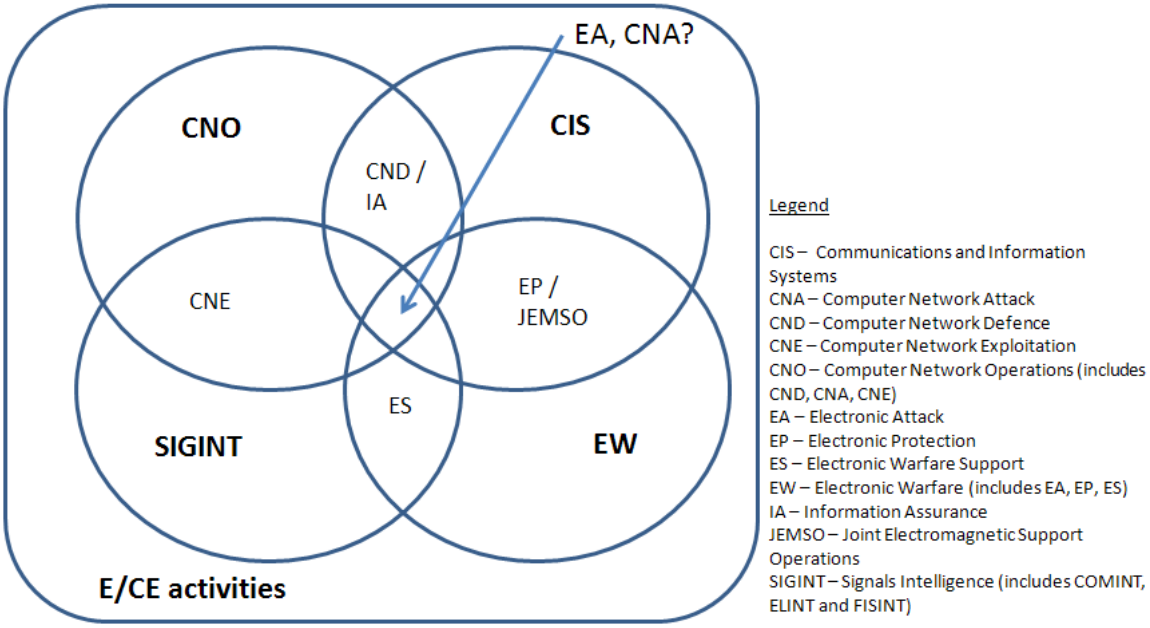


Figure 3.6 – Inter-relationships of E/CE-related Disciplines and Activities.

Source: Author.

Based on the above explanations, Figure 3.6 illustrates where each of the E/CE-related disciplines indicate some overlapping expertise and activities in the E/CE. As will

[123] "C4" is an acronym for Command and Control (C2), Communications, and Computers; "C2IS" for Command and Control Information Systems, and "C3I" occasionally used to combine C2 systems with Communications and Intelligence.

[124] Information assurance (IA) is "employed to ensure the security of information and the communications system through information protection, intrusion/attack detection and effect isolation, and incident response to restore information and system security." US DoD, JP 6-0, *Joint Communications System* . . ., I-11.

be discussed in Chapter 4, the mandates and authorities of the organizations involved in these disciplines vary in terms of focus and capabilities available, which leads to rather haphazard support to Commander CJOC at the operational-level. Therefore, an organization that encompasses all of these disciplines would enable CJOC to confront the myriad of challenges posed by the E/CE.

Expertise Needed for Legal Framework in the E/CE

Militaries around the world are wrestling with the concepts of fighting wars in the E/CE. The CF is no different. When the Stuxnet worm that attacked Iran's nuclear program in 2010 marked the first known transition from the virtual cyber world to the physical world, it highlighted that cyberspace (included in our described E/CE) is another place that "enable[s] an actor to utilize its strengths and exploit and adversary's vulnerabilities."[125] It also highlighted that it is incumbent upon operational commanders to fully prepare themselves to tackle the complexity of legal issues inherent to deterrence and use of force in order to respond in kind. To do so, CJOC will require an organizational construct that leverages all of the possible expertise available, including necessary legal and other subject matter experts.

Despite an increasing number of cyber-attack case studies, including a theoretical "e-9/11" or "Cyber Pearl Harbour" scenario, militaries generally lack a shared framework for how to recognize and then escalate a response to a hostile intent or act within

[125] Vincent Mazo, "Deterrence and Escalation in Cross-domain Operations: Where Do Space and Cyberspace Fit?" *Strategic Forum* 272 (December 2011), 2. last accessed 2 April 2013, http://www.ndu.edu/inss/docUploaded/SF%20272_Manzo%20.pdf

cyberspace.[126] NATO attempted to discuss possible response measures to cyber-attacks against Estonia in 2007, and to-date is working on bolstering its defensive capabilities, but has not yet reached a consensus on pursuing its own offensive actions within cyberspace.[127] This is because it has not yet defined the threshold as when a cyber-attack constitutes an "act of war" against the alliance or one of its members. Fred Schreier, of the neutral DCAF organization, attempts to tackle the "attack" definition:

> *Cyber attack as a mode of conflict* raises many operational issues and, due to inherent ambiguities, some other problems. Among these is the *'use of force'* and *'act of war' conundrum*. Problems also derive from the *legal framework governing cyber attacks*. Then, there is the *problem of deterrence in cyberspace* that is affecting retaliation, preemption, and conflict escalation. *Networked forces*, the most recent military innovation, hold the promise of fighting more effectively, but they also create more uncertainties. In order to *effectively manage cyber conflicts*, these may have to be categorized into various levels, depending on their intensity and impact on war.[128]

Canadian doctrine lists deterrence and coercion as general strategies, but neither has been explored to any significant detail in the context of the E/CE.[129] Similarly, although NATO recognizes the significance of the cyber threat, its *Strategic Concept* maintains only a generic approach to the deterrence problem – "Deterrence, based on an appropriate mix of nuclear and conventional capabilities, remains a core element of our overall

---

[126] *Ibid.*, 1.

[127] The NATO Cyber Incident Response Capablity (NCIRC) and the Rapid Reaction Team (RRT) are defensive capabilities created from the 2010 Lisbon Summit and the 2010 Strategic Concept. NATO, "NATO Rapid Reaction Team to fight cyber attack," 13 March 2012, last accessed 2 April 2013, http://www.nato.int/cps/en/natolive/news_85161.htm.

[128] "DCAF" is a Swiss initiative for the Democratic Control of Armed Forces. Original italics emphasis. Fred Schreier, *On Cyberwarfare – DCAF Horizon 2015 Working Paper 7* (Geneva: DCAF), 68, http://www.dcaf.ch/Publications/On-Cyberwarfare.

[129] Deterrence as the "military preparedness of the nation and the overt willingness to use military power such that an adversary decides that the risk of carrying out a particular course of action is not worth the potential consequences." Coercion is defined as another method "to persuade others to do something that may not be in their particular national interest. Canadian Forces Warfare Centre. B-GJ-005-000/FP-001 *CFJP-01 - Canadian Military Doctrine* (Ottawa: Department of National Defence, 2011), 2-2 to 2-3.

strategy."[130] US Deputy Secretary of Defense, William J. Lynn, opined "traditional arms control agreements would likely fail to deter cyber-attacks because of the challenges of attribution, which make the verification of compliance almost impossible."[131] Martin Libicki of RAND Corporation argues that the aggressor and the target may wish to keep the matter *sub rosa*, in that public visibility of an attack only complicates matters and leads to required escalation.[132] However, the conundrum remains as to "how to credibly threaten to impose costs on aggressors and deny benefits of attack."[133]

As there is no common definition as to what constitutes an "attack" (or "use of force") in cyberspace on national sovereignty (or "act of war"), it is difficult to develop a coherent deterrence strategy with measures of defined proportional response.[134] For instance, the similarity between cyber exploitation and cyber-attacks are very similar. Exploitation extracts information from a network without authorization, while an attack deliberately uses force to degrade, destroy or alter an adversary's system. Although the threshold for calling any activity an "act of war" is ultimately a political decision, it has become customary "practice that propaganda, harassment, hacktivism, and crime [in the

[130] This approach continues the Nuclear Deterrence approach of the Cold War, where escalation will only broaden the geographic operational area, the targets to be considered, and an increasing intensity to the violence. NATO, *Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization* (Brussels: NATO Public Diplomacy Division, 20 November 2010), 14.

[131] William J. Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (September/October 2010), 100.

[132] Libicki argues that neither side wants to acknowledge the conflict for two reasons: in order that the battle damage remains invisible, and that attribution can be very difficult. Martin C. Libicki, "Sub Rosa Cyber War," in *The Virtual Battlefield: Perspectives on Cyber Warfare*, edited by Christian Czosseck and Kenneth Geers, 53-65 (Fairfax, VA: IOS Press Inc., 2009).

[133] Mazo, "Deterrence and Escalation in Cross-domain Operations". . ., 3;

[134] "There is no international consensus on a precise definition of a use of force, in or out of cyberspace. Consequently, individual nations may assert different definitions, and may apply different thresholds for what constitutes a use of force." Lieutenant-General Keith Alexander, as cited in "Answers to Advance Questions for Lieutentant General Keith Alexander, USA, Nominee for Commander US Cyber Command," 15 April 2010, last accessed 2 April 2013, http://www.washingtonpost.com/wp-srv/politics/documents/questions.pdf; This is in spite of Geneva Convention Additional Protocol I, Article 49(1), that defines "attack" as "an act of violence against the adversary, whether in offence or defence."

E/CE] do not justify the use of force in response."[135] Unfortunately, the media also tends to over represent reported incidents of exploitation as "attacks," thereby giving the impression that deterrence has already failed and that responses to exploitations will diminish the credibility of any future responses to "attacks."[136]

Therefore, military planners likely possess dissimilar assumptions regarding proportionality and escalation. Does a response to a non-kinetic attack have to be a non-kinetic, or does a kinetic response indicate an escalation? It is rather evident that states will contemplate all responsive actions at their disposal, even those that may differ from the "domain" from which the attack originated. In other words, although an attack may come from cyberspace, it should not mean that that a symmetrical retaliation must occur in cyberspace. Therefore, it should be reasonable to conclude that despite the additional inclusion of cyberspace, a response will be based on the real-world effects of the attack, and not on the "domain." Pre-emption is even more complicated to discern since an assessment is based on the threat of hostile intent.

Although the government has yet to task publicly the CF with a particular role in conducting offensive cyber action, this should not dissuade Commander CJOC from proactively discerning the operational planning considerations and assemble the legal and other expertise to prepare for such a mission. Despite the added complexity of "offensive cyber action" issues within a combined E/CE, Commander CJOC still has other E/CE related activities that must be carried out in a given theatre of operations. These also have real unique planning considerations.

---

[135] Schreier, *On Cyberwarfare . . .*, 70.
[136] *Ibid., 7.*

Other Unique Operational Planning Considerations in E/CE

As discussed at the start of this chapter, the E/CE is a complex operational environment that must be fully integrated with other aspects of military planning. Although there are a number of unique operational planning considerations to the E/CE, two fundamental areas stand out – interoperability coordination, and use of force.

Interoperability Coordination

Coordinating operational EM/Cyber effects requires a level of interoperability with other government departments (OGDs), coalition partners, and other planning staffs. In order to minimize collateral effects to friendly forces and neutral parties within a given theatre of operations, liaison and planning must occur at multiple levels. For operations within Canada, liaison will be required with OGDs that have specific mandates and authorities – Chapter 4 will discuss the relationships with CSEC, Industry Canada and Public Safety Canada. Outside Canada, there is currently no known "Coalition Cyber" staff construct; however, for EW/JEMSO, allied partners such as the US often take on lead nation responsibility. Additionally, strategic level coordination is already a continuous activity between DND/CF and entities within NATO and the Five-Eyes Combined Communication Electronics Board (CCEB).[137] When a Canadian TF conducts

[137] NATO coordination is through various capability panels of the civil/military NATO Consultation, Command and Control Board (NC3B), which is now part of the NATO Communications and Information Agency (NCI Agency). NCI Agency, "Welcome to the NCI Agency", last accessed 2 April 2013, http://www.ncia.nato.int/Pages/default.aspx; The Five-Eyes nations coordinate spectrum management through the Combined Communications Electronics Board (CCEB); Combined Communications Electronics Board, ACP 190(C), *Guide to Spectrum Management in Military Operations*, September 2007,

operations within the E/CE, it must also liaise with several coalition elements, including (but not limited to):

- Higher EW Coordination Centre (EWCC) and other higher and lateral EW planning staffs; [138]
- US Joint Frequency Management Office (JFMO) or Joint Spectrum Management Element (JSME) – at coalition HQ or at a US Combatant Command HQ level;[139]
- Host Nation spectrum management authority;
- Theater Network Operations Control Center (TNCC) and other higher and lateral Cyber planning staffs (yet to be determined);[140] and/or
- SIGINT channels such as Cryptologic Support Groups/Teams.

Additionally, liaison is required between the deployed Canadian TF HQ and the subordinate tactical component commands in order to understand their own integral E/CE capabilities and to coordinate effects. For some economy of effort, intelligence channels could facilitate some of this liaison, as EW and SIGINT plays a significant part in intelligence processes; however, this would be pursued on an exceptional basis only.[141]

---

http://jcs.dtic.mil/j6/cceb/acps/acp190/ACP190C.pdf; see also US DoD, JP 6-1, *Joint Electromagnetic Spectrum Management Operations* . . ., Figure II-1.

[138] US DoD, JP 3-13.1, *Electronic Warfare* . . ., II-2.

[139] This entity is also generically known as a Combined Spectrum Management Cell (CSMC). US DoD, JP 6-1, *Joint Electromagnetic Spectrum Management Operations* . . ., II-5.

[140] US DoD, JP 6-0, *Joint Communications System*. . ., III-2.

[141] SIGINT channels are highly classified which creates some challenges to information sharing amongst coalition members. In addition, depending on the coalition membership of troop contributing nations, SIGINT channels may not be inclusive to all coalition members.

Although allied doctrine would be a significant enabler to this interoperability effort, very little has been developed to date.[142]

Use of Force

As an instrument of national power, the CF's use of force is controlled by government policy, and both national and international law, all of which guides the extent to which actions are proportional, reasonable, and necessary to achieve legitimate military objectives.[143] Within the E/CE, rules of engagement (ROE) approved by the Chief of Defence Staff authorizes the appropriate use of force via and delegated through Commander CJOC to a deployed TF commander. Although a deployed Canadian TF commander may not necessarily have their own integral E/CE resources (such as EW or CNO), they will need appropriate ROE prior to enabling another coalition member to conduct an offensive effect in the E/CE on their behalf.

Use of force planning within the E/CE is akin to any other kinetic activity targeting process involving "joint fires." Consequently, there are numerous unique considerations concerning the *jus in bello* principles of military necessity, distinction, proportionality, perfidy, neutrality, and unnecessary suffering, that still require legal and policy considerations.[144] For instance, the complexity of cyber and EM systems makes determining whether a target creates a "definite military advantage" a challenge. Additionally, most cyber attackers lack sufficient information of the downstream effects

[142] There is nothing in the unclassified literature regarding interoperability other than that prescribed in the latest US doctrine publications on JEMSO and EW.

[143] Canadian Forces Warfare Centre, *CFJP-01 - Canadian Military Doctrine . . .*, art. 0242 (2-6).

[144] Geneva Convention Additional Protocol I, Articles 51-58.

of their actions to predict the indirect consequences of an attack.[145] This is easier to do in the EMS due to the known power outputs and frequencies of the equipment. Subsequently, if the means and methods of a cyber-attack produce the same effects in the real world as conventional weapons (i.e. destruction, disruption, damage, injury or death), there is argument that it should be governed by the same rules as conventional weapons.[146] However, it may take a while before cyber-specific considerations make it into military doctrine.[147] Irrespective the chosen method of attack, ROEs should be reviewed prior to the actual use of these weapons, so that operators have the proper guidance and laws of armed conflict training such that they can be held accountable under specific operational circumstances.[148]

Chapter Summary

Beginning with a review of the "operational functions" it was clear that military operations are dependent on the availability of the E/CE. It was equally evident that the capabilities in the E/CE are reciprocally dependent on each "function." The complexity of the E/CE considerations with respect to these "operational functions" lends to the argument that CJOC requires a dedicated organization to focus the planning and execution of operations in the E/CE. A review of the inter-relationships amongst the E/CE-related disciplines of CIS, CNO, EW, and SIGINT determined that considerably synergy could be attained by a collective subordinate organization under Commander

---

[145] Schreier, *On Cyberwarfare* . . .,73.

[146] *Ibid.*, 69.

[147] Some action has been taken to capture legal opinions related to the cyber warfare. Published in 2013, the Tallinn Manual reflects the opinions of a group of independent experts, but it is non-binding and therefore is not yet reflected in NATO doctrine or policy. NATO CCD COE. *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013), 1. https://www.ccdcoe.org/249.html.

[148] David P. Fidler, "Inter arma silent leges Redux? The Law of Armed Conflict and Cyber Conflict," In *Cyberspace and National Security*, … 81-83; and Schreier, *On Cyberwarfare* . . ., 104-105.

CJOC that encompasses all of these disciplines. Lastly, the problems associated with deterrence and offensive operations highlighted that militaries around the world are still wrestling with the concepts of fighting wars in the E/CE. Despite an increasing number of case studies regarding cyber-attacks, militaries still lack a shared legal framework for how to recognize and then escalate a response to a hostile intent or act within cyberspace. Although the Government of Canada has yet to task publicly the CF with a particular role in conducting offensive cyber-attacks, CJOC should include legal and other subject matter experts within its E/CE organization to discern amongst the considerations that such a mission requires. Regardless, the entire scope of E/CE activities necessitates knowledgeable liaison staff and prior considerations related to the use of force within the scope of the laws of armed conflict.

This chapter set out to highlight that operations within the E/CE require a clear understanding of many considerations for the operational-level commander. As generalists, these operational-level commanders should be able to rely upon a single subordinate specialist organization to coordinate these effects on their behalf.

CHAPTER 4 – THE CANADIAN FORCES DEFENCE STRATEGY AND THE EM AND CYBER ACTORS

If the CF is going to remain relevant to the Canadian populace, it must ensure that it maintains the right capabilities for achieving the missions and tasks levied upon it. Although the CF never wishes to see itself employed as the force of primary resort, it must continue to work with the other government actors in a supporting role, while it quietly remains prepared to take the lead as contingencies or situations require it to do so.

Within the current missions assigned, CJOC must anticipate what tasks that it could receive and prepare the necessary forces to respond accordingly. As discussed in Chapters 2 and 3, CJOC already has a unique challenge in the E/CE due to the complexity of the threats and the planning considerations associated with it. Chapter 3 also demonstrated that CJOC should seek to create a subordinate organization capable of leveraging the inter-relationships amongst the various E/CE-related disciplines to plan and conduct operations in this environment on its behalf. Unfortunately, the many military and non-military actors that influence CF operations in the E/CE are dispersed throughout the DND/CF organization, and are not entirely focussed on supporting CJOC's operations. Also considering the OGDs and agencies that influence the CF's operations within the E/CE, CJOC will need to examine the mandates, missions and/or roles of these specific actors in order to identify areas where it is possible to optimize coordination and improve unity of effort.

This chapter will start with an examination of the new CJOC and its intended mission, roles and tasks within the current government's *CFDS* strategy, noting that the previously discussed threats and operational functions related to the E/CE factors into all

the *CFDS* missions. An analysis of the missions and roles of both military CF and DND supporting actors within the E/CE disciplines at the strategic, operational and tactical levels will identify interrelationships and gaps amongst these actors that are vital for CJOC's operations. As will be shown, some organizations such as Director General Information Management Operations (DGIMO) and CF Information Operations Group (CFIOG) are organizations most suited from which to build a subordinate E/CE organization for CJOC, however it is misplaced in its current command and control relationship under the Assistant Deputy Minister (Information Management) (ADM(IM)). Finally, a review of the other government actors in the E/CE will demonstrate that the CJOC must work with national mandates and authorities held by Communications Security Establishment Canada (CSEC), Industry Canada (IC), Shared Services Canada (SSC) and Public Safety Canada (PSC) in order to conduct its own business within the E/CE. In its routine operations and as the government's force of last resort, CJOC must harmonize its relationships with these organizations in order to conduct operations within the E/CE.

The Supported Commander - CFDS missions and CJOC

In October 2012, CJOC was stood up to integrate the functions and capabilities of its precursors, Canada COM, CEFCOM and CANOSCOM, into "an agile formation able to conduct continental and expeditionary operations efficiently and effectively, in response to [GC] priorities."[149] Based on recommendations from the *Report on*

[149] CF Transformation 2005 efforts to establish more effective command and control over domestic/continental, expeditionary and operational support capabilities for CF operations led to the creation of Canada Command (Canada COM), Canadian Expeditionary Forces Command (CEFCOM), and Canadian Operations Support Command (CANOSCOM) in 2006. Department of National Defence, "Canadian Joint

Transformation 2011, one of the substantiations for a "single Force Employer entity" (now known as CJOC) was to leverage

Operational Command: Mission and Mandate," last accessed 2 April 2013, http://www.cjoc-coic.forces.gc.ca/wwh-qqc/mission-eng.asp#mandat;

developing capabilities such as intelligence and cyber:

> . . . moving to a single Joint Force Employment entity would present a valuable opportunity to further integrate CF C4ISR capabilities into a single, all-encompassing organization. This would leverage the positive progress already made by [Chief of Defence Intelligence] to create a national intelligence capability that encompasses both Force Employment and Force Generation functions for already established units and capabilities, such as the [Canadian Forces Information Operations Group (CFIOG)] and [Canadian Forces Network Operations Centre (CFNOC)]. *It would also allow the development and maturation of emerging capabilities such as Cyber to take place with strong Force Employment-oriented oversight, thereby reinforcing the operational organizational culture so critical to the healthy evolution of these highly specialized capabilities.*[150]

Despite this specific reference to the direct benefits of "cyber" under CJOC, only a rudimentary staff liaison capability from CFIOG has been established installed in CJOC to date.[151]

As the operational-level Supported Commander for the CF, as shown in Figure 4.1, the "Canadian Joint Operations Command anticipates and conducts [CF] operations, and develops, generates and integrates joint force capabilities for operations."[152] Recognizing the unique natures of the Canadian Special Operations Forces Command (CANSOFCOM) and the bi-national NORAD Command, Commander CJOC becomes the de facto principal commander for the following six missions under the current government's *Canada First Defence Strategy (CFDS)*:

---

[150] Italicized emphasis added. "C4ISR" is acronym for Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance. CF Chief of Transformation, *Report on Transformation 2011* (Ottawa: DND, 6 July 2011), 48-49, last accessed 2 April 2013, http://www.forces.gc.ca/site/reports-rapports/transfo2011/_doc/Report_on_Transformation_2011_eng.pdf.

[151] Joint Cyber Operations Team, *Joint Cyber Operations Team (JCOT) Concept of Operations – Draft Version 2.0*, n.p., 12 December 2012.

[152] DND, "Canadian Joint Operational Command: Mission and Mandate," last accessed 2 April 2013, http://www.cjoc-coic.forces.gc.ca/wwh-qqc/mission-eng.asp#mandat.

- Conduct daily domestic and continental operations, including in the Arctic [with the exception of NORAD's mission];
- Support a major international event in Canada;
- Respond to a major terrorist attack;
- Support civilian authorities during a crisis in Canada such as a natural disaster;
- Lead and/or conduct a major international operation for an extended period; and
- Deploy forces in response to crises elsewhere in the world for shorter periods.[153]

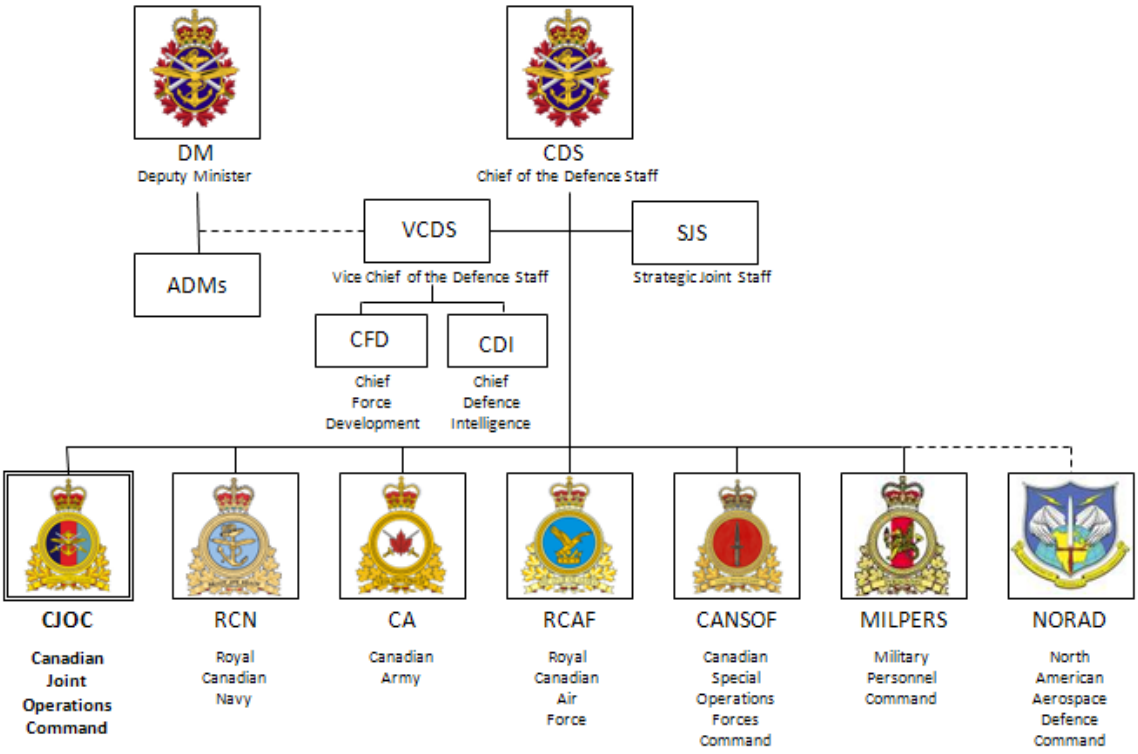


Figure 4.1 – Command and Control of CJOC within the DND/CF

Source: Adapted from Department of National Defence, "DND Organization Chart."[154]

From the threats describe in Chapter 2 and the operational considerations defined in Chapter 3, Commander CJOC is concerned with activities in the E/CE on a continuous basis, in addition to the above specified *CFDS* operations which occur in or require

[153] Government of Canada, *Canada First Defence Strategy . . .*, 3.
[154] DND, "DND Organization Chart," last accessed 2 April 2013, http://www.forces.gc.ca/site/about-notresujet/org-eng.asp.

"freedom of manoeuvre" within the E/CE. Whether it is intelligence horizon scanning for the next potential expeditionary operations area, or fending off daily "attacks" to the CF's own computer networks and EMS, there is an ongoing need for dedicated E/CE specialists to directly support CJOC.

Despite these ongoing threats and the importance of the E/CE to CJOC's mission set there is no organization directly responsible to Commander CJOC for the E/CE. This is significantly unusual considering that CJOC has other dedicated subordinate organizations, as depicted at Appendix 4, such as the Regional Joint Task Forces (RJTFs), the Maritime and Air Component Commands (MCC and ACC), and a deployable 1st Canadian Division Headquarters to "command" operations in the physical air, sea, and land environments, and the CF Joint Operational Support Group (CFJOSG) dedicated entirely to the "Sustain" function.[155] CJOC anticipates that the current JOINTEX series will highlight further areas for convergence between operational and tactical commands that conduct multiple "operational functions," in addition to identifying specific gaps and overlaps for E/CE capabilities.[156]

---

[155] The operational function "Command" is conducted by the Regional Joint Task Forces (RJTFs) who report to directly to Commander CJOC in matters of domestic operations and consequence management; a Maritime Component Command (MCC) to command ships deployed; a Joint Forces Air Component Commander (JFACC) from the RCAF to command air elements; and a deployable operational Task Force Headquarters (TF HQ) based on CA Brigade HQs or the 1st Canadian Division HQ deploy as a Combined Joint Inter-Agency Task Force Headquarters (CJIATF HQ). DND, "Canadian Forces Joint Operational Support Group," last accessed 2 April 2013, http://www.cjoc.forces.gc.ca/os-so/osc-soc-eng.asp; and Commander 1st Canadian Division, *Force Employment Concept 1st Canadian Division Headquarters* (1st Canadian Division Headquarters: file 3350-1 (Comd), 21 March 2012.

[156] DND, "JOINTEX drives a CF cultural evolution," *The Maple Leaf* 15, issue 04 (April 2012): 11, last accessed 2 April 2013, http://www.forces.gc.ca/site/tml/article-eng.asp?id=17&y=2012&m=04; and DND, "JOINTEX 13 prepares CF for future operations," *The Maple Leaf* 15, issue 11 (December 2012): 6, last accessed 2 April 2013, http://www.forces.gc.ca/site/tml/article-eng.asp?id=9&y=2012&m=12.

The Military Supporting Actors

A number of CF entities operating within the E/CE regularly contribute to CJOC operations, but are not directly responsible to it due to their current command and control relationships. This section will review their roles in order to ascertain potential gaps and the interrelationships of their activities towards CJOC at the operational-level. Strategic-level entities such as DGIMO and CFIOG likely provide the most focus towards CJOC's efforts in the E/CE at the operational level. Other tactical-level entities and other actors within the CF and DND have capabilities and subject matter expertise from which CJOC should be able to leverage.

DGIMO and CFIOG

The one military entity that contributes the most to operational-level E/CE activities is DGIMO. As the operational division within the ADM(IM) group, DGIMO has military responsibilities in all E/CE disciplines of CIS, CNO, EW and SIGINT. As Deputy CF J6, the position of DGIMO also has a staff responsibility to the CF's Strategic Joint Staff (SJS) in terms of planning and advice. The DGIMO division comprises several subordinate formations: CFIOG, which will be discussed later; 76 Communication Group, which provides CIS support to CJOC HQ in Ottawa; national cryptologic support and maintenance units; and, departmental information assurance directorates.[157]

The DGIMO/J6 Coordination staff provides supported commanders and staffs at all levels with strategic planning by coordinating CIS activities across the CF, providing

[157] 76 Comm Group, which provides direct CIS support to NDHQ entities, including CJOC HQ. The CF Cryptologic Support Unit (CFCSU) and the CF Cryptologic Maintenance Unit (CFCMU) and the Directorate of Information Management Security (D IM Secur) are CIS-related entities under DGIMO. ADM(IM), "DGIMO: Mission," last accessed 2 April 2013, http://img.mil.ca/aim-pgg/org/dgi-dgo/index-eng.asp#mis (DWAN).

advice in support of CF operations, in addition to engagement with NATO, the Five-Eyes CCEB and other interoperability programs.[158] As the highest level DND/CF entity organized for coordinating E/CE operations, this division of ADM(IM) would likely provide the most benefit to Commander CJOC as a future subordinate E/CE entity. An alternative would be to move its subordinate formation of CFIOG that encompasses elements of the CNO, EW and SIGINT disciplines required by CJOC.

Within geographic proximity of the CJOC in Ottawa, CFIOG is a formation of headquartered at CFS Leitrim, with three units: CFS Leitrim, the CF Network Operations Centre (CFNOC), and the CF Electronic Warfare Centre (CFEWC), with detachments scattered across Canada, and performing liaison in the US and the UK.[159] While CFIOG performs only a subset of the doctrinal "information operations" capabilities, its stated roles and responsibilities are:

- To operate and maintain [SIGINT] collection and geolocation facilities in support of the [CF]/Canadian government;
- To operate and maintain radio frequency direction finding facilities in support of search and rescue and other programs;
- To maintain an operationally ready Cryptologic [elements] in support of military operations;
- To provide technical [EW] support to the [CF]; and
- To provide computer network defence support to the [DND].[160]

---

[158] J6 Coord staff enable CJOC by coordinating predominantly CIS support into the ADM(IM) group of engineering and technical support directorates. Director General Information Management Operations, *Director General Information Management Operations Strategic Assessment and Business Plan – FY 2009/10* (NDHQ: file 1948-4 (DGIMO), 19 June 2009.

[159] CFIOG has elements located at Fort Meade, MD and members on exchange with several US and UK organizations.

[160] CFIOG's mission statement is "To coordinate, develop and employ assigned *information operations* enabling capabilities for the [CF] and the [DND]" This is a rather outdated mission statement, as it does not perform "information operations" in the doctrinal sense. Assistant Deputy Minister (Information Management), "CFIOG Roles and Responsibilities," last accessed 2 April 2013, http://img.mil.ca/aim-pgg/org/dgi-dgo/cfi-goi/index-eng.asp (DWAN).

As shown in Figure 4.2, DGIMO has full command over CFIOG. However, this is where the command and control relationship splits. As the CF's technical control authority for SIGINT, CFIOG is under the operational control of Chief Defence Intelligence (CDI) for the day-to-day SIGINT responsibilities that befall CFS Leitrim and CFEWC missions.[161] Meanwhile, the remainder of CFIOG, CFNOC, has the mission to "fight the networks" in six main mission areas: "National System Operations, Incident Management, Computer Network Defence, Security Operations, [Information Technology Infrastructure] Situational Awareness, [and] Problem Management."[162] CFIOG works closely with its closest foreign intelligence allies in the remaining Five-Eyes nations "to share the collection burden and the resultant intelligence yield."[163] Based on these long established relationships within the national defence intelligence community and the larger international EM/Cyber community of practice, CFIOG is the nexus for operations in the E/CE for commander CJOC. To enable this relationship, Commander CFIOG has extended a planning, liaison and advisory capability known as the "Joint Cyber Operations Team" directly into the CJOC HQ.[164]

---

[161] CFS Leitrim's published roles are "To operate and maintain signals intelligence collection and geolocation facilities in support of the CF/Canadian government." Assistant Deputy Minister (Information Management), "CFIOG: Roles and Responsibilities," last accessed 2 April 2013, http://img.mil.ca/aim-pgg/org/dgi-dgo/cfi-goi/index-eng.asp (DWAN); and CFEWC's mandate is the maintenance and development of the CF EW Database (CFEWDB) which contains an extensive repository of radar parametric data on a multitude of air, land, and sea platforms and their associated weapon systems. Assistant Deputy Minister (Information Management), "CFEWC Fact Sheet," last accessed 2 April 2013, http://img.mil.ca/os-so/io-oi/ewc-cge/fs-fr-eng.asp (DWAN).

[162] Assistant Deputy Minister (Information Management), "CFNOC: Mission," last accessed 2 April 2013, http://img.mil.ca/aim-pgg/org/dgi-dgo/cfi-goi/cfn-cor/index-eng.asp#mis (DWAN).

[163] Assistant Deputy Minister (Information Management), "CFIOG Roles and Responsibilities," last accessed 2 April 2013, http://img.mil.ca/aim-pgg/org/dgi-dgo/cfi-goi/index-eng.asp (DWAN).

[164] Joint Cyber Operations Team, *Joint Cyber Operations Team (JCOT) Concept of Operations – Draft Version 2.0*, n.p., 12 December 2012, 4.

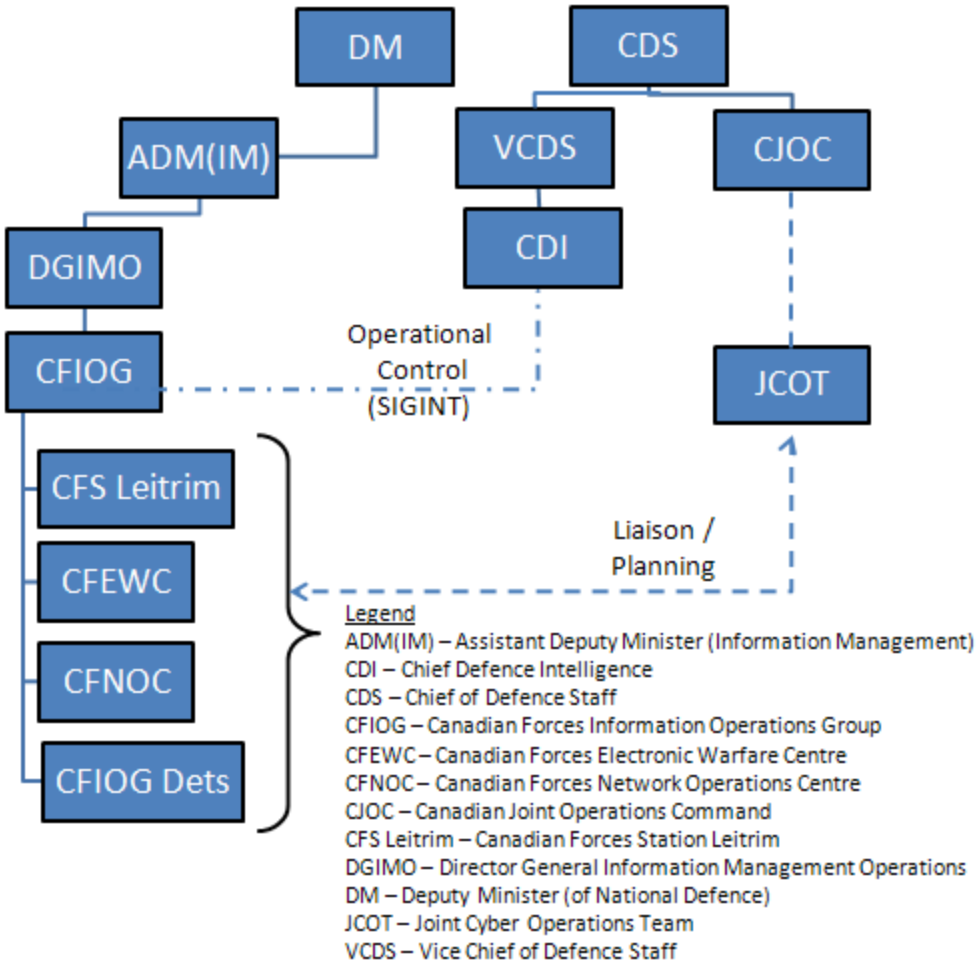


Figure 4.2 – Command and Control of DGIMO and CFIOG within DND/CF

Source: Based on information from Joint Cyber Operations Team, *Joint Cyber Operations Team (JCOT) Concept of Operations – Draft Version 2.0*.[165]

Navy, Army, Air Force and Other Joint Actors

All military actors generally participate in the E/CE through their use of office equipment (e.g. computers, telephones, cell phones), their unique platforms (e.g. ships, aircraft, and land vehicles), and general military hardware such as sensors, radios and other information devices. As their primary purpose is at the tactical level, the

[165] *Ibid.*

information systems are oriented for their own tactical purposes with some common office automation application software.[166] Due to their unique nature, and as described at Appendix 5, each of the CF's environmental services has different occupational trades that train in the various E/CE disciplines. Based on the descriptions provided at Appendix 5, Figure 4.3 illustrates that there is an overlap of current CF occupations operating within the given E/CE disciplines. Appendix 5 also highlights that few occupations and units work currently at the operational-level of war (which is relevant for CJOC operations). As such, it will be necessary to leverage the planning and deployable technical expertise resident in strategic units such as those in CFIOG and at the tactical level for CJOC.

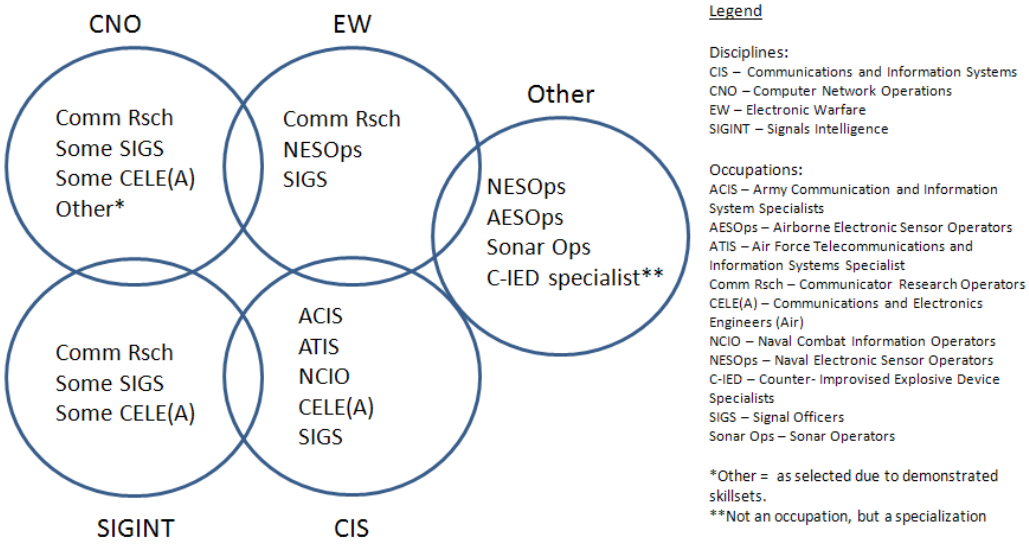


Figure 4.3 – CF Occupations Operating in the E/CE

[166] At the tactical level, the Army has the Land Command Support System (LCSS), the RCAF has the Air Force Command and Control Information System (AFCCIS), and the RCN has the Maritime Command Operation Information Network (MCOIN). The operational-level joint network is referred to as the "Comd-Net" which integrates the tactical level networks over the bearer Classified Secure Network Infrastructure (CSNI). Chief of Staff (Information Management), *Implementation Order 005/12 – IM Gp Support to LCCS/CSNI Convergence* (National Defence Headquarters: file 3350-3 (J6 Coord), 26 July 2012.

Sources: Canadian Forces Recruiting, "Browse Jobs."[167]

The CA's corps of Signals is the principal entity that handles EM/Cyber matters on Army bases, and at tactical unit and brigade formations. Signals has the role, "To provide commanders and their staffs with the means to exercise command and control through the exploitation of the military and global information environment while denying and exploiting the enemy's use of the same."[168] Signals doctrine focuses on the tactical efforts shared between EW and CIS disciplines.[169] The majority of Signals are Signal Officers and Army Communication and Information System (ACIS) Specialists employed in battalion signal troops and brigade signal squadrons, which provide the necessary CIS required by commanders for command and control.[170]

21 EW Regiment has a troop's complement of Communicator Research Operators available for force employment in a deployed Canadian TF.[171] This unit also has the responsibility to force generate an EW Coordination Centre (EWCC) for 1st Canadian Division HQ (as a CJIATF) in order to provide tactical-level coordination with a higher

---

[167] Occupational information available from Canadian Forces Recruiting, "Browse Jobs," last accessed 2 April 2013, http://www.forces.ca/en/JobExplorer/BrowseJobs-70.

[168] Chief of Land Staff, B-GL-351-001/FP-001, *Signals in Support of Land Operations – Volume 1* (Ottawa: DND, 1 May 2008), Art. 102 (1-1).

[169] Canadian Forces Recruiting, "Communicator Research Operator," last accessed 31 January 2013, http://www.forces.ca/en/job/communicatorresearchoperator-29; and Canadian Forces Recruiting, "Army Communication and Information Systems Specialist," last accessed 2 April 2013, http://www.forces.ca/en/job/armycommunicationandinformationsystemsspecialist-171.

[170] Signal Offers are specialists trained primarily in CIS, but may also acquire EW, CNO or SIGINT experience at later intervals in their careers. Army Communication and Information System (ACIS) Specialists deploy intra-theatre telecommunications networks over satellite and wireless networks using allocated frequencies, installing fibre optic and cable infrastructure, and information assurance enforcement. Canadian Forces Recruiting, "Signals Officer," last accessed 2 April 2013, http://www.forces.ca/en/job/signalsofficer-79; and, Canadian Forces Recruiting, "Army Communication and Information Systems Specialist," last accessed 2 April 2013, http://www.forces.ca/en/job/armycommunicationandinformationsystemsspecialist-171.

[171] See Annex B to Commander Canadian Army, *Army Strategic Transition Roadmap (ASTR)* (Commander Canadian Army: file 1901-1 (DLFD 3), 13 April 2012.

coalition EWCC and JSME as the case may be.[172] The Land Integrated Support Section (LISS), co-located with the CFEWC, provides the Army with specific EW operational support.[173]

Finally, various ground-based C-IED Task Force and ISTAR sensor specialists are quite familiar with the effects and dependence of their systems within the E/CE.[174] Regardless, other than an annual information system security brief and a very cursory introduction of EW and CIS during the Army Operations Course for Army captains/majors, few Army occupations receive any further formalized E/CE professional development. If the Army heeds its own advice, it will develop future capabilities that are more integrated and agile to the future land operating environment:

> Technological foresight and organizational speed will become increasingly important enablers of institutional resilience.
>
> Network-enabled operations will provide a key means of ensuring the Army is highly adaptive, agile and combat effective within the JIMP environment. This concept involves the integration of a network of tactical forces and other elements supported by sensor, direct and indirect fire, combat service support, influence activity, and command and control systems linked by voice and data to create a

---

[172] Due to its highly specialized training and the high security clearance requirements, the EWCC generated by 21 EW Regiment is the likely framework from which to build future Canadian JSME or JEMSO Coordination Centres (JEMSOCC) as needed for CJOC deployed TFs. Commander 1st Canadian Division, *Force Employment Concept 1st Canadian Division Headquarters* (1st Canadian Division Headquarters: file 3350-1 (Comd), 21 March 2012.

[173] The Land Information Support Section provides specialised electronic intelligence management tools, parameter databases and training support. Canadian Army, "DLCI 6-4-3 section (LISS)," last accessed 2 April 2013, http://lfcms.kingston.mil.ca/Default.aspx?sectionID=143000440012209&type=S (DWAN).

[174] Counter-Improvised Explosive Device (C-IED) and Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR) elements within the Canadian Army employ systems that require a detailed level of EM/Cyber expertise, or seek advice from EW. ISTAR elements include armoured reconnaissance, artillery surveillance and target acquisition (STA), military intelligence analysis, Army-operated unmanned aerial vehicles (UAVs), and EW. Department of National Defence, "Counter Improvised Explosive Device Task Force," last accessed 2 April 2013, http://www.army.forces.gc.ca/land-terre/ciedtf-focdec/index-eng.asp; and Chief of Land Staff, B-GL-352-001/FP-001, *ISTAR Volume 1 – The Enduring Doctrine - Study Draft* (Kingston, ON: Director of Army Doctrine, 22 August 2012), 4-10 to 4-11.

level of situational awareness, mobility and support that will overwhelm adversaries' understanding of the operating space and their ability to react. [175]

The RCAF has units comprised of Communications and Electronics Engineers (CELE) and Air Force Telecommunications and Information Systems (ATIS) technicians. Together, their role is:

> To provide telecommunications and information management services, operate and maintain tactical Air Force and strategic communications systems, manage air traffic control and electronics systems, and advise on the planning and acquisition of ground based surveillance, communications and information technology systems, . . . [and the] full spectrum of terrestrial radio and satellite communications from HF to EHF radar and navigation systems, electronic warfare, cryptography, electronic intelligence, or communications and network security.[176]

Embedded within the RCAF's wing/base logistic organizations, these occupations predominantly support CIS infrastructure. Deployable airfield CIS and air traffic services for an ACC in an expeditionary Canadian TF would likely come from the 8 Air Communications and Control Squadron (8 ACCS). [177] Meanwhile, the Aerospace and Telecommunications Engineering Support Squadron (ATESS) supports "unique

---

[175] HF is high frequency and EHF is extreme high frequency. Commander Canadian Army, *Designing Canada's Army of Tomorrow - A Land Operations 2021 Publication* (Ottawa: Department of National Defence, 2011), 23 and 33, http://www.army.forces.gc.ca/CALWC-CGTAC/pubs/armyoftomorrow/DesigningCanadasArmyofTomorrow_full_e.pdf.

[176] Canadian Forces Recruiting, "Communications and Electronics Engineering (Air) Officer," last accessed 2 April 2013, http://www.forces.ca/en/job/communicationsandelectronicsengineeringairofficer-77; and Canadian Forces Recruiting, "Aerospace Telecommunication & Information Systems Technician," last accessed 2 April 2013, http://www.forces.ca/en/job/aerospacetelecommunicationinformationsystemstechnician-18#info-1.

[177] It is also likely that the CIS for an Air Component Commander could be supported from Army or Joint CIS organizations. Royal Canadian Air Force (RCAF), "8 Air Communication and Control Squadron," last accessed 2 April 2013, http://www.rcaf-arc.forces.gc.ca/8w-8e/sqns-escs/page-eng.asp?id=679.

aerospace and air force Command and Control Information Systems (C2IS) support capabilities."[178]

Most in line with the EW discipline is the RCAF's Aerospace Warfare Centre's EW Operational Support (EWOS) section.[179] This small section provides critical advice to the Canadian deployed EWCC (or JEMSOCC) on matters related to RCAF and coalition air force's EW counter-measures.[180] The RCAF also has professional development in the form of a basic and an advanced EW course that enhances planning staff and specialists in ever-changing EW equipment and tactics, techniques and procedures.[181] Airborne Electronic Sensor Operators (AESOps) play a significant part in the E/CE by operating radar, electro-optical (EO) and infra-red (IR) systems, magnetic anomaly detection, and EW equipment onboard long-range patrol aircraft, maritime helicopters and unmanned aerial vehicles.[182]

The RCN has a distinctive approach to the E/CE, considering today's seagoing vessels are predominantly floating sensor platforms. The Naval Electronic Sensor Operators (NESOps), Sonar Operators and Naval Combat Information Operators

---

[178] RCAF, "Aerospace and Telecommunications Engineering Support Squadron (ATESS)," last accessed 2 April 2013, http://www.rcaf-arc.forces.gc.ca/8w-8e/units-unites/page-eng.asp?id=691.

[179] Working with the CFEWC, the EWOS's role is "To provide timely and quality . . . reprogramming, in-theatre support and operational test and evaluation." RCAF, "CFAWC: Electronic Warfare Operational Support (EWOS)" last accessed 2 April 2013, http://www.airforce.forces.gc.ca/CFAWC/EWOS_e.asp.

[180] Capabilities and measures on both rotary and fixed-wing fleets include chaff, flares, on-board electro-optical (EO) and infra-red (IR) sensors, and radio frequency jammers and signature reduction. Chief of the Air Staff, B-GA-403-002/FP-001, *Aerospace Electronic Warfare Doctrine* . . ., 8.

[181] Basic and Advanced EW courses are offered by the Canadian Forces School of Aerospace Studies (CFSAS) to specialists and air staff planners. RCAF, "Basic Electronic Warfare (BEW)," last accessed 2 April 2013, http://www.rcaf-arc.forces.gc.ca/itp-pfi/page-eng.asp?id=939 (DWAN); and RCAF, "Advanced Operational Electronic Warfare (AOEW)," last accessed 2 April 2013, http://www.rcaf-arc.forces.gc.ca/itp-pfi/page-eng.asp?id=931 (DWAN).

[182] Canadian Forces Recruiting, "Airborne Electronic Sensor Operator," last accessed 2 April 2013, http://www.forces.ca/en/job/airborneelectronicsensoroperator-8.

(NCIOs) are dedicated trades that operate systems in the E/CE. [183] In addition to the dedicated non-commissioned member occupations, the RCN also trains its officers through the CF Maritime Warfare Centre on onboard EW and CIS capabilities.[184] The Naval EW Centre (NEWC) "enables the conduct of effective Naval EW operations through the provision of parametric data, ES libraries, EA programs and techniques, analysis, and supporting subject matter expertise [. . .] including tactics, policy, training, trials, requirements and R&D.[185]

Lastly, there are other joint EM/Cyber organizations within the CF. In addition to the aforementioned DGIMO and CFIOG (which operate as "joint" entities) the only remaining capability is the CF Joint Signal Regiment (CFJSR), under the CFJOSG. Principally focussed on the CIS discipline, CFJSR's mission is "to provide high readiness and sustainment [CIS] to deployed commanders domestically and throughout the world, allowing effective [C2] of assigned forces."[186] Although the CFJSR already provides CIS support to CJOC, and the deployable CJIATF HQ (1st Canadian Division HQ), it would

---

[183] NESOps operate radar and radio detection devices, radar jamming systems and decoys. Canadian Forces Recruiting, "Naval Electronic Sensor Operator," last accessed 2 April 2013, http://www.forces.ca/en/job/navalelectronicsensoroperator-23; Operators compile and analyze acoustic intelligence information from a combination of active and passive sonars, sonar simulators, communication equipment, bathythermograph equipment, sonobuoys and data transmission systems. Canadian Forces Recruiting, "Sonar Operator," last accessed 2 April 2013, http://www.forces.ca/en/job/sonaroperator-25; NCIOs operate all shipboard surveillance radars and associated equipment of the shipboard intelligence, surveillance and recognizance systems, including configuring data links and global C2 systems. Canadian Forces Recruiting, "Naval Combat Information Operator," last accessed 2 April 2013, http://www.forces.ca/en/job/navalcombatinformationoperator-22.

[184] Officers of the Naval Combat Systems Engineering and Martime Surface and Sub-surface Warfare occupations are trained in the various sensor, EW and CIS systems that are employed onboard ships. Canadian Forces Recruiting, "Maritime Surface and Sub-surface Officer," last accessed 2 April 2013, http://www.forces.ca/en/job/maritimesurfaceandsubsurfaceofficer-65; or Canadian Forces Recruiting, "Naval Combat Systems Engineering Officer," last accessed 2 April 2013, http://www.forces.ca/en/job/navalcombatsystemsengineeringofficer-82.

[185] Royal Canadian Navy, "Naval Electronic Warfare Centre (NEWC)," last accessed 2 April 2013, http://marcom-comar.mil.ca/cfmwc-cgnfc/newc-cgen/default-eng.asp (DWAN)

[186] Canadian Forces Base Kingston, "Canadian Forces Joint Signal Regiment (CFJSR)," last accessed 2 April 2013, http://www.army.forces.gc.ca/asu_kingston/cfjsr.aspx.

need considerable revision of its tasks and considerable new resources in order to take on even the most closely related E/CE discipline responsibilities of CNO and/or JEMSO.

As discussed in Chapter 3, use of the E/CE leads to operational considerations for Commander CJOC, which requires commensurate expertise and ideally a dedicated organization. Although their intended roles are to provide support to their respective local tactical level commanders, Command CJOC should be able to leverage the aforementioned CF tactical actors' expertise and capabilities at the operational-level. A grouping of these like-minded capabilities would focus training and provide deployable support in this regard.

Other Actors/Enablers in the DND/CF

The previous section discussed the tactical military actors of the specific E/CE discipline. By no means was this an exhaustive list of actors with an E/CE nexus. A number of DND/CF organizations operating at the strategic level of the department also enable those tactical level organizations. Mindful of these relationships, CJOC needs to be able to leverage their mandates or their capabilities when needed for operational-level purposes.

Director General Space (DG Space), under CFD, is the current organization responsible for integrating the pervasive use of Space-based capabilities into CF operations. Space-based capabilities within the E/CE include global communication networks, satellite surveillance, navigation capabilities (e.g. Global Navigation System Surveillance/Navigation Warfare), Space-based surveillance of Space debris and missile

warning systems, and participation in related coalition Space operations.[187] In addition to extending and providing redundancies for terrestrial EM/Cyber use, these capabilities are dependent upon effective control of the E/CE.

The Chief Defence Intelligence (CDI) is another significant contributor to EM/Cyber operations. In addition to providing strategic intelligence regarding threats to the E/CE, it also has functional authority over SIGINT in the CF, which it exercises through its operational control relationship over CFIOG.[188] Due to the nature of SIGINT, there are strong relationships and critical information sharing arrangements established with like-minded militaries and civilian organizations that are critical for CJOC operations in the E/CE. Any consideration towards changing the command and control of DGIMO and/or CFIOG with CJOC will need to revisit this particular relationship with CDI.

The research and development of military EM/Cyber capabilities is enhanced by the efforts of Assistant Deputy Minister (Science and Technology) – ADM(S&T) - and the Defence Research and Development Canada (DRDC) centres. Working in partnership with Canadian industry, universities, and allied defence S&T organizations, there are a number of research areas focusing on E/CE-related capabilities at DRDC Centres in

---

[187] DG Space projects include an array of capabilities that affect EM/Cyber environment – Polar Epsilon (persistent ground surveillance from satellites), Global Navigation Satellite System/Navigation Warfare (GNSS/NAVWAR) technologies, Protected Military SATCOM, Mercury Global, UHF Terminal Upgrade, Low Earth Orbit search and rescue satellite repeaters (LEOSAR) and Medium Earth Orbit satellite repeater (MEOSAR). Department of National Defence, "DND/CF Space Operations: To The Future and Beyond," *The Maple Leaf* Vol 15, Issue 5 (May 2012): 8-9, last accessed 2 April 2013, http://www.forces.gc.ca/site/tml/article-eng.asp?id=1&y=2012&m=05.

[188] "Operational Control" provides CDI with the authority to give CFIOG mission and tasks related to its functional intelligence accountabilities. Director General Military SIGINT (DGMS) is the military staff appointment that oversees the SIGINT function on behalf of CDI. Chief Defence Intelligence, *CF Signals Intelligence (SIGINT) Policy (ratification draft)*, n.p., 25 June 2007.

Ottawa and Valcartier.[189] Moreover, DRDC provides expertise across a number of C4ISR capabilities including field trials, supporting integration of capabilities into ongoing operations and equipment training.[190] ADM(S&T)/DRDC is a critical enabler for any organization within the CF that is conducting operations within the E/CE.

EM/Cyber capabilities within the CF have extensive procurement processes. These processes fall under the auspices of Assistant Deputy Minister (Materiel) (ADM(MAT)) and the multitude of staffs that capture requirements, acquire equipment and services from industry, and ultimately procure and integrate the equipment or services for the CF end-users. Tactical EM/Cyber capabilities are the responsibilities of ADM (Mat) sub-directorates responsible for CA, RCN or RCAF capabilities. Historically, joint EM/Cyber organizations such as CFIOG and CFJSR had their requirements captured through DGIMO, with project directors and managers and life-cycle managers assigned from within the ADM(IM) organization. This equipment procurement and sustainment process will need revisiting if there is a move to optimize E/CE capabilities under a single operational commander.

The last, and certainly not least, DND/CF actor within the E/CE is ADM(IM), as the corporate organization responsible for enterprise information holdings and

---

[189] DRDC Ottawa's "expertise includes: radio frequency (RF) sensing; RF electronic warfare; RF communications technology; cyber operations; space systems." DRDC Valcartier has "expertise in optronic systems, information systems, and combat systems." Defence Research and Development Canada (DRDC), "DRDC Ottawa," last accessed 2 April 2013, http://www.drdc-rddc.gc.ca/drdc/en/centres/drdc-ottawa-rddc-ottawa/; and Defence Research and Development Canada, "DRDC Valcartier," last accessed 2 April 2013, http://www.drdc-rddc.gc.ca/drdc/en/centres/drdc-valcartier-rddc-valcartier/.

[190] DRDC, "Areas of Science and Technology Expertise," last accessed 2 April 2013, http://www.drdc-rddc.gc.ca/drdc/en/sciences/expertise/.

information technologies.[191] In addition to capability development, ADM(IM) directorates provide services related to enterprise applications systems and integration, leasing of commercial telecommunication services, information assurance coordination and enforcement, and configuration control management of information technology across the department. Most pertinent to the operational-level commander, they have a dedicated sub-directorate that handles all spectrum management requirements (i.e. frequency allocation, hardware licensing, etc.) for the DND/CF with IC and coalition lead nation agencies in NATO, CCEB, and the like. Having this section under ADM(IM) for domestic coordination to IC makes sense, but it is rather convoluted when it also the conduit through which the CF coordinates frequency and spectrum requirements for deployed operations to coalition partners. The mandate of this specific sub-directorate should be revisited to ensure that it is directly meeting CJOC's requirements.

The Other Government Departments

The E/CE is an important sector of Canada's *National Strategy for Critical Infrastructure* due to its interdependencies with other sectors and the need for comprehensive and proactive risk management processes through all levels of government.[192] Starting with the 2010 *Speech from the Throne* and culminating in *Canada's Cyber Security Strategy*, the government has leveraged existing partnerships

---

[191] ADM(IM)'s enabling mission is in the "planning, development, delivery and support of innovative IM/IT capabilities that enable successful [CF] Operations."[191] Department of National Defence, "Assistant Deputy Minister (Information Management)," last accessed 2 April 2013, http://www.img.forces.gc.ca/index-eng.asp; and Assistant Deputy Minister (Information Management), "Mission," last accessed 2 April 2013, http://img.mil.ca/aim-pgg/mv/index-eng.asp (DWAN).

[192] The E/CE is referred is the "Information & Communication Technology" sector within the 10 sectors of the National Cross-Sector Forum comprising: Energy & Utilities, Finance, Food, Transportation, Government, Health, Water, Safety, and Manufacturing. Government of Canada, *National Strategy for Critical Infrastructure* (Ottawa: Public Safety Canada, 2009), 5-9, http://www.publicsafety.gc.ca/prg/ns/ci/_fl/ntnl-eng.pdf

based on the *National Action Plan for Critical Infrastructure* and the *Federal Emergency Response Plan (FERP)* to assign Public Safety Canada (PSC) as lead department for coordinating responses to emergencies involving the E/CE.[193]

PSC's Canadian Cyber Incident Response Centre (CCIRC) conducts daily reporting and coordination of national response of cyber-related incidents, while the Government Operations Centre (GOC) coordinates extensive emergencies involving multiple sectors. CCIRC works together with the Royal Canadian Mounted Police (RCMP), the Canadian Security Intelligence Service (CSIS), the Communications Security Establishment Canada (CSEC) and DND/CF in terms of monitoring, analyzing domestic and international criminal acts, terrorism, and other cyber threat actors within Canada and abroad.[194] As a signatory to the Council of Europe's *Convention on Cybercrime*, Canada strongly supports the territorial jurisdiction to prosecute in cybercrime cases, where the attacked computer is on its territory and the perpetrator of the attack is not.[195] Noteworthy to CJOC's own concerns over the E/CE, recent Office of the Auditor General (OAG) reporting indicates that PSC should augment CCIRC's operational capability to 24 hours a day, 7 days a week and should improve its

---

[193] Government of Canada, (speech, Speech from the Throne, Ottawa, Ontario, March 3, 2010), last accessed 5 February 2013, http://www.speech.gc.ca/eng/media.asp?id=1388; Government of Canada, *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada*. . ., 9-10; Government of Canada, *Action Plan for Critical Infrastructure* (Ottawa: Public Safety Canada, 2009), 2 and 12, http://www.publicsafety.gc.ca/prg/ns/ci/_fl/ct-pln-eng.pdf; and, Government of Canada. *Federal Emergency Response Plan* (Ottawa: Public Safety Canada, January 2011), A-5, http://www.publicsafety.gc.ca/prg/em/_fl/ferp-2011-eng.pdf.

[194] Public Safety Canada, "Cyber Security in the Canadian Federal Government," last accessed 2 April 2013, http://www.publicsafety.gc.ca/prg/ns/cybr-scrty/fdrl-gvt-eng.aspx.

[195] Although signed in 23 November 2001, Canada has not yet ratified the *Convention on Cybercrime* nor created legislation to enact this measure. Dominique Valiquet, *Cybercrime: Issues*, Publication No. 2011-36-E (Ottawa: Library of Parliament, 5 April 2011), 2; and Council of Europe, *Convention on Cybercrime* CETS No. 185, last accessed 2 April 2013, http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG.

information sharing across all levels of government and across all critical infrastructure sectors.[196]

Under these critical infrastructure strategies and plans, IC has the responsibility as the primary department for matters related to "Telecommunications Emergency Support Function" which includes:

- coordinating with the telecommunications industry;
- restoration and expansion of telecommunications infrastructure and services;
- safeguarding and restoration of national telecommunications-related cyber and information technology resources; and
- coordinating of federal actions to provide the required temporary emergency telecommunications and restoration of the affected telecommunications infrastructure.[197]

IC is primarily responsible for spectrum management, while the Canadian Radio-television and Telecommunications Commission (CRTC) is responsible for broadcast licensing and foreign ownership oversight.[198] This convoluted bureaucracy has been unable to find an appropriate balance that retains IC's responsibility to set policy only, and gives CRTC sole responsibility as the national regulator.[199] As the lead department for "information and communication technology sector network" under the *National Critical Infrastructure Action Plan*, IC has included the telecommunications providers in

---

[196] Office of the Auditor General of Canada, "Protecting Canadian Critical Infrastructure Against Cyber Threats," Chapter 3 in *2012 Fall Report of the Auditor General of Canada to the House of Commons* (Ottawa: PWGSC, 2012), 16-18. http://www.oag-bvg.gc.ca/internet/English/parl_oag_201210_03_e_37347.html.

[197] Government of Canada. *Federal Emergency Response Plan* . . ., A-5.

[198] Spectrum management is split between Industry Canada (*Radiocommunication Act*), and the Canadian Radio-television and Telecommunications Commission (*Broadcasting Act* and *Telecommunications Act)*, while DND manages spectrum for its own use due to national security considerations. See Canadian Radio-television and Telecommunications Commission Act, R.S.C., c. C-22 (1985) and Radiocommunication Act, R.S.C., c. R-2 (1985).

[199] CRTC's responsibility as national regulator is to manage spectrum, auction available spectrum, and issue licences to broadcasters, wireless and telecommunication services providers. Konrad von Finckenstein, Q.C. (speech, Spectrum Roundtable Panel on "The Institutions of Spectrum Management: Time for a Change?" Ottawa, Ontario, April 22, 2010), speech notes last accessed 2 April 2013, http://www.crtc.gc.ca/eng/com200/2010/s100422.htm.

the sector's deliberations, and has omitted broadcaster groups, global navigation, remote sensing, and other areas until future expansion.[200] This is indicative of the lack of EM/Cyber collaboration in the greater communities of interest, and should be a lesson for tighter collaboration in the DND/CF.

As the national cryptologic authority and the lead IT security agency, the CSEC has mandates to conduct the collection of EM/Cyber foreign intelligence, and provide response and mitigation advice and guidance to government departments and agencies regarding IT security.[201] CSEC benefits significantly from the collaborative efforts of its SIGINT foreign intelligence allies in the US, UK, Australia and New Zealand "to share the collection burden and the resulting intelligence yield."[202] In accordance with the *Policy on Government Security*, CSEC's expertise in IT security leads the government's ability to detect threats and respond accordingly, particularly with regards to critical infrastructure protection.[203] Although CSEC shares the same minister as DND, CSEC's interface with the CJOC is facilitated through CFIOG and CDI. [204]

All GC departments and agencies fall under the jurisdiction of Treasury Board Secretariat (TBS) policies related to IT asset management, IT standards and IT security

---

[200] Office of the Auditor General of Canada, "Protecting Canadian Critical Infrastructure Against Cyber Threats" . . ., 13-14.

[201] "CSEC provides leadership and coordination for departmental activities that help ensure the protection of electronic information and information systems of importance and serves as the government's national authority for SIGINT and Communication Security (COMSEC)." Treasury Board of Canada, "Policy on Government Security," Updated effective April 1, 2012, Appendix B, last accessed 2 April 2013, http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578&section=text; and National Defence Act, R.S.C., c. N-5, s.273.64 (1985).

[202] Communications Security Establishment Canada (CSEC), "Signals Intelligence (SIGINT)," last accessed 2 April 2013, http://www.cse-cst.gc.ca/home-accueil/what-que/sigint-eng.html.

[203] CSEC, "About IT Security," last accessed 2 April 2013, http://www.cse-cst.gc.ca/its-sti/index-eng.html.

[204] Chief CSEC is a Deputy Minister under the Minister of national Defence. CSEC, "Place in Government," last accessed 5 February 2013, http://www.cse-cst.gc.ca/home-accueil/about-apropos/place-in-gov-place-dans-gouv-eng.html.

oversight.[205] Responding to a 2010 OAG Report regarding aging IT infrastructure across several government departments, the government responded by creating Shared Services Canada (SSC) on 1 April 2012.[206] With the mandate "to *operate* and *transform* the government's IT infrastructure," the creation of SSC will affect CJOC operations due to its responsibilities over DND/CF unclassified networks, particularly during a domestic operations situation.[207] With the interface between the CF and SSC through the CF Shared Services Group (CFSSG) under ADM(IM), it will be important for CJOC to reinforce operational priorities in order to leverage required support when necessary.[208]

Furthermore, as "government" is also deemed a critical infrastructure sector, TBS created the *Government of Canada Information Technology Incident Management Plan (GC IT IMP)* as the means to which it escalates and handles threats in the IT environment to ensure the continuity and confidence of all departments within the federal government.[209] Critical to CJOC's CND activities, DND/CF is included in the *GC IT IMP* as shown in Figure 4.4 below.

---

[205] Treasury Board of Canada Secretariat, "Welcome to the Chief Information Officer Branch," last accessed 2 April 2013, http://www.tbs-sct.gc.ca/cio-dpi/index-eng.asp.

[206] Office of the Auditor General of Canada, "Aging Information Technology Systems," Chapter 1 in *2010 Spring Report of the Auditor General of Canada to the House of Commons* (Ottawa: PWGSC, 2010), 1-3. http://www.oag-bvg.gc.ca/internet/English/parl_oag_201004_01_e_33714.html

[207] Shared Services Canada, *Integrated Business Plan 2012-2013* (Ottawa: Shared Services Canada, 2012), 2, last accessed 2 April 2013, http://www.ssc-pc.gc.ca/media/documents/IBP%202012_E_VA9D1.pdf.

[208] Canadian Forces Shared Services Group (CFSSG) executes command and administration of military personnel assigned to deliver Shared Services Canada (SSC). This is conducted through 4 x Shared Services Units (SSUs) in each of Eastern, Western, Central and Atlantic regions. ADM(IM), "Canadian Forces Shared Services Group (CFSSG)," last accessed 2 April 2013, http://img.mil.ca/ssc-spc/index-eng.asp (DWAN).

[209] Treasury Board of Canada Secretariat, "GC Information Technology Incident Management Plan," last accessed 2 April 2013, http://www.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimti01-eng.asp.

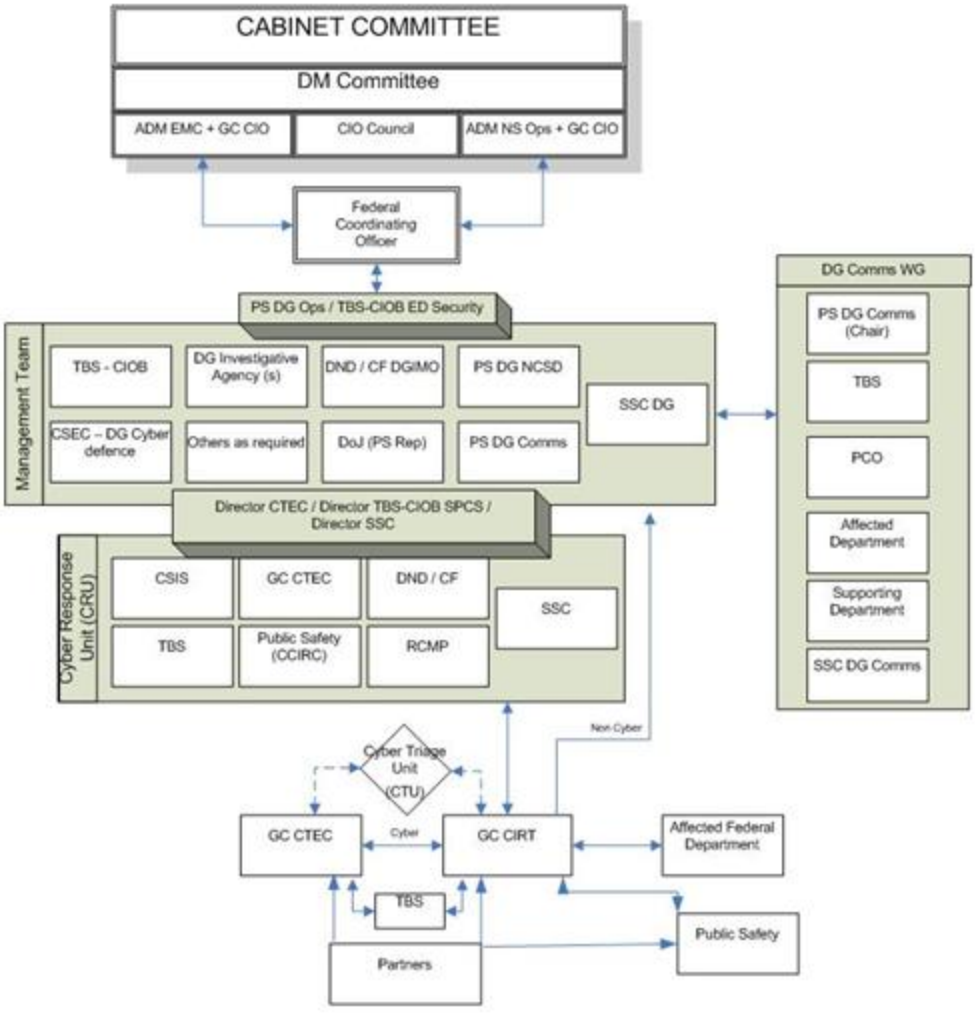


Figure 4.4 – IT Security Incident Response Governance Model

Source: Treasury Board of Canada Secretariat, *GC IT Incident Management Plan.*[210]

Due to its defence responsibilities and its alliance relationships, the DND/CF contributes to the overall EM/Cyber critical infrastructure risk management processes with PSC, CSEC, RCMP and CSIS. Conversely, DND/CF relies on the national mandates and authorities held by CSEC, IC (and CRTC), SSC and PSC in order to conduct its own business within the E/CE, particularly for the conduct of military domestic operations. Logically, it should follow that CJOC should enhance liaison

[210] *Ibid*., Figure 1.

directly with these agencies in order to streamline their support to CJOC's planning and conduct of operations in the E/CE.

Chapter Summary

The CF's relevance to the Canadian population will depend on its ability to achieve the missions, roles and tasks entrusted to it by the GoC. Although the CF primarily sees itself in a supporting role with other government actors, it must also be prepared to take the lead as contingencies or situations require it to do so. Therefore it is incumbent upon the principal supported CF military commander, Commander CJOC, to understand the mandates and missions of current supporting EM and Cyber actors from within the DND/CF and from across OGDs and agencies in order to leverage capabilities and expertise when required.

This chapter started with a review of the new CJOC and its intended mission, with a view to understanding the role of the supported commander. Under the government's six core *CFDS* missions/tasks, Commander CJOC becomes the de facto principal military commander, supported by an integral CFJOSG, domestic regional joint task force HQs, supporting component commands, and a deployable CJIATF HQ. Ongoing efforts to identify areas for convergence should lead to the conclusion for a dedicated organization under CJOC for the collective operations required in the E/CE. A review of the military and DND supporting actors that operate within E/CE at the strategic, operational and tactical levels then followed. Due to their existing relationships in the E/CE disciplines of CIS, CNO, EW, and SIGINT, DGIMO and CFIOG appear to be the entities most logically postured for a future direct supporting relationship to CJOC. A review of the

E/CE-related occupations and units of the RCN, CA, and RCAF illustrated that CJOC operations at the operational-level will need to leverage the capabilities and expertise diffused amongst other strategic and tactical-level organizations. An optimized grouping that encompasses each of the E/CE disciplines should be explored by CJOC. The final section explored the mandates and roles of OGD actors and industry as they affect CF operations. Governed by the same TBS policies as other federal departments, the CF contributes to and benefits from the overall EM/Cyber critical infrastructure risk management processes in conjunction with other security actors such as PSC, CSEC, RCMP and CSIS. As noted, CJOC relies upon the national authorities and responsibilities of CSEC, IC (and CRTC), SSC and PSC for the conduct of daily operations within the E/CE. Reinforcing the relationships with these organizations through a single E/CE organization will be critical for CJOC's operations.

Now that there is a better understanding of the actors within DND/CF, it would be advantageous to explore how allies are approaching the E/CE.

CHAPTER 5 –
ALLIES' APPROACHES TO THE EM/CYBER ENVIRONMENT

The previous chapter discussed the manner in which the CF and the rest of the Canadian government are approaching the E/CE in terms of current forms and functions. As a military force, the CF must be cognisant of not only its domestic responsibilities and accountabilities, but also how it conducts operations within the larger global E/CE and particularly how it interoperates with its international allies. The threats presented in Chapter 1 are trends consistently found around the world. Despite the recognition that governments need to come together in order to confront the impending threats, momentum has been slow. At least for Western nations, this is primarily due to two very politically-charged and competing issues related to the E/CE – regulation and privacy.[211] Each nation will approach these issues based on their own interests and values. While some nations have imposed significant controls over the E/CE within their borders, others have only regulated portions thereof (mostly in the management of the EMS). Consequently, most Western militaries have predominantly focussed their efforts on protecting that which they can control - defending their own portion of the E/CE, and specifically their own C4ISR systems. However, this is now starting to change as the CF's allies recognize that in order to achieve "freedom of action" within the environment they also need to establish the full spectrum of defensive through offensive capabilities.[212]

---

[211] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It (*New York: Harper Collins Publishers, 2010), 141.

[212] Secretary of Defense, Donald Rumsfeld, and Chairman of the Joint Chiefs of Staff, General Pace, refer respectively to "freedom of action"and "strategic superiority in the domain" in their Forward memoranda; see US Chairman of the Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations (Unclassified)*

In a coalition, interoperability intends to establish a common understanding of the operating environment (as discussed in Chapter 3), to develop common doctrine and standards, and to share tested tactics, techniques and procedures (TTPs).[213] As very little policy and doctrine has been developed to date, and any doctrine and TTPs that do exist tend to be highly classified, these specific aspects cannot be explored in this paper. [214] Nevertheless, much can be gleaned from national and allied efforts by looking at other national policies, their strategies and any newly constructed entities that are working in the E/CE. Any CF contribution to coalition operations, as commanded through Commander CJOC, must seek EM/Cyber interoperability with its coalition partners as an enduring goal in order that it can function either as a troop contributing nation or, if necessary, as a lead nation.

Whether it is continental or expeditionary operations overseas, it is incumbent upon the CF's operational-level commanders to appreciate how other nations are approaching the E/CE in order to leverage pertinent lessons (and risks) for their own strategies and structure. To do this, this chapter will undertake an overview of what Canada's allies are doing, as reflected in their current government strategies or policies, their lead government and military actors, and their considerations or approaches they have adopted for operating in the E/CE. Based on the quantity and quality of unclassified

---

(Washington, D.C.: US DoD, December 2006), v and vii, last accessed 2 April 2013, http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf.

[213] Interoperability in this context refers to the NATO definition: "The ability to act together coherently, effectively and efficiently to achieve Allied tactical, operational and strategic objectives." NATO Standardization Agency, AAP-06, *NATO Glossary of Terms and Definitions* (Brussels: NATO Standardization Agency, 2012), 2-I-8.

[214] Some action has been taken to capture legal opinions related to the cyber warfare. Published in 2013, the Tallinn Manual reflects the opinions of a group of independent experts and does not yet reflect doctrine or policy. NATO CCD COE. *Tallinn Manual on the International Law Applicable to Cyber Warfare.* New York: Cambridge University Press, 2013. https://www.ccdcoe.org/249.html.

material available regarding EM/Cyber efforts by CF allies, this review will start with the US, the CF's closest and most important bilateral partner. This will be followed by reviews of the efforts within NATO, and then subsequently with information available regarding the other Five-Eyes nations. By the end of this review, it should be apparent that the CF's part in overall government cyber strategy is an approach common with that taken by its allies. Moreover, there are opportunities that CJOC should exploit such as participation in the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) and NATO Cyber Incident Response Centre (NCIRC), liaison and exchange within US Cyber Command, the US Service-level Cyber organizations, or the UK Defence Cyber Operations Group (DCOG) as priority.

United States

As the CF's most important ally, and considering Canada's internetworking of EM/Cyber critical infrastructure with the US, any approach that the US undertakes in the E/CE will have a strong influence on how Canada does so.[215] According to the US Information Technology (IT) Dashboard, the US DoD spent approximately $33 Billion on IT while DHS spent approx. $5.6 Billion in 2012.[216] Due to its self-proclaimed global military dominance in other warfighting domains, through its Unified Command Plan, the US immediately embraced cyberspace as an important warfighting domain that it should

[215] US Department of Homeland Security and Public Safety Canada. *Canada-United States Action Plan for Critical Infrastructure*. 2010, last accessed 2 April 2013, http://www.dhs.gov/xlibrary/assets/ip_canada_us_action_plan.pdf.

[216] United States Government, "IT Dashboard," last accessed on 2 April 2013, http://www.itdashboard.gov/portfolios.

also seek to dominate.[217] It was in 2006 that the Joint Chiefs of Staff first defined cyberspace "as a domain characterized by the use of electronics and [EMS] to store, modify and exchange data via networked systems and associated physical infrastructures."[218] In order to appreciate the US overall approach to EM/Cyber, it is important to understand the US government policies and strategies including the role of non-military actors such as DHS. Looking at the immense transformation undertaken by the new Cyber Command and other EM/Cyber units in the US Services, there is significant leading-edge example and opportunity from which a CJOC EM/Cyber entity could learn.

United States Government

In 2009, President Obama launched a comprehensive review of cyberspace security that recommended that the coordination of government and national efforts required a single central official appointed by the President.[219] From this, the only policy document that has followed has been the *International Strategy for Cyberspace*, which speaks to coordination with allies and presents a defense objective to "oppose those who would seek to disrupt networks and systems, dissuading and deterring malicious actors, and reserving the right to defend these national assets as necessary and appropriate."[220]

---

[217] William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs* 89, no. 5 (September/October 2010): 101.

[218] US Chairman of the Joint Chiefs of Staff, *The National Military Strategy for Cyberspace*. . ., 3.

[219] US White House. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. Washington, D.C.: White House, May 2009, last accessed 2 April 2013, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[220] US White House, I*nternational Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World* (Washington, D.C.: White House, May 2011), 12, 20-21, last accessed 2 April 2013, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

Whether intended or not, this statement has opened the door for considerations of retaliation and other such actions.[221]

On the home front, the strategy fails to address key domestic policy areas such as leadership within the US government and for the nation as a whole.[222] Various presented options

[221] Siobhan Gorman and Julian E. Barnes, "Cyber Combat: Act of War," *Wall Street Journal*, May 30, 2011, last accessed 2 April 2013, http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html?KEYWORDS=cyber+combat.

[222] US goals include international promotion of "an open, interoperable, secure and reliable information and communications infrastructure" in which "norms of responsible behaviour guide states' actions, sustain partnerships, nd support the rule of law in cyberspace." *Ibid.*, 8.

include:

- a cyber czar working for the Executive Branch – status quo, but deemed insufficient as the incumbent is not accountable to Congress through confirmation process nor has any delegated budget authority;
- a lead Cabinet department – allows Congressional oversight, but it is difficult decision as to which of DHS or DoD (both of which have their advantages) to dictate cyber response to other departments; or
- the creation of a new entity with the federal government.[223]

DHS, through its National Cybersecurity and Communications Integration Center (NCCIC) has established relationships with industry via the Information Sharing Analysis Centers (ISACs) and through activities such as Homeland Security Exercises Cyber Storm.[224] However, due to the ever-increasing threats including foreign intelligence agencies and militaries, even DHS realizes that the scope is beyond its mandate. Naturally, this opens the argument that DoD with its extensive experience and manpower should have lead. In addition to the limitations of the Posse Comitatus Act and a lack of regulatory and law enforcement authorities, this option remains severely contentious as it would essentially give DoD responsibility over civilian systems.[225] The third option regarding the creation of a Director of Cyber, akin to the Director of National Intelligence (DNI), that would give legal and budget authority while requiring Congressional oversight, appears most viable.

---

[223] Kevin P. Newmeyer, "Who Should Lead U.S. Cybersecurity Efforts?" *Prism 3,* no. 2 (March 2012): 116, last accessed 2 April 2013, http://www.ndu.edu/press/us-cybersecurity-efforts.html.

[224] US Department of Homeland Security, "Cyber Storm: Securing Cyber Space," last accessed 2 April 2013, http://www.dhs.gov/cyber-storm-securing-cyber-space.

[225] Newmeyer, "Who Should Lead U.S. Cybersecurity Efforts?". . ., 121.

To add to the challenges, US Congress has not been able to pass any comprehensive legislation regarding security in cyberspace despite even the President's own persuasive efforts.[226] Like their Canadian counterparts, US politicians face many legal considerations and debates on whether it should indeed regulate cyberspace within its borders. In a 2008 report, the Center for Strategic and International Studies recommended that government-imposed regulation of cyberspace is required in four key areas:

- The development of shared standards and best practices for cyber security in the three critical infrastructure sectors (ICT, finance, energy) to improve performance and increase efficiency;
- The creation of new regulations that apply to . . . SCADA and other ICSs;
- Changes to federal acquisitions rules to drive security in products and services; and
- Mandatory authority of identify using robust credentials for critical infrastructure sectors.[227]

The latest round of the proposed *Cybersecurity Act of 2012* even reduced the minimal security standards to be voluntary (instead of mandatory) requirements for companies operating critical infrastructure sectors in cyberspace.[228] The security of cyberspace remains an ongoing struggle, not likely to be resolved any time soon in the current US political climate.

---

[226] CBC News, "Cybersecurity bill fails to pass in U.S. Senate," last accessed 2 April 2013, http://www.cbc.ca/news/technology/story/2012/08/02/tech-cybersecurity-bill-us.html; and Barack Obama, "Taking the Cyber Threat Seriously," *Wall Street Journal*, July 19, 2012, last accessed 2 April 2013, http://online.wsj.com/article/SB10000872396390444330904577535492693044650.html?KEYWORDS=Obama+cybersecurity.

[227] James R. Langevin, et al, *Securing Cyberspace for the 44th Presidency* (Washington, D.C.: Center for Strategic and International Studies, December 2008), 50, last accessed 2 April 2013, http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

[228] Bill proposal for the "Cybersecurity Act of 2012," last accessed 2 April 2013, http://www.wired.com/images_blogs/threatlevel/2012/02/CYBER-The-Cybersecurity-Act-of-2012-final.pdf.

Touching briefly on the EMS, the Obama Administration's 2009 *Wireless Innovation and Infrastructure Initiative* aims to provide 4G wireless access to 98 percent of Americans within 5 years (2014), while doubling wireless spectrum availability for mobile broadband, including a public safety wireless network, and enhancing research and development on mobile communications.[229] Through the *National Broadband Plan*, the Federal Communications Commission (FCC) has already begun tackling the "greatest infrastructure challenge of the 21st Century" by auctioning off large swaths of federally controlled spectrum in order to accrue the anticipated $10 billion of revenue and toward providing 100 megabytes per second connectivity to 100 million homes in the US by 2020.[230]

Although the scope, mandates and structures of the US differs from their Canadian counterparts, it is essential for a military operational commander to have an appreciation of the considerations that could ultimately affect continental operations.

US Department of Defense (DoD)

With over 15,000 networks and over 90,000 people supporting it, US DoD's global IT infrastructure provides everything from logistics, administration and global C4ISR. This lucrative target has been the target of well over 100 foreign intelligence agencies and many more individuals and non-state actors.[231]The gargantuan task of securing the networks has been the purview of service level organizations in the US

---

[229] US White House, "President Obama Details Plan to Win the Future through Expanded Wireless Access," February 10, 2011, last accessed 2 April 2013. http://www.whitehouse.gov/the-press-office/2011/02/10/president-obama-details-plan-win-future-through-expanded-wireless-access.

[230] FCC is aiming to provide 300MHz of spectrum by 2015 with a total of 500MHz by 2020. Federal Communications Commission. *Connecting America: The National Broadband Plan*. March 2010, last accessed 2 April 2013, http://www.broadband.gov/download-plan/.

[231] Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy,". . . , 99.

Army, Navy, Air Force and Marine Corps and the US Defence Information Services Agency (DISA).[232] In May 2010, US Cyber Command (CYBERCOM) was stood up as a sub-unified command under US Strategic Command, in order to protect DoD networks, provide accountability from the commander-in-chief (the President) through individual military units, and work with US Government and allied governments to share threat information and address vulnerabilities.[233] Due to the prominence of cyber threats and vulnerabilities in the DoD, some proponents argue that CYBERCOM should grow to a full Combatant Command, in order to provide:

- unity of command and effort;
- synchronization across the Services and other Combatant Commands;
- exclusive authority and responsibility to mass effects;
- emphasis on the offensive form of cyberspace operations; and
- a more diverse mission focus (potentially on behalf of the entire government and the nation at large, instead of just DoD).[234]

Since its inception, there has been hope that CYBERCOM would reduce interdepartmental friction, and repair broken processes, and be empowered, and in turn empower others, to meet its mission. It is still too early to tell on how well the new

---

[232] US Service level cyber formations under operational control of US Cyber Command include: US Army Cyber Command/2nd Army, see US Cyber Command, "Army Cyber Command/2nd Army," last accessed 2 April 2013, http://www.arcyber.army.mil/index.html; US Air Forces 24th Air Force, see Air Force Cyber/24th Air Force, "24th Air Force Fact Sheet," last accessed 2 April 2013, http://www.24af.af.mil/library/factsheets/factsheet.asp?id=15663; and US Fleet Cyber Command, see US Fleet Cyber Command/US 10th Fleet, see US Navy, "Navy Stands Up Fleet Cyber Command, Reestablishes US 10th Fleet,", last accessed 2 April 2013, http://www.navy.mil/submit/display.asp?story_id=50954; US Strategic Command, "US Cyber Command (Fact Sheet)," last accessed 2 April 2013, http://www.stratcom.mil/factsheets/cyber_command/.

[233] Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy,". . . , 102.

[234] David M. Hollis, "US CYBERCOM: The Need for a Combatant Command versus a Subunified Command," *Joint Forces Quarterly* 58 (3rd Quarter 2010): 49-53.

command is effectively doing, however key areas appear to be wanting – such as setting priorities between defending the networks versus its perceived offensive information operations responsibilities.[235] As an example, for a joint force commander (JFC) operating under US Code Title 10 and who is normally authorized to collect intelligence for the purposes of operational preparation of the environment and targeting purposes, must, due to legal concerns of cyberspace, send their collection requirements to Title 50 authorities (i.e. NSA). Yet, due to limited resources, these Title 50 agencies are usually not able to meet the JFCs' intelligence requirements, leaving JFCs unable to take advantage of cyberspace.[236] Consequently (and relative to the hypothetical scenario in this paper's Introduction), US JFCs are more likely to revert to dropping a bomb on an adversary than conduct any action within cyberspace due to these impracticalities. Moreover, rules of engagement are being staffed within DoD in order to provide guidance to the DoD "Cyber Force" in how to defend their networks.[237] One dissenting article opined that there is still significant work to be done in achieving consensus between DoD's Chief Information Officer and CYBERCOM regarding network security accountabilities, and that the tenuous new organizational structure continues to struggle between being a "single, ubiquitous, centrally managed entity [and] a distributed network conjoined through diffuse pockets of geographic responsibility [through Combatant Commands]."[238] As CYBERCOM is still maturing as a new command, this should not

---

[235]Wesley R. Andrues, "What U.S. Cyber Command Must Do," *Joint Forces Quarterly* 59 (4th Quarter 2010): 115-116.

[236] Rosemary M. Carter, Brent Feick, and Roy C. Undersander, "Offensive Cyber for the Joint Force Commander: It's Not That Different," *Joint Forces Quarterly* 66 (3rd Quarter 2012): 23-25.

[237] Donna Miles, "Doctrine to Establish Rules of Engagement Against Cyber Attack," October 20, 2011, last accessed 2 April 2013, http://www.defense.gov/news/newsarticle.aspx?id=65739.

[238] Andrues, "What U.S. Cyber Command Must Do". . . , 116-118.

detract the CF from considering further consolidation and centralization of its limited capabilities into a single "unified" organizational entity akin to CYBERCOM.

Regarding the EMS, DISA's Joint Spectrum Centre, under the Defense Spectrum Organization (DSO), "conducts global operations using background data from DoD, civilian, and allied emitters." Working on the shrinking EMS problem, DSO, in conjunction with NATO and the National Telecommunications and Information Administration (NTIA), has created software tools to reuse spectrum that is available to other federal agencies and to allies through foreign military sales.[239] In accordance with new JEMSO doctrine, each of the Services coordinates its spectrum requirements through the centralized DSO, yet Combatant Commanders are responsible for establishing their own Joint Frequency Management Office (JFMO) or Joint Spectrum Management Element (JSME) and issuing their own guidance related to Joint EMS management operations pertinent to their geographical requirements.[240] As the CF's de facto "combatant command", CJOC would benefit from establishing a similar JFMO organization that could coordinate the JEMSO requirements for Canadian operations. As indicated in Chapter 4, ADM(IM) has a sub-directorate that performs a function similar to that of DISA's DSO.

In order to conduct operational testing and permit simulation training, the Defense Advanced Research Projects Agency (DARPA) is creating the National Cyber Range (NCR).[241] As a not-so-secretive project, the NCR is a collection of testbeds that will

---

[239] Sokolow and Leed, *Seizing the Wireless Advantage . . .*, 12.

[240] Joint EMS management operations include: spectrum management, frequency management, joint spectrum interference resolution , and host nation coordination. US DoD, JP 6-1. *Joint Electromagnetic Spectrum Management Operations . . .*, IV-3.

[241] Defense Advanced Research Projects Agency (DARPA), "National Cyber Range Rapidly Emulates Complex Networks," last accessed 2 April 2013, http://www.darpa.mil/NewsEvents/Releases/2012/11/13.aspx.

allow the testing of test new network protocols, satellite and radio frequency (RF) communications and mobile tactical and maritime communications for DoD and other government departments and agencies. Once enabled, this capability would be very beneficial to close allies, such as the CF.

NATO

As a member of the Alliance, the CF must consider the collective actions of the NATO, and those of its constituent member nations, in the E/CE. As briefly mentioned in Chapter 3, NATO's consensus on the definition of a cyber-attack will weigh heavily into future deterrence options and the actions that NATO members will be able to conduct in the E/CE as part of NATO Article 5 collective defence. As a troop contributing nation, the CF must ensure that its actions are consistent with what NATO undertakes in the E/CE in order to posture itself to contribute to the alliance in peace and in order to interoperate with deployed coalition organizations led by NATO or a subset thereof. As described below, the CF, and in particular a CJOC EM/Cyber organization, should come to appreciate and to contribute to NATO policy and doctrine development. Moreover, CJOC should consider participating directly in the newest NATO EM/Cyber organizations such as the Cooperative Cyber Defence Centre of Excellence (CCD COE) in Tallinn, Estonia and/or the NATO Computer Incident Response Capability (NCIRC), which falls under the auspices of the NATO Communications and Information (NCI) Agency.

At the 2010 Lisbon Summit, by recognizing the increasing frequency and sophistication of cyber threats, the Council member governments collectively declared the importance of the E/CE:

> In order to ensure NATO's permanent and unfettered access to cyberspace and integrity of its critical systems, we will take into account the cyber dimension of modern conflicts in NATO's doctrine and improve its capabilities to detect, assess, prevent, defend and recover in case of a cyber attack against systems of critical importance to the Alliance.[242]

In addition to noting the threat to member governments, supply, transportation and other critical infrastructure, the Alliance also noted the significant trends in EW, lasers and other technologies that could affect their access to space-based assets, thus potentially impacting global operations.[243] Under the banner of "Defence and Deterrence", NATO's latest Strategic Concept (2010) intended to "develop further our ability to prevent, detect, defend against and recover from cyber-attacks, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities."[244]

In May 2008, NATO created the CCD COE to integrate NATO cyber awareness, research and training with member nations.[245] Accredited by NATO as an International Military Organization in October 2008, the CCD COE includes sponsors from Estonia, Latvia, Lithuania, Germany, Hungary, Italy, Poland, Slovakia, Spain, the Netherlands and

---

[242] NATO, "Lisbon Summit Declaration," November 20, 2010, last accessed 2 April 2013, http://www.nato.int/cps/en/natolive/official_texts_68828.htm#cyber.

[243] NATO, *Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization* (Brussels: NATO Public Diplomacy Division, 20 November 2010), 11-12, last accessed 2 April 2013, http://www.nato.int/nato_static/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf.

[244] *Ibid*., 16-17.

[245] NATO created the CCD COE based on the lessons emanating from the cyber attacks on Estonia in May 2007. NATO, "Strengthening Cyber Security" In *NATO Briefing: Tackling New Security Challenges*, 31 January 2012, 10-11, last accessed 2 April 2013, http://www.nato.int/nato_static/assets/pdf/pdf_publications/20120116_new-security-challenges-e.pdf; and NATO CCD COE, "Cyber Defence," last accessed 2 April 2013, http://www.ccdcoe.org/2.html.

US, with the UK and France announcing intentions to participate in 2013.[246] The CCD COEs Annual International Conference on Cyber Conflict (also known as "CyCon") provides a plethora of literature on the latest commentary regarding cyber conflict, legal considerations, theories, policies and the like.[247] The CF, and particularly a CJOC entity dealing with E/CE, would benefit significantly from participating at this forum.

The NCIRC, which currently provides cyber protection to NATO centralized bodies, anticipates having full operational status in 2013 with the implementation of its Rapid Reaction Teams (RRT) that will assist member states that are experiencing an attack of national significance.[248] The NCIRC Coordination Centre, with its co-located Cyber Threat Assessment Cell (CTAC), is responsible for coordination of cyber defence activities within NATO and with member nations, staff support to the Cyber Defence Management Board (CDMB), the planning for the Annual "Cyber Coalition" Exercise and cyber defence liaison with European Union entities and the United Nations and International Telecommunications Union (ITU).[249] NATO's primary focus, under the *NATO Policy on Cyber Defence*, is on the "protection of its own communication and information systems" with objectives to "integrate cyber defence into national defence frameworks" and to "develop minimum requirements for those national networks that are

---

[246] As an International Military Organization, the CCD COE is not an operational entity of NATO. NATO CCD COE, "Institutional Status," last accessed 2 April 2013, http://www.ccdcoe.org/38.html.

[247] NATO CCD COE, "CyCon," last accessed 2 April 2013, http://ccdcoe.org/362.html and http://ccdcoe.org/363.htm.

[248] Originally initiated as phase 1 of a three-phase Cyber Defence Programme at the 2002 Prague Summit, the NCIRC completed phase 2 when it became fully operational in 2012. In Phase 3, the RRTs will deploy as endorsed by the NATO Cyber Defence Management Board (CDMB) to help eliminate or mitigate future attacks on a nation state (if a bi-lateral MoU is in place), or to a non-NATO state if approved by the North Atlantic Council (NAC). NATO, "NATO Rapid Reaction Team to fight cyber attack," 31 March 2012, last accessed 2 April 2013, http://www.nato.int/cps/en/natolive/news_85161.htm.

[249] NATO, "NATO and cyber defence," last accessed 2 April 2013, http://www.nato.int/cps/en/natolive/topics_78170.htm.

connected to or process NATO information."[250] CJOC will be required to integrate CF requirements into the NATO Defence Planning Process (NDPP), which will be used to integrate and prioritize relevant cyber defence requirements.[251] In addition to the aforementioned NATO activities in the E/CE, the *NATO 2020* Experts Group recommended that, "Over time, NATO should plan to mount a fully adequate array of cyber defence capabilities, including passive and active elements" and NATO should be "developing an array of cyber defence capabilities aimed at effective detection and deterrence."[252] The author suspects that these recommendations are already being addressed under the classified and constantly updated NATO *Action Plan on Cyber Defence*.[253]

The Other Five-Eyes Nations

Despite the contemplations in the E/CE by the US and NATO, the CF would likely gain more from the approaches considered by the other Five-Eyes nations when it comes to doctrinal, policy or structural considerations. The intelligence sharing partnership that the CF enjoys with its United Kingdom (UK), Australia and New Zealand (NZ) and US allies, which grew out of the Second World War, has only been strengthened when dealing with the common threats posed in the E/CE.[254] As the sheer size of the US military is beyond the scope and capabilities of the other Five-Eyes

[250]NATO, *Defending the networks: The NATO Policy on Cyber Defence* (Brussels: NATO Public Diplomacy Division, 4 October 2011), last accessed 2 April 2013, http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf.

[251] *Ibid.*

[252] NATO. *NATO 2020: Assured Security; Dynamic Engagement* . . . , 11, 45.

[253] The Action Plan is mentioned as part of the Policy document. See NATO, *Defending the networks: The NATO Policy on Cyber Defence.*

[254] National Security Agency, "Declassified UKUSA Signals Intelligence Agreement," last accessed 2 April 2003, http://www.nsa.gov/public_info/press_room/2010/ukusa.shtml.

nations, the CF has traditionally turned to the Australian and the NZ defence forces for examples in how to handle new challenges. Although there is little unclassified information publically available specific to defence and military strategies and policies in these nations (see Appendix 7), except as disclosed above for the US, CF operational commanders should be comfortable that the CF approach to confronting the issues in the E/CE is consistent with those of the UK, Australia and NZ. More importantly, the CF's military actors should be able to share and leverage information and expertise from these international partners whilst conducting its own operations.

United Kingdom

The UK has acknowledged the importance of the E/CE as two separate elements of the operating environment, by including cyberspace in the information dimension and a separate electromagnetic dimension.[255] In addition to the common threat trends and operational considerations (discussed in Chapters 2 and 3), the UK Ministry of Defence has similarly recognized cyber-security as a significant hot topic issue to their future operating environment, with "attribution, intent and legitimacy of cyber-attacks *will* all be disputed."[256] In dealing with the non-traditional threats posed by the E/CE, UK joint doctrine also acknowledges that they need to adopt cyber operations responses that are likely new and have yet to be developed.[257] The UK Army doctrine also refers to "cyber power" as an important objective to ensure land-based elements' freedom of manoeuvre whilst defending against attack. [258] Moreover, UK's analysis of the E/CE is that it will become increasingly more congested, cluttered, and congested as the physical, cognitive and virtual aspects become increasingly more interconnected.[259] To confront the

---

[255]Much of the high order joint UK doctrine and concept publication describe the operating environment in terms of dimensions of land, air, sea, space, information (including cyberspace), electromagnetic and time. UK Ministry of Defence (MoD). *Joint Doctrine Publication 0-01: British Defence Doctrine, 4th Edition* (Shrivenham, U.K.: Development, Concepts and Doctrine Centre (DCDC), November 2011), 2-13 (para 229). https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/33697/20111130jdp001_bdd_Ed4.pdf

[256] Italics in orginal. UK MoD, *Global Strategic Trends – Out to 2040*, 4th Edition (Shrivenham, U.K.: Development, Concepts and Doctrine Centre, 2010), 17, 150-151. https://www.gov.uk/government/publications/dcdc-global-strategic-trends-programme-global-strategic-trends-out-to-2040.

[257] UK MoD, *Strategic Trends Programme: Future Character of Conflict* (Shrivenham, U.K.: Development, Concepts and Doctrine Centre, February 2010), 13. http://webarchive.nationalarchives.gov.uk/20121026065214/http://www.mod.uk/NR/rdonlyres/A05C6EB5-5E8F-4115-8CD6-7DCA3D5BA5C6/0/FCOCReadactedFinalWeb.pdf.

[258] "Cyber Power" is defined as "The ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power. From Joint Doctrinal Note 4/11, as cited in U.K. MoD, *Joint Concept Note 2-12: Future Land Operating Environment* (Shrivenham, U.K.: DCDC, May 2012), Lexicon-1. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/33688/20120829jcn2_12_floc_u.pdf.

[259] UK MoD, *Strategic Trends Programme: Future Character of Conflict* . . ., 21-23.

increased cyber threats to its own critical infrastructure, recognized as Tier 1 threats in its *National Security Strategy*, the UK government invested into the Cyber Security Operations Centre (CSOC), located at the UK's cryptologic intelligence agency, Government Communications Headquarters (GCHQ), and the Office of Cyber Security & Information Assurance (OCSIA) in the Cabinet Office.[260] Specific to the Ministry of Defence and the UK's military forces, the UK government initiated the creation of the Defence Cyber Operations Group (DCOG) under Joint Forces Command / Permanent Joint Headquarters (JFC/PJHQ), with operational readiness expected by 2015.[261] The proposed DCOG is a "federation of cyber units across defence" with the following proposed mission:

> . . . to mainstream cyber security throughout the [Ministry of Defence] MOD and ensure the coherent integration of cyber activities across the spectrum of defence operations. This will give MOD a significantly more focussed approach to cyber, by ensuring the resilience of our vital networks and by placing cyber at the heart of defence operations, doctrine and training. We will also work to develop, test and validate the use of cyber capabilities as a potentially more effective and affordable way of achieving our national security objectives.[262]

---

[260] The UK National Security Council included "Hostile attacks upon UK cyberspace by other states and organized crime" amongst four of its highest priority risks. Government of the United Kingdom, *A Strong Britain in an Age of Uncertainty: The National Security Strategy* (London, UK: Cabinet Stationery Office, October 2010), 11, 27. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf; and Government of the United Kingdom, *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world* (London, UK: Cabinet Stationery Office, November 2011), 25. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

[261] Government of the United Kingdom, "hc 106 Defence and Cyber-security – Session 2012-13," 18 April 2012 (prepared 9 May 2012), last accessed 2 April 2013, http://www.publications.parliament.uk/pa/cm201213/cmselect/cmdfence/writev/106/m01a.htm

[262] UK MoD, "Defence Cyber Operations Group," slide 10, last accessed 2 April 2013, http://www.google.ca/url?sa=t&rct=j&q=defence%20cyber%20operations%20group&source=web&cd=2&ved=0CDoQFjAB&url=http%3A%2F%2Fwww.science.mod.uk%2Fcontrols%2Fgetpdf.pdf%3F606&ei=JQ_zUJHMBqbc2QWo-oCwBA&usg=AFQjCNHy4kB9a-T6IlEVKybfV_HxZHHnDA&bvm=bv.1357700187,d.b2I.

Separate, but related, the UK has created Joint Cyber Units (JCUs) at Corsham and Cheltenham (co-located within GCHQ) with respective responsibilities to defend MoD's networks and "by 2015 and will have the role of developing new tactics, techniques and plans to deliver military effects, including enhanced security, through operations in cyberspace."[263] This latter mission for JCU Cheltenham has implied to many observers the likely creation of an offensive cyber capability. This cannot be confirmed in the unclassified literature that is available. In addition to the DCOG and JCUs, the UK *Cyber Security Strategy's* includes plans to employ reservists who possess specialist skills and expertise to augment the JCUs.[264] From the above proposed mission statement, it appears that the DCOG is similar to the organization proposed by this paper for CJOC. As PJHQ is the UK's equivalent of the CF's CJOC, any lessons garnered from the stand-up of the DCOG will be fruitful for any created CJOC subordinate E/CE organization.

Australia

In a similar manner to the UK, the Australian government recognized the threats identified within their own *Cyber Security Strategy*, to create the Computer Emergency Response Team (CERT) under the Attorney General's Department and a Cyber Security Operations Centre (CSOC) as part of their the Defence Signals Directorate (DSD) intelligence organization.[265] The CSOC encompasses representation from the Australian

---

[263] Government of the United Kingdom, "hc 106 Defence and Cyber-security – Session 2012-13," 18 April 2012 (prepared 9 May 2012), last accessed 2 April 2013, http://www.publications.parliament.uk/pa/cm201213/cmselect/cmdfence/writev/106/m01a.htm

[264] Government of the United Kingdom, *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world . . .* , 27.

[265] Australian Government, *Cyber Security Strategy* (Canberra: Attorney General's Department, 2009), vii. http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf; and, Australia Department of Defence, "Cyber Security Operations Centre," last accessed 2 April 2013, http://www.dsd.gov.au/infosec/csoc.htm.

Defence Force, the Defence Intelligence Organization, the Defence Science and Technology Organization and other national security and intelligence agencies. In January 2013, the Australian Prime Minister announced their government's latest *National Security Strategy*, which initiated the process to create an integrated cyber policy within the next five years that will "enhance the defence of [Australia's] digital networks."[266] Moreover, the *National Security Strategy* announced the creation of an Australian Cyber Security Centre (ACSC) that will consolidate the CSOC, the CERT, and other cyber-based organizations. Accordingly, the new ACSC will be responsible for "developing sophisticated capabilities to maximise Australia's strategic capacity and reach in cyberspace, giving the Government the ability to detect, deter and deny offshore malicious cyber actors targeting Australia."[267] An organization similar to CSOC, or the new ACSC, is another example worth following for consideration by the Canadian CJOC, and perhaps in concert with Public Safety Canada's CCIRC.

New Zealand

Following on the heels of the UK and Australia is New Zealand's response. Commensurate with the other Commonwealth nations in the Five-Eyes partnership, the *New Zealand Cyber Security Strategy* also acknowledged the growing cyber threat to its critical infrastructure and national security, and established a National Cyber Security Centre (NCSC) as part of its intelligence agency, the Government Communications

---

[266] Australian Government. *Strong and Secure: A Strategy for Australia's National Security* (Canberra, AS: Department of the Prime Minister and Cabinet, 2013), 40. http://www.dpmc.gov.au/national_security/docs/national_security_strategy.pdf.

[267] *Ibid.*; and Australia DoD. "Australian cyber security centre to be established," last accessed 2 April 2013, http://www.defence.gov.au/defencenews/stories/2013/jan/0124.htm.

Security Bureau (GCSB).[268] The key role of the NCSC is to "build on existing cyber security and information assurance capabilities to provide enhanced protection of government systems and information against advanced and persistent threats…and enhance cyber security practices within government agencies."[269] A noticeable difference in the NZ strategy is that the NCSC will absorb responsibilities currently inherent to the NZ Centre for Critical Infrastructure Protection (CCIP).[270] The NZ Ministry of Defence (NZ MoD) and the NZ Defence Force (NZDF) are separate organizations. In its 2010 Defence White Paper, the MoD acknowledges that "If New Zealand does not keep up with the pace of change in this area there is a risk that we could become a weak link in the shared effort to deter hostile cyber intrusions."[271] This is the only significant reference to cyber security or defence activities by either the MoD or the NZDF in unclassified published documents. Due its small size, at under 10,000 regular force personnel, the NZDF will leverage the "whole of government" coordinated action through the NCSC. There is no identified separate NZDF organization identified to pursue operational level military cyber capabilities.[272]

National Comparison and Chapter Summary

[268] New Zealand Government, *New Zealand Cyber Security Strategy*, 7 June 2011, 8. http://www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-strategy-june-2011_0.pdf.

[269] *Ibid.*

[270] *Ibid.*, 9.

[271] New Zealand Government. *New Zealand Defence White Paper 2010* (Wellington, NZ: NZ Ministry of Defence, November 2010), 25. http://www.defence.govt.nz/pdfs/defence-review-2009-defence-white-paper-final.pdf.

[272] Cyber is mentioned only once in the Statement of Intent (business plan) for the NZ forces for 2011-2014. New Zealand Defence Force, *New Zealand Defence Force Statement of Intent 2011-2014* (Wellington, NZ: NZ Defence Force, 2010), 12. http://www.nzdf.mil.nz/downloads/pdf/public-docs/2011/soi/nzdf-soi-2011-14.pdf.

From the strategies and policies that are available in the unclassified domain, it appears that Canada's principal allies in NATO and the other Five-Eyes Nations have all similarly acknowledged the scope and importance of the cyber threat to their national (or alliance) security and critical infrastructure. Most of the allies reviewed here have created policies that explicitly mandate that their own military forces are solely responsible for defending their own systems, leaving other government entities to be the lead in defending the government's networks. The NATO Alliance has similarly instituted the NCIRC as the principal organization to defend NATO operational networks, the networks of central NATO agencies, and provide a means of assisting member nations that experience an attack. Through the NATO CCD CoE, there is also the potential to leverage leading edge technologies, techniques and procedures for the benefit of all its membership. In order to permit CF interoperability on Alliance operations and for defending Canadian sovereignty, CJOC would likely gain from an exchange or a liaison position within the NCIRC and/or CCD CoE. Furthermore, the Annual Cyber Conference provides a venue to leverage cyber-related response tactics, techniques and procedures and acquire information regarding leading edge concepts and issues regarding the E/CE.

Allied nations differentiate themselves in how they have organized to respond to cyber threats. In the UK, Australia and NZ, the principal signals intelligence and information technology agencies of GCHQ, DSD, and GCSB have nested integral "Cyber Centres" to defend government networks. With the exception of the UK's DCOG, these "Cyber Centres" also coordinate and defend the networks of their respective MoDs and those of their military forces. On the other hand, the US splits responsibilities between the NSA and DHS. While NSA provides technical information technology advice and

signal intelligence support across US government, DHS is the lead department for coordinating cyber-related domestic response, with the perspective that most cyber-attacks are generally viewed as a criminal activity. The creation of US CYBERCOM was deemed necessary to coordinate DoD's expanding appetite in the "cyber domain" under a single unified command organization with operational control of the Service-level entities (e.g. 10th Fleet, 24th Air Force and 2nd Army, etc.) exercised through it. The proposed UK DCOG, under the operational-level PJHQ/JFC, anticipates centralizing military cyber response capabilities under a single operational commander by 2015. The lessons from this creation should clinch CJOC's interest as a potential example to be explored. Similar to the US, CSEC is Canada's lead agency for advising government departments, in concert with Public Safety's CCIRC (as discussed in Chapter 4) regarding cyber related activities. As there is no single Canadian "Cyber Centre" that coordinates as the hub of government's response to a cyber-attack affecting across government, the CF must coordinate any response to cyber threats by its forces with both PSC and CSEC.

This chapter reviewed what Canada's closes allies are doing in the E/CE in order to understand the policies and strategies as well as the organizations created to confront the increasing threat. Commander CJOC must be aware of these peripheral considerations by its closest allies such that CF deployed forces are interoperable and such that their capabilities can be leveraged. By the comparison above, the CF's part in overall government cyber strategy appears to be in line with approaches taken by its allies. In the meantime, CJOC should exploit opportunities such as participation in the NATO CCD COE, liaison and exchange within US CYBERCOM, and/or the US Service-level Cyber entities, or the UK DCOG as priority. As this review was based on available unclassified

literature, it is very likely that a review of classified documentation could yield a significantly different perspective.

CHAPTER 6 - CONCLUSION

This paper argued that it is essential that an operational-level CF commander, such as the new Canadian Joint Operational Command and its deployed task force commanders, to have the staff and subordinate resources to work effectively with all of the actors at home or abroad to counter the increasing number and sophistication of threats in the E/CE. Whether it is for self-preservation in a defensive role against a myriad of threats and potential adversaries, or in the consideration of offensive operations in either the EMS or cyberspace, the CF must invest heavily in transforming itself to integrate the effects desired in the E/CE. Despite its limited current role within *Canada's Cyber Security Strategy*, the CJOC, operating under the missions of the *Canada First Defence Strategy*, must begin posturing itself to respond with appropriate offensive and defensive contingencies in the E/CE.

The inexpensive commercially available and emerging technologies of the E/CE provide a multitude of ways and means for potential adversaries to threaten Canadians and its military forces. With the ability to launch an attack from anywhere around the world with no attribution, it is extremely difficult for the government and the CF to prepare against threats that ranging from stealing personal information to physically destroying critical infrastructure. The continuum of national risk varying from individuals, to transnational terrorist networks and criminal organizations, to the most dangerous and likely involving nation-state foreign military and intelligence agencies, demonstrate that the CF must work diligently with allies and national security actors. In addition, experts expect that an already congested EMS will rise to a national level of significance on par with the buzz surrounding all things 'cyber." As the demand for

spectrum space continues to rise exponentially, finding alternative supply will be a challenge for regulators and innovators. To unify focus of military force developers and force generators towards supporting their principal force employer (CJOC), to confront these threats, it was recommended to recognize the convergence of technologies between both the EMS and the technical aspects of the "Cyber domain" into a combined "EM/Cyber environment" (E/CE). Moreover, Commander CJOC will need to take a comprehensive, integrated, adaptive, and networked approach to the E/CE that leverages all available capability.

Looking at the operational planning considerations in the E/CE of the "operational functions" it was clear that military operations are dependent on the availability of the E/CE. It was similarly evident that the capabilities in the E/CE are reciprocally dependent on each "function." The complexity of the E/CE considerations with respect to these "operational functions" argued that CJOC requires a dedicated organization to focus the planning and execution of operations in the E/CE. Based on the inter-relationships amongst the E/CE-related disciplines of CIS, EW, SIGINT and CNO, it was determined that considerably synergy could be leveraged by a collective subordinate organization under Commander CJOC that encompasses expertise from all of these disciplines. Lastly, the problems associated with deterrence and offensive operations highlighted that militaries around the world are still wrestling with legal aspects surrounding operations within the E/CE. Despite an increasing number of case studies regarding cyber-attacks, militaries are diligently working to develop a shared legal framework for how to recognize and then escalate a response to a hostile intent or act within cyberspace. Although the Government of Canada has yet to task publicly the

CF with a particular role in conducting offensive cyber-attacks, CJOC needs to consider including legal and other subject matter experts within a dedicated subordinate E/CE organization to liaise with others and to discern amongst the legal and other planning considerations required for operations within the E/CE.

Although CJOC sees itself primarily in a supporting role with other government actors, it must also be prepared to take the lead as contingencies or situations require it to do so. Under the government's six core *CFDS* missions, Commander CJOC becomes the de facto principal commander, with subordinated component commands and task forces ready for force employment. Recognizing that each of these missions requires the ability to conduct operations in the E/CE, a review of the E/CE-related occupations and units of the CA, RCAF, and RCN illustrated that CJOC operations at the operational level will need to leverage the capabilities and expertise diffused amongst other strategic and tactical level organizations. Due to their already existing relationships in the E/CE disciplines of CIS, CNO, EW, and SIGINT, DGIMO and CFIOG appear to be the entities most logically postured to support CJOC directly in the E/CE and should be considered for a future direct supporting relationship. By reviewing the roles of OGD actors and industry, it was demonstrated that the CF contributes to and benefits from the overall EM/Cyber critical infrastructure risk management processes in conjunction with other government security actors such as PSC, CSEC, RCMP and CSIS. Based on the national authorities and responsibilities of CSEC, IC (and CRTC), SSC and PSC for the conduct of daily operations within the E/CE, it was determined that CJOC must reinforce the relationships with these organizations through a single operational-level E/CE organization to leverage capabilities and expertise when required.

Finally, it was determined that the CF's part in overall government cyber strategy appears to be in line with approaches taken by its closest allies in the Five-Eyes and NATO. Commander CJOC must remain aware of the E/CE considerations by its closest allies such that CF deployed forces can be interoperable and that allied capabilities can be leveraged when necessary. CJOC should also exploit opportunities such as participation in the NATO CCD COE, liaison and exchange within US CYBERCOM, and/or the US Service-level Cyber entities, or the UK DCOG.

As this paper was written based primarily on unclassified literature inclusive of the latest available doctrine, opinions expressed in trade journals and published government policies, it is very likely that a review of classified documentation could yield a significantly different perspective. Further, it would be advantageous to studying the long-term benefit of not only re-rolling existing occupations and organizations, but also in expanding the resources dedicated to the E/CE, pending the lifting of fiscal and human resource constraints.

Appendix 1

List of Acronyms

Acronym	Meaning
21 EW Regt	21 Electronic Warfare Regiment
76 Comm Gp	76 Communication Group
8 ACCS	8 Air Command and Control Squadron
ACC	Air Component Command
ACIS	Army Communications and Information Systems Specialist (includes operators, technicians, line specialists)
ACSC	Australian Cyber Security Centre
ADF	Australian Defence Force
ADM(IM)	Assistant Deputy Ministry (Information Management)
ADM(Mat)	Assistant Deputy Ministry (Materiel)
ADM(S&T)	Assistant Deputy Ministry (Science & Technology)
AESOps	Airborne Electronic Sensor Operators
APT	advanced persistent threats
ARIN	American Registry for Internet Numbers
ATESS	Aerospace and Telecommunication Engineering Support Squadron
ATIS	Aerospace Telecommunications and Information Systems Technician
C2IS	command and control information systems
C4ISR	Command and Control, Communications, Computer, Intelligence, Sensors, Reconnaissance
CA	Canadian Army
CanadaCOM	Canada Command (pre-CJOC)
CANOSCOM	Canadian Operational Support Command (pre-CJOC)
CANSOFCOM	Canadian Special Operations Forces Command
CCD COE	Cooperative Cyber Defence Centre of Excellence (NATO)
CCEB	Combined Communications Electronics Board (Five-Eyes)
CCIRC	Canadian Cyber Incident Response Centre
CDI	Chief Defence Intelligence
CDMB	Cyber Defence Management Board
CDS	Chief of Defence Staff
CEFCOM	Canadian Expeditionary Forces Command (pre-CJOC)
CELE(A)	Communications and Electronics Engineer (Air)
CERT	Computer Emergency Response Team (Australia)
CF	Canadian Forces
CFCMU	CF Cryptologic Maintenance Unit
CFCSU	CF Cryptologic Support Unit
CFD	Chief of Force Development

Acronym	Meaning
CFDS	*Canada First Defence Strategy*
CFEWC	CF Electronic Warfare Centre
CFEWDB	CF Electronic Warfare Database
CFIOG	CF Information Operations Group (includes CFNOC, CFEWC and CFS Leitrim)
CFJOSG	CF Joint Operational Support Group
CFJSR	CF Joint Signal Regiment
CFNOC	CF Network Operations Centre
CFS	CF Station (e.g. CFS Leitrim)
CFSSG	CF Shared Services Group (under ADM(IM))
C-IED	Counter-Improvised Explosive Device
CIS	Communications and Information Systems
CJIATF	Combined Joint Inter-Agency Task Force
CJOC	Canadian Joint Operations Command
CMBG Sig Sqn	Canadian Mechanized Brigade Group Signal Squadron
CNA	computer network attack
CND	computer network defence
CNE	computer network exploitation
CNO	computer network operations (comprised of CND, CNE and CNA)
COMINT	communications intelligence (component of SIGINT)
Comm Rsch	Communicator Research Operator
CRTC	Canadian Radio-television and Telecommunications Commission
CSEC	Communication Security Establishment Canada
CSIS	Canadian Security Intelligence Service
CSMC	Combined Spectrum Management Cell
CSNI	Classified Secure Network Infrastructure
CSOC	Cyber Security Operations Centre (Australia and UK)
CTAC	Cyber Threat Assessment Cell (with NCIRC)
CYBERCOM	Cyber Command (US)
DARPA	Defense Advanced Research Projects Agency (US)
DCOG	Defence Cyber Operations Group (UK)
DG	Director General (i.e. DG Cyber or DG Space)
DGIMO	Director General Information Management Operations (division under ADM(IM)
DHS	Department of Homeland Security (US)
DISA	Defense Information Systems Organization (US)
DM	Deputy Minister (of Defence)
DND	Department of National Defence

Acronym	Meaning
DNI	Director of National Intelligence (US)
DoD	Department of Defense (US)
DRDC	Defence Research Development Canada
DSD	Defence Signals Directorate (Australia)
DSO	Defense Spectrum Organization (US)
DWAN	Defence Wide Area Network
EA	electronic attack
E/CE	Electromagnetic spectrum/Cyber Environment
ELINT	electronic intelligence (component of SIGINT)
EME	electromagnetic environment
EMP	electromagnetic pulse
EMS	electromagnetic spectrum
EMSO	electromagnetic spectrum operations
EO/IR	electro-optical / infrared
EP	electronic protection
ES	electronic warfare support
EW	electronic warfare (includes three divisions EA, EP and ES)
EWCC	Electronic Warfare Coordination Centre
EWOS	Electronic Warfare Operational Support
FCC	Federal Communications Commission (US)
FERP	*Federal Emergency Response Plan*
Five-Eyes	United States, United Kingdom, Canada, Australia and New Zealand
GC	Government of Canada
GCHQ	Government Communications Headquarters (UK
GC IT IMP	*Government of Canada Information Technology Incident Management Plan*
GCSB	Government Communications Security Bureau (NZ)
GOC	Government Operations Centre
GPS	Global Positioning System
GSM	General Subscriber Mobile
IANA	Internet Assigned Number Authority
IC	Industry Canada
ICC	*Integrated Capstone Concept*
ICS	industry control system(s)
IEEE	Institute of Electrical and Electronic Engineers
IO	information operations
IP	Internet Protocol
ISAC	Information Sharing Analysis Centers (US)
ISR	Intelligence, Surveillance, Reconnaissance

Acronym	Meaning
ISTAR	Intelligence, Surveillance, Target Acquisition and Reconnaissance
IT	information technology
ITU	International Telecommunications Union (UN)
JCOT	Joint Cyber Operations Team
JCU	Joint Cyber Unit (UK)
JEMSOCC	Joint Electromagnetic Spectrum Operations Coordination Centre – term used in CJIATF Force Employment Concept for an entity that coordinates EW, SIGINT, and CNO for Commander CJIATF.
JFC	Joint Forces Commander (US)
JFMO	Joint Frequency Management Organization (US)
JIMP	Joint Inter-agency Multinational Public
JOINTEX	Joint Exercise
JSME	Joint Spectrum Management Element (used in US doctrine)
JTF	joint task force
LISS	Land Integrated Support Section (under Army Directorate of Land Integration)
MCC	Maritime Component Command
MoD	Ministry of Defence (applies UK, Australia, NZ)
NATO	North Atlantic Treaty Organization
NCCIC	National Cybersecurity and Communications Integration Center (US DHS)
NCI	NATO Communications Information
NCIRC	NATO Cyber Incident Response Capability
NCIO	Naval Combat Information Operator
NCR	National Cyber Range (US)
NCSC	National Cyber Security Centre (NZ)
NCS Engr	Naval Combat Systems Engineer
NDPP	NATO Defence Planning Process
NESOp	Naval Electronic Sensor Operator
NEWC	Naval Electronic Warfare Centre (co-located with CFEWC)
NGN	next generation network
NORAD	North American Aerospace Defence (Canada/US)
NSA	National Security Agency (US)
NTIA	National Telecommunications and Information Administration (US)
NZ	New Zealand
NZDF	New Zealand Defence Force

Acronym	Meaning
OAG	Office of the Auditor General
OGDs	other government departments
OCSIA	Office of Cyber Security & Information Assurance (UK)
PJHQ/JFC	Permanent Joint Headquarters / Joint Forces Command (UK)
PNT	Positioning, Navigation and Timing (used in GPS, mobile communications, wireless computer technology, etc.)
PRICIE+G	People and Leadership; Research and Development and Operational Research, (plus Experimentation); Infrastructure, Environment, and Organization, Concepts and Doctrine; Information Management and Technology; Equipment and Support; and Generate
PSC	Public Safety Canada
RCAF	Royal Canadian Air Force
RCMP	Royal Canadian Mounted Police
RCN	Royal Canadian Navy
RF	radio frequency
RJTF	Regional Joint Task Force
ROE	rules of engagement
RRT	Rapid Response Team (within NCIRC)
SCADA	supervisory control and data acquisition
SIGS	Signals Officer
SIGINT	signals intelligence
SD	secure digital (i.e. SD cards)
SJS	Strategic Joint Staff
Sonar Op	Sonar Operator
SSC	Shared Services Canada
TBS	Treasury Board Secretariat
TNCC	Theatre Network-Operations Control Centre (from US doctrine)
TTPs	tactics, techniques and procedures
UK	United Kingdom
UN	United Nations
US	United States
USB	universal serial bus (i.e. USB memory sticks)
WTIS	Wing Telecommunication and Information System Section

Appendix 2

Cyber Threats Defined

Term	Definition	Reported Example(s) or Consequences
Botnet	A network of zombie machines used by hackers for massive coordinated system attacks.	
Denial of Service (DoS)	Employing a botnet to send massive simultaneous requests to servers prevents legitimate use of the servers.	
Digitization^	As paper records are converted to electronically stored information, data breaches are likely more possible.	Healthcare privacy compromised Retail fraud
Doppelganger Attack^	A method of mirror profiling in which information gathered on an individual is used to steal usernames and password credentials on one site for access to another site.	Dozens of Xbox Live IDs and Passwords Leaked: http://www.pcmag.com/article2/0,2817,2396083,00.asp
Infected software^	Open source and freeware commonly used by organizations is	Brazilian ISPs Hit with Large-Scale DNS Attack: http://www.securityweek.com/brazilian-isps-hit-large-scale-dns-attack

Term	Definition	Reported Example(s) or Consequences
	manipulated and posted back to the Internet for download by unsuspecting users.	
Infrastructure Attacks^	Targeting mobile towers and telecommunications, or emergency service communication. Other possibilities include air traffic control, water systems, etc.	Vulnerabilities give hackers ability to open prison cells from afar: http://arstechnica.com/business/2011/11/vulnerabilities-give-hackers-ability-to-open-prison-cells-from-afar/ Oil cyber-attacks could cost lives, Shell warns: http://www.bbc.co.uk/news/technology-16137573
Insider Threats^	Although most threats originate from unknown individuals, these threats are from those that are known to the organization.	Typically four classes of insider incidents: • Accidents • Malicious Behaviour • Pretexting (falling prey to social engineering scams) • Negligence Canadian Officer removed from military for espionage: http://www.huffingtonpost.ca/2013/02/13/jeffrey-delisle-spy-removed-canadian-military_n_2680436.html; http://www.cbc.ca/news/canada/nova-scotia/story/2013/02/08/ns-spy-faces-sentencing.html Bradley Manning leaks secret documents and messages to Wikipedia: http://www.cbc.ca/doczone/lovehatepropagandawaronterror/2012/06/bradley-manning.html Chicago Mercantile insider leaks secrets to China: http://it.slashdot.org/story/11/07/07/1756205/Chicago-Mercantile-Exchange-Secrets-Leaked-To-China
Logic bomb	Camouflaged segments of programs that destroy	Fannie Mae contractor indicted for logic bomb: http://www.informationweek.com/security/management/fannie-mae-

Term	Definition	Reported Example(s) or Consequences
	data when certain conditions are met.	contractor-indicted-for-logic/212903521 TSA worker gets 2 years for planting logic bomb in screening system: http://www.wired.com/threatlevel/2011/01/tsa-worker-malware/
Mobility Threats	Access point for hackers through a mobile device (iPad, laptop, personal communication device, etc) when connected to internal network.	Austrian ISP's wireless routers set up secret network: http://www.h-online.com/security/news/item/Austrian-ISP-s-wireless-routers-set-up-secret-network-1287652.html
Peer-to-Peer (P2P) Software^	Software commonly used for downloading illegal music, videos, movies and applications. When first installed, it scans the system and any connected systems for files to share with others on the Internet.	Used by criminals to scan for sensitive information. The hidden security risks of P2P traffic: http://threatpost.ca/en_us/blogs/hidden-security-risks-p2p-traffic-062712
Phising, Pharming, SMSishing, Vishing^	An email or electronic message sent to someone usually disguised as coming from a legitimate person or organization. It is usually accompanied with instructions such as clicking on a link, opening an attachment, etc.	Fraud Identify theft Data breaches Governments, IOC and UN hit by massive cyber-attack: http://www.bbc.co.uk/news/technology-14387559 Cisco: Targeted phishing helped hackers earn $150 million: http://searchsecurity.techtarget.com/news/2240037497/Cisco-Targeted-phishing-helped-hackers-earn-150-million-last-month
Social and Financial	Large-scale disruption of banking services, stock	Public panic

Term	Definition	Reported Example(s) or Consequences
Threats^	exchanges, credit-card-processing, etc.	
Social Networking Threats^	Sometime referred to as a "cyber-stalker's dream come true," the information made available on social networking sites is available to everyone who can make an account.	Fraud Identity Theft Hacking a Fox News Twitter account: http://www.nytimes.com/2011/07/05/business/media/05fox.html?_r=1 http://www.bbc.co.uk/news/technology-14012294
Spam^	Slang term for unsolicited email.	
Third-Party Threats^	A compromises that allow a perpetrator to access the company's network through an otherwise trusted third-party connection (such as a Virtual Private Network (VPN)).	Washington Post hacked and 1.27 million emails potentially compromised: http://www.washingtonpost.com/wp-srv/jobs/product-pages/fraud-email.html
Trojan horse	Stealthy code that executes under the guise of a useful program but performs malicious acts such as the destruction of files, the transmission of private data, and the opening of a back door to allow third-party control of a machine.	
Virus	Malicious code that can	

Term	Definition	Reported Example(s) or Consequences
	self-replicate and cause damage to the system it infects. The code can delete information, infect programs, change the directory structure to run undesirable programs, and infect the vital part of the operating system that ties together how files are stored.	
Vulnerability Exploits^	When the software running on a system is manipulated into doing something it was not designed to do.	Modified permissions. Install back door for later entry and control. Iran hijacked US RQ-170 drone: http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video Medical devices such as insulin pump controlled through cyber-attack: http://www.medicaldaily.com/articles/9486/20120410/medical-implants-pacemaker-hackers-cyber-attack-fda.htm#md5KuC237zm6BE5m.99 http://www.cardiosource.org/News-Media/Publications/CardioSource-World-News/Homeland-Security.aspx
Website Middleware Threats^	Targeting website-hosting software that makes it easy to host, update, and maintain a website. Website administrators often fail to upgrade software due to fear it will break a	"Google hacking" where indexed pages within search engines are used to identify similar sites, thus allowing a hacker to exploit multiple sites as necessary. Google warns users about active malware infection: http://www.net-security.org/malware_news.php?id=1777

Term	Definition	Reported Example(s) or Consequences
	page, a link, or other process.	
Worm	Similar to virus, a worm is distinctive for its ability to self-replicate without infecting other files in order to reproduce.	Son of Stuxnet Found in the Wild on Systems in Europe (Duqu): http://www.wired.com/threatlevel/2011/10/son-of-stuxnet-in-the-wild/
Zombie	A computer that has been covertly compromised and is controlled by a third party.	

Sources:

Adapted from Derek S. Reveron, *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, 8.
^ Additional entries based on information from Doug Howard and Kevin Prince, *Security 2020: Reduce Security Risks This Decade*, 97-130.

Sources of Cyber Threats

Threat source	Motivation	Examples*
Intelligence services	Foreign intelligence services use cyber tools as part of their information gathering and espionage activities. These include exploitation and potential disruption or destruction of information infrastructure.	US blames China, Russia for cyber espionage: http://www.reuters.com/article/2011/11/03/us-usa-cyber-china-idUSTRE7A23FX20111103; http://www.reuters.com/article/2011/11/04/us-china-usa-cyber-idUSTRE7A31FW20111104 China reverse engineers downed EP-3E Aries II reconnaissance plane to intercept US Navy communications: http://www.newyorker.com/reporting/2010/11/01/101101fa_fact_hersh South Korean web attacks might have been intelligence gathering activity: http://www.reuters.com/article/2011/07/05/us-korea-cyberattack-idUSTRE76479M20110705 RSA, a top US Security firm, hacked and security codes stolen: http://www.npr.org/2011/06/06/137000302/latest-hacks-could-set-the-stage-for-cyberwar
Criminal groups	Criminal groups use cyber intrusions for monetary gain.	FBI takes out $14M DNS malware operation: http://www.networkworld.com/community/blog/fbi-takes-out-14m-dns-malware-operation
Hackers	Hackers sometimes crack into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download	Hacker published the details of the internal Florida Voting Database online: http://www.zeropaid.com/news/94099/abhaxas-dumps-details-of-the-internal-florida-voting-database-online/

		attack scripts and protocols from the Internet and launch them against victim sites. Thus, attack tools have become more sophisticated and easier to use.	
	Hacktivists	These groups and individuals conduct politically motivated attacks, overload e-mail servers, and hack into websites to send a political message.	Hacktivist Group 'Anonymous' Hacks Turkish Government Site: http://www.theinquirer.net/inquirer/news/2086549/anonymous-hacks-turkish-government-web-sites
	Disgruntled insiders	The disgruntled insider, working from within an organization, is a principal source of computer crimes. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a victim system often allows them to gain unrestricted access to cause damage to the system or to steal system data.	Man accused of crashing UBS servers: http://www.theregister.co.uk/2006/06/08/ubs_hack_attack/
	Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence. The CIA believes terrorists will stay focused on traditional attack methods, but it anticipates growing cyber	Islamist group Izz ad-Din al-Qassam Cyber Fighters, a military wing of Hamas, attack US banks: http://www.securityinfowatch.com/blog/10796084/cyber-terror-rages-in-the-banking-sector Cyberattacks could become as destructive as 9/11, says Panetta (US Secretary of Defense): http://www.businessweek.com/news/2012-10-12/cyberattacks-could-become-as-destructive-as-9-11-panetta

		threats as a more traditionally competent generation enters the ranks.	

Sources:
US Government Accountability Office, GAO 10-230T, *Statement for the Record to the Subcommittee on Terrorism and Homeland Security, Committee on the Judiciary, US Senate; Cybersecurity: Continued Efforts are Needed to Protect Information Systems from Evolving Threats*, November 17, 2009, last accessed 13 February 2013, http://www.defense.gov/home/features/2010/0410_cybersec/docs/d10230t.pdf.

*Examples column added. From various sources as indicated.

Appendix 3

CF "Operational Functions" and the E/CE Disciplines

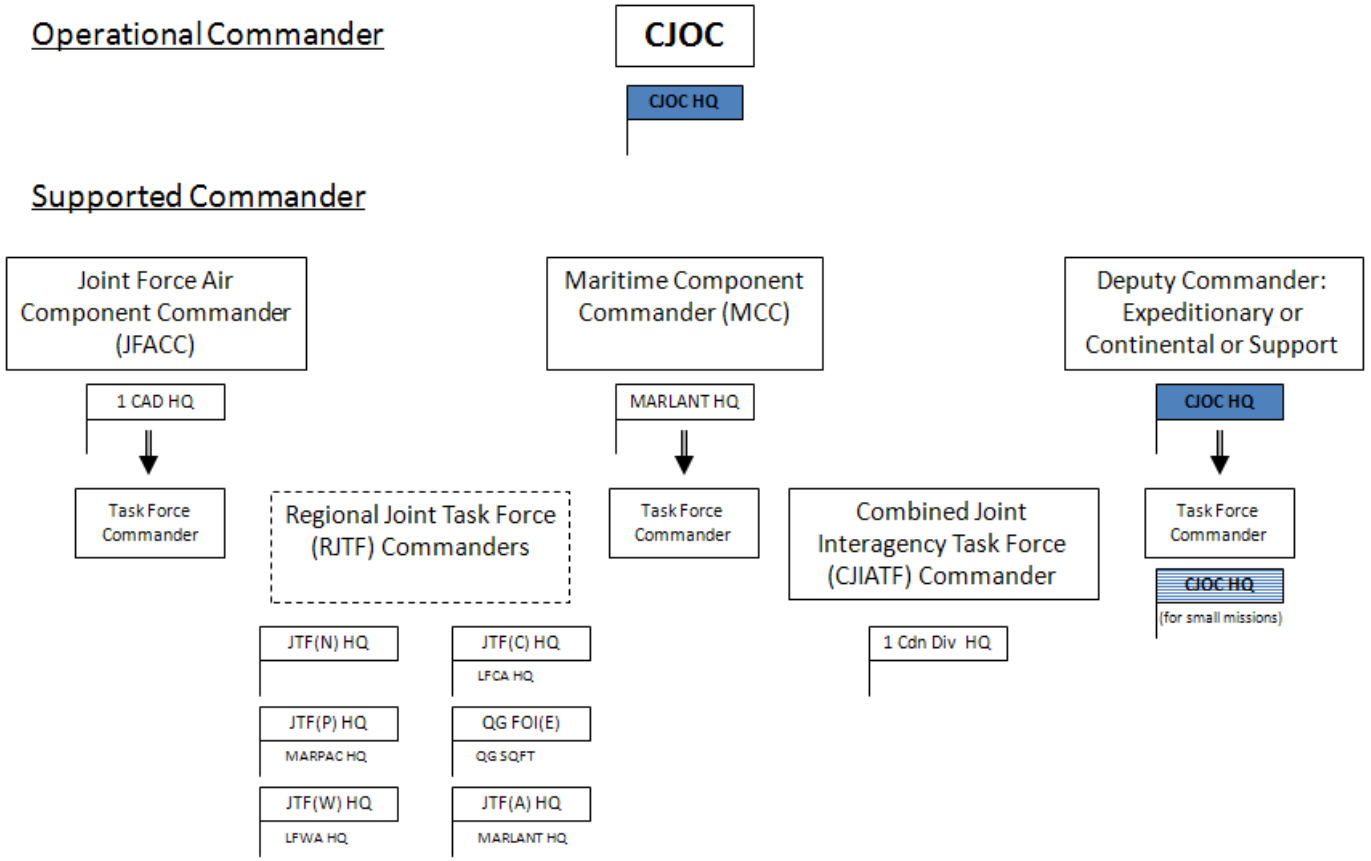
Function	**Definition (Proposed and Current)**	**Related E/CE disciplines** (and their sub-activities)
Command	The creative and purposeful exercise of legitimate authority to accomplish the mission legally, professionally, and ethically. Command Support, Communications, Joint Effects Targeting	CIS
Sense	The acquisition and processing of information to enable commanders and authorities to understand the characteristics and conditions of the operating environment pertinent to military decision-making. Intelligence, Surveillance and Reconnaissance	EW (ES) SIGINT CNO (CND, CNE)
Act	The military use of capabilities to achieve desired effects in support of national policy. Aerospace effects production, land effects production, maritime effect production, special operations effects production.	EW (ES and EA) SIGINT and CNO (CNE/CNA) – if authorized
Shield	The comprehensive approach to the protection of tangible and intangible elements through the integrating activities of detection, assessment, warning, defence (active and passive), and recovery. Force protection.	CNO (CND) CIS (Info Assurance) EW (EP, ES, some passive EA) SIGINT (threat warning)
Sustain	The provisioning of all support services required to maintain routine and contingency operations – domestic, continental, and expeditionary – including prolonged operations. Sustainment, support services, movements, theatre	Some sustain capability is integral to CIS organizations. Force

	activation and deactivation	Generators and CFD.

Sources: Adapted from Canadian Forces Warfare Centre, B-GJ-005-000/FP-001 *CFJP-01 - Canadian Military Doctrine* (Ottawa: Department of National Defence, 2011), Table 2-1 and Chief of Force Development, A-FD-005-002/AF-001, *Integrated Capstone Concept* (Winnipeg, MB: 17 Wing Winnipeg Publishing Office, 20 October 2009), 39.

Appendix 4

CJOC and the Supported Component Commanders



Sources: Based on information from Commander Canada Command, *Standing Operations Order for Domestic Operations (SOODO) – Draft*. (Canada Command Headquarters: file 6397-03000-01 (Dom Strat 1), February 2012); and Commander 1st Canadian Division, *Force Employment Concept 1st Canadian Division Headquarters* (1st Canadian Division Headquarters: file 3350-1 (Comd), 21 March 2012.

Appendix 5

CF Occupations Operating in E/CE According to Service

Service	CF Occupations Operating in E/CE	Occupation Reference	Principal Employing Units / Formations
Joint	Comm Rsch	http://www.forces.ca/en/job/communicatorresearchoperator-29	CFIOG (CFNOC, CFEWC, CFS Leitrim)
Royal Canadian Navy	NCIO	http://www.forces.ca/en/job/navalcombatinformationoperator-22	RCN ships
	NESOps	http://www.forces.ca/en/job/navalelectronicsensoroperator-23	
	Sonar Ops	http://www.forces.ca/en/job/sonaroperator-25	
	Some MARS/NCS Engr	http://www.forces.ca/en/job/maritimesurfaceandsubsurfaceofficer-65; or http://www.forces.ca/en/job/navalcombatsystemsengineeringofficer-82	
Canadian Army	SIGS	http://www.forces.ca/en/job/signalsofficer-79	CFJSR CMBG Sig Sqns Unit Sig Troops 21 EW Regt LISS Garrison Sig Sqns
	ACIS	http://www.forces.ca/en/job/armycommunicationandinformationsystemsspecialist-171	
Royal Canadian Air Force	CELE(A)	http://www.forces.ca/en/job/communicationsandelectronicsengineeringairofficer-77	CFJSR 8 ACCS ATESS RCAF WTIS
	ATIS	http://www.forces.ca/en/job/aerospacetelecommunicationinformationsystemstechnician-18	
	AESOps	http://www.forces.ca/en/job/airborneelectronicsensoroperator-8.	

			Sections EWOS

Sources: As indicated.

Appendix 6

Comparison of CF Occupations and CF Units Conducting Activities in E/CE

Level of war	CF Occupations in E/CE Disciplines				Units / Formations (By Level of War)
	CIS	CNO	EW	SIGINT	
Strategic	SIGS CELE(A) ACIS ATIS Some MARS/NCS Engr	Comm Rsch Some Other* Some SIGS Some CELE(A)	Comm Rsch NESOps Some SIGS^ Some CELE(A)^	Comm Rsch Some SIGS^ Some CELE(A)^	CFIOG (CFNOC, CFEWC, CFS Leitrim for CNO, EW and SIGINT only)
Operational	SIGS CELE(A) ACIS ATIS	Same as Strategic Level		Same as Strategic Level	CFJSR (for CIS only) LISS / EWOS
Tactical	SIGS CELE(A) ACIS ATIS NCIO		Comm Rsch NESOps AESOps Sonar Ops	Same as Strategic Level	Army Brigade Sig Sqns/Unit Sig Troops (CIS only) 21 EW Regt RCAF WTIS Sections (CIS only) RCN ships (CIS and EW)
Units / Formations (By E/CE discipline)	<u>Strategic</u> • 764 Comm Sqn • CFJSR (inter-theatre CIS) <u>*Operational Level*</u> • *CFJSR* • *8 ACCS*	<u>Strategic / Operational</u> • CFNOC	<u>Strategic</u> • CFEWC <u>*Operational*</u> • *21 EW Regt (EWCC only)* <u>Tactical</u> • 21 EW Regt (2	<u>Strategic</u> • CFS Leitrim	

	Tactical Level • 76 Comm Gp (NDHQ) • 8 ACCS • CMBG Sig Sqns • RCAF WTIS Sections		EW Sqn) • Ships (Destroyers, Frigates) • Maritime Patrol Aircraft Sqns		

Source: Compiled from multiple sources. Occupational information available from Canadian Forces Recruiting, "Browse Jobs," http://www.forces.ca/en/JobExplorer/BrowseJobs-70.
*Other – other occupation based on demonstrated skill sets
^SIGS / CELE(A) – this discipline is acquired through on-the-job training and experience; basic occupational training.provides minimal exposure to these particular disciplines.

Legend (alphabetical order):

Non-Commissioned Member Occupations:	Units / Sections / Formations:	
ACIS – Army Communications and Information Systems Specialist (includes operators, technicians, line specialists) AESOps - Airborne Electronic Sensor Operators ATIS – Aerospace Telecommunications and Information Systems Techician Comm Rsch – Communicator Research Operator NCIO – Naval Combat Information Operator NESOp – Naval Electronic Sensor Operator Sonar Op – Sonar Operator Officer Occupations: CELE(A) – Communications and Electronics Engineer (Air) MARS – Maritime Surface and Sub-surface Officer (if appointed) NCS Engr – Naval Combat Systems	ATESS – Aerospace and Telecommunication Engineering Support Squadron CFEWC – CF Electronic Warfare Centre CFIOG – CF Information Operations Group (includes CFNOC, CFEWC and CFS Leitrim) CFJSR – CF Joint Signal Regiment CMBG Sig Sqn – Canadian Mechanized Brigade Group Signal Squadron CFNOC – CF Network Operations Centre CFS Leitrim – CF Station Leitrim EWCC – Electronic Warfare Coordination Centre EWOS – Electronic Warfare Operational Support (under CF Aerospace Warfare Centre)	LISS - Land Integrated Support Section (under Army's Directorate of Land Integration) NEWC – Naval Electronic Warfare Centre (co-located with CFEWC) WTIS – Wing Telecommunication and Information System Section 21 EW Regt – 21 Electronic Warfare Regiment 76 Comm Gp – 76 Communication Group 8 ACCS – 8 Air Command and Control Squadron

Engineer (if appointed) SIGS – Signals Officer		

Appendix 7

Joint Defence Cyber and EMS Concepts, Strategies and Doctrine

	Defence Cyber-related entities	Defence Cyber Concepts/Strategies/Doctrine	Defence EMS-related entities	Defence EMS Concepts/Strategies/Doctrine
United States	National Security Agency / Central Security Services (NSA/CSS) US Cyber Command (CYBERCOM)	- JP 3-12 - *Cyberspace Operations* (classified), http://www.dtic.mil/doctrine/doctrine/status.pdf - National Military Strategy for Cyberspace Operations, December 2006, http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf	Joint EW Centre (JEWC)	- JP 6-1 – *Joint Electromagnetic Spectrum Operations* – 20 Mar 2012, http://www.dtic.mil/doctrine/new_pubs/jp6_01.pdf - JP 13-1.1 - *Electronic Warfare* – 08 February 2012, http://info.publicintelligence.net/JCS-EW.pdf
United Kingdom	Government Communications Headquarters/Cyber Security Operations Centre (GCHQ/CSOC) UK Permanent Joint Headquarters (PJHQ) / Defence Cyber	- JDP 6-00 - *Communications and Information Systems Support to Joint Operations*, 3rd Edition, January 2008, under Annex 3D (Security and Information Governance), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/33709/20111221JDP600_Ed3_inc_Chg1.pdf - JDN 4/10 – *Single SIGINT Battlespace*, September 2010. (Restricted)	*Nil joint unit found.*	- JDP 6-00 – *Communications and Information Systems Support to Joint Operations*, 3rd Edition, January 2008, under Annex 3E (Battle space Spectrum Management), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/33709/20111221JDP600_Ed3_inc_Chg1.pdf - JDP 3-70 - *Joint Battlespace Management*

	Defence Cyber-related entities	Defence Cyber Concepts/Strategies/Doctrine	Defence EMS-related entities	Defence EMS Concepts/Strategies/Doctrine
	Operations Group (DCOG)			
Australia	Defence Signals Directorate /Cyber Security Operations Centre (DSD/CSOC) - To be subsumed under Australian Cyber Security Centre (ACSC)	- ADDP 6.0 – *Communication and Information Systems*, 2nd Edition, 26 June 2012, CNO at para 2.45. http://www.defence.gov.au/adfwc/Documents/DoctrineLibrary/ADDP/ADDP_6-0_CIS.pdf - ADFP 6.0.1—*Communication and Information Systems Planning* (under development)	*Nil found.*	- ADDP 6.0 – *Communication and Information Systems*, 2nd Edition, 26 June 2012, Defence use of EMS at section 3.43. - ADFP 6.0.1—*Electromagnetic Spectrum Planning (under development)*
New Zealand	Government Communications Security Bureau/National Cyber Security Centre (GCSB/NCSC)	*Nil found.*	*Nil found.*	*Nil found.*
5-Eyes All		*Nil found.*	Combined Communications	- ACP 194 - Policy for the Coordination of Military Radio Frequency Allocation between Cooperating Nations, June 2011,

	Defence Cyber-related entities	Defence Cyber Concepts/Strategies/Doctrine	Defence EMS-related entities	Defence EMS Concepts/Strategies/Doctrine
ied			Electronics Board (CCEB)	http://jcs.dtic.mil/j6/cceb/acps/acp194/ACP194.pdf
NATO	NATO Communications and Information (NCI) Agency NATO Computer Incident Response Capability (NCIRC) Cyber Defence Management Board NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE)	- Defending the networks: The NATO Policy on Cyber Defence, 4 October 2011, http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf -	NATO Joint Electronic Warfare Core Staff (JEWCS)	- MC 0064, NATO Policy for Electronic Warfare (no website found).

Bibliography

Andrues, Wesley R. "What U.S. Cyber Command Must Do." *Joint Forces Quarterly* 59 (4th Quarter 2010): 115-120.

Anti-Phishing Working Group. "Phishing Activity Trends Report – 2nd Quarter 2012." Last accessed 2 April 2013. http://docs.apwg.org/reports/apwg_trends_report_q2_2012.pdf.

Association of Old Crows. "A (Pragmatic) Future for Joint Electronic Warfare: Does EW + CNO = Cyber?" *The Journal of Electronic Defense* (September 2008): 31-38.

Australia. Australian Government. *Cyber Security Strategy*. Canberra, AS: Attorney General's Department, 2009. http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf.

———. Australian Government. *Strong and Secure: A Strategy for Australia's National Security*. Canberra, AS: Department of the Prime Minister and Cabinet, 2013. http://www.dpmc.gov.au/national_security/docs/national_security_strategy.pdf.

———. Department of Defence. "Australian cyber security centre to be established." Last accessed 2 April 2013. http://www.defence.gov.au/defencenews/stories/2013/jan/0124.htm.

———. Department of Defence. "Cyber Security Operations Centre." Last accessed 2 April 2013. http://www.dsd.gov.au/infosec/csoc.htm.

BBC News. "US plants hit by USB stick malware attack." 16 January 2013. Last accessed 2 April 2013. http://www.bbc.co.uk/news/technology-21042378.

Beaudoin, Luc, Michael Froh, Marc Gregoire, and Julie Lefebvre. "Computer Network Defence Situational Awareness Information Requirements." Last accessed on 2 April 2013. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4086552.

Bernier, Melanie and Joanne Treurniet. "Understanding Cyber Operations in a Canadian Strategic Context: More Than C4ISR, More Than CNO." In *Conference on Cyber Conflict Proceedings 2010*, edited by C. Czosseck and K. Podins, 227-243, Tallinn, Estonia: CCD COE Publications, 2010. http://www.ccdcoe.org/publications/2010proceedings/Benier%20-%20Understanding%20Cyber%20Operations%20in%20a%20Canadian%20Strategic%20Context%20More%20than%20C4ISR,%20More%20than%20CNO.pdf.

Bourque, J. "Spectrum Control: Controlling the EMS Domain." February 2011. n.p.

Bowden, Mark. *Worm: The First Digital World War*. New York: Atlantic Monthly Press, 2011.

Brachman, Jerret and Lianne Kennedy Boudali. *The Islamic Imagery Project: Visual Motifs in Jihadi Internet Propaganda*. West Point, NY: The Combating Terrorist Centre at West

Point, March 2006. http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&lng=en&id=19674.

Brown, Gary D. "Why Iran Didn't Admit Stuxnet Was an Attack." *Joint Forces Quarterly* 63 (4th Quarter 2011): 70-73.

Bucci, Steven. "Joining Cybercrime and Cyberterrorism: A Likely Scenario." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World,* edited by Derek S. Reveron, 57-68. Washington, DC: Georgetown University Press, 2012.

Canada. Assistant Deputy Minister (Information Management). "Mission." Last accessed 2 April 2013. http://img.mil.ca/aim-pgg/mv/index-eng.asp (DWAN).

———. Chief Defence Intelligence. *CF Signals Intelligence (SIGINT) Policy (ratification draft)*, n.p., 25 June 2007.

———. Canadian Forces Chief of Transformation. *Report on Transformation 2011* (Ottawa: Department of National Defence, 6 July 2011. http://www.forces.gc.ca/site/reports-rapports/transfo2011/_doc/Report_on_Transformation_2011_eng.pdf

———. Canadian Forces Communications and Electronics Branch. "Organization." Last accessed 2 April 2013. http://www.commelec.forces.gc.ca/org/index-eng.asp.

———. Canadian Forces Leadership Institute. *Broadsword or Rapier? The Canadian Forces' Involvement in 21st Century Coalition Operations.* Kingston, ON: Canadian Defence Academy, April 2008.

———. Canadian Forces Provost Marshall. "Information Systems (IS) Security." Chapter 70 in A-SJ-100-001/AS-000. *National Defence Security Instructions*. Ottawa: Department of National Defence, 1999.

———. Canadian Forces Recruiting, "Browse Jobs." Last accessed 2 April 2013. http://www.forces.ca/en/JobExplorer/BrowseJobs-70.

———. Canadian Forces School of Communications and Electronics. *Transforming the Network Fight: Unique Skills, Unique Tactics, Unique Effects – CFSCE Campaign Plan.* Kingston, ON: CFSCE Publication Development, 27 June 2008.

———. Canadian Forces Warfare Centre. B-GJ-005-000/FP-001, *CFJP-01 - Canadian Military Doctrine*. Ottawa: Department of National Defence, 2011. http://www.cfd-cdf.forces.gc.ca/cfwc-cgfc/Index/JD/CFJP%20-%20PDF/CFJP%2001/CFJP-01_Cdn_Mil_Doctrine_EN_2011_09.pdf

———. Canadian Forces Warfare Centre. B-GJ-005-200/FP-001, *CFJP 2-0 – Joint Intelligence.* Ottawa: Department of National Defence, 2011.

———. Canadian Forces Warfare Centre. B-GJ-005-300/FP-001, *CFJP 3.0 – Joint Operations.* Ottawa: Department of National Defence, 2011.

———. Chief of the Air Staff. B-GA-403-002/FP-001, *Aerospace Electronic Warfare Doctrine*, 1st Ed. Ottawa: Department of National Defence, March 2011. http://www.airforce.forces.gc.ca/cfawc/CDD/Doctrine/Pubs/Operational/403_Series/B-GA-403-002-FP-001.pdf.

———. Chief of Defence Staff, B-GG-005-004/AF-010. *CF Information Operations*. Ottawa: Department of National Defence, 1998.

———. Chief of Force Development. A-FD-005-002/AF-001. *Integrated Capstone Concept*. Winnipeg, MB: Department of National Defence (17 Wing Winnipeg Publishing Office), 20 October 2009. http://publications.gc.ca/collections/collection_2012/dn-nd/D2-265-2010-eng.pdf.

———. Chief of Force Development. B-GJ-005-500/FP-000. *CFJP 5.0 – The Canadian Forces Operational Planning Process (OPP), Change 2.* Ottawa: Department of National Defence, 2008.

———. Chief of Force Development. *Department of National Defence / Canadian Forces National Surveillance Study 2010 (Unclassified).* Ottawa: Department of National Defence, 15 January 2011.

———. Chief of Force Development. *The Future Security Environment 2008-2030 – Part 1: Current and Emerging Trends*. Ottawa: Department of National Defence, 27 January 2009. http://www.cfd-cdf.forces.gc.ca/documents/CFD%20FSE/Signed_Eng_FSE_10Jul09_eng.pdf

———. Chief of Land Staff. B-GL-351-001/FP-001, *Signals in Support of Land Operations – Volume 1*. Ottawa: Department of National Defence, 1 May 2008.

———. Chief of Land Staff. B-GL-351-003/FP-003, *Signals in Support of Land Operations – Volume 3: Tactical Electronic Warfare and Signals Intelligence*. Ottawa: Department of National Defence, 28 March 2011.

———. Chief of Land Staff. B-GL-352-001/FP-001, *ISTAR Volume 1 – The Enduring Doctrine*, Study Draft. Kingston, ON: Director of Army Doctrine, 22 August 2012.

———. Chief of Staff (Information Management). *Implementation Order 005/12 – IM Gp Support to LCCS/CSNI Convergence*. National Defence Headquarters: file 3350-3 (J6 Coord), 26 July 2012.

———. Commander 1st Canadian Division. *Force Employment Concept 1st Canadian Division Headquarters*. 1st Canadian Division Headquarters: file 3350-1 (Comd), 21 March 2012.

———. Commander Canada Command. *Standing Operations Order for Domestic Operations (SOODO)- Draft*. Canada Command Headquarters: file 6397-03000-01 (Dom Strat 1), February 2012.

———. Commander Canadian Army. *Designing Canada's Army of Tomorrow - A Land Operations 2021 Publication*. Ottawa: Department of National Defence, 2011. http://www.army.forces.gc.ca/CALWC-CGTAC/pubs/armyoftomorrow/DesigningCanadasArmyofTomorrow_full_e.pdf.

———. Commander Canadian Army. *Army Strategic Transition Roadmap (ASTR)* (Commander Canadian Army: file 1901-1 (DLFD 3), 13 April 2012.

———. Communications Security Establishment Canada. "Signals Intelligence (SIGINT)." Last accessed 2 April 2013. http://www.cse-cst.gc.ca/home-accueil/what-que/sigint-eng.html.

———. Communications Security Establishment Canada. "About IT Security." Last accessed 2 April 2013. http://www.cse-cst.gc.ca/its-sti/index-eng.html.

———. Directorate of Land Concepts and Design. *Land Operations 2021: Adaptive Dispersed Operations: The Force Employment Concept for Canada's Army of Tomorrow*. Kingston, ON: Department of National Defence, 2007. http://www.army.forces.gc.ca/CALWC-CGTAC/pubs/landops2021/Land_Ops_2021_eng.pdf.

———. Defence Research and Development Canada. "DRDC Ottawa." Last accessed 2 April 2013. http://www.drdc-rddc.gc.ca/drdc/en/centres/drdc-ottawa-rddc-ottawa/.

———. Defence Research and Development Canada. "DRDC Valcartier." Last accessed 2 April 2013. http://www.drdc-rddc.gc.ca/drdc/en/centres/drdc-valcartier-rddc-valcartier/.

———. Defence Research and Development Canada. "Areas of Science and Technology Expertise." Last accessed 2 April 2013. http://www.drdc-rddc.gc.ca/drdc/en/sciences/expertise/.

———. Department of National Defence. "Shaping the Future of the Canadian Forces: A Strategy for 2020." Last accessed on 2 April 2013. http://www.cds.forces.gc.ca/str/index-eng.asp.

———. Department of National Defence. "JOINTEX drives a CF cultural evolution," *The Maple Leaf* 15, issue 04 (April 2012): 11. http://www.forces.gc.ca/site/tml/article-eng.asp?id=17&y=2012&m=04.

———. Department of National Defence. "DND/CF Space Operations: To the Future and Beyond." *The Maple Leaf* 15, issue 5 (May 2012): 8-9. http://www.forces.gc.ca/site/tml/article-eng.asp?id=1&y=2012&m=05.

———. Department of National Defence. "JOINTEX 13 prepares CF for future operations," *The Maple Leaf* 15, issue 11 (December 2012): 6. http://www.forces.gc.ca/site/tml/article-eng.asp?id=9&y=2012&m=12.

———. Government of Canada. *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada*. Ottawa: Public Safety Canada, 2010. http://www.publicsafety.gc.ca/prg/ns/cybr-scrty/ccss-scc-eng.aspx.

———. Government of Canada. *Canada First Defence Strategy*. Ottawa: Department of National Defence, 2008. http://www.forces.gc.ca/site/pri/first-premier/June18_0910_CFDS_english_low-res.pdf.

———. Government of Canada. *Federal Emergency Response Plan.* Ottawa: Public Safety Canada, January 2011. http://www.publicsafety.gc.ca/prg/em/_fl/ferp-2011-eng.pdf.

———. Government of Canada. *National Strategy for Critical Infrastructure.* Ottawa: Public Safety Canada, 2009. http://www.publicsafety.gc.ca/prg/ns/ci/_fl/ntnl-eng.pdf.

———. Government of Canada. *Action Plan for Critical Infrastructure*. Ottawa: Public Safety Canada, 2009. http://www.publicsafety.gc.ca/prg/ns/ci/_fl/ct-pln-eng.pdf.

———. Industry Canada. *Policy and Technical Framework: Mobile Broadband Services (MBS) — 700 MHz Band, Broadband Radio Service (BRS) — 2500 MHz Band*. Ottawa, ON: Industry Canada, March 2012. http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf10121.html#pA4.

———. Joint Cyber Operations Team. *Joint Cyber Operations Team (JCOT) Concept of Operations – Draft Version 2.0*, n.p., 12 December 2012.

———. Office of the Auditor General of Canada. "Aging Information Technology Systems," Chapter 1 in *2010 Spring Report of the Auditor General of Canada to the House of Commons*. Ottawa: Public Works and Government Services Canada, 2010. http://www.oag-bvg.gc.ca/internet/English/parl_oag_201004_01_e_33714.html.

———. Office of the Auditor General of Canada. "Protecting Canadian Critical Infrastructure Against Cyber Threats." Chapter 3 in *2012 Fall Report of the Auditor General of Canada to the House of Commons*. Ottawa: PWGSC, 2012. http://www.oag-bvg.gc.ca/internet/English/parl_oag_201210_03_e_37347.html.

———. Public Safety Canada. "Cyber Security in the Canadian Federal Government." Last accessed 2 April 2013. http://www.publicsafety.gc.ca/prg/ns/cybr-scrty/fdrl-gvt-eng.aspx.

———. Public Safety Canada. "Cyber Security Publications." Last accessed 2 April 2013. http://www.publicsafety.gc.ca/prg/em/ccirc/anre2012-eng.aspx.

———. Royal Canadian Air Force. "Basic Electronic Warfare (BEW)." Last accessed 2 April 2013. http://www.rcaf-arc.forces.gc.ca/itp-pfi/page-eng.asp?id=939 (DWAN).

———. Royal Canadian Air Force. "Advanced Operational Electronic Warfare (AOEW)." Last accessed 2 April 2013. http://www.rcaf-arc.forces.gc.ca/itp-pfi/page-eng.asp?id=931 (DWAN).

———. Shared Services Canada. *Integrated Business Plan 2012-2013.* Ottawa: Shared Services Canada, 2012. Last accessed 2 April 2013. http://www.ssc-pc.gc.ca/media/documents/IBP%202012_E_VA9D1.pdf.

———. Treasury Board of Canada Secretariat. "*Policy on Government Security*", updated 1 April 2012. Last accessed 2 April 2013. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578&section=text.

———. Treasury Board of Canada Secretariat. "GC Information Technology Incident Management Plan." Last accessed 2 April 2013. http://www.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimti01-eng.asp.

———. Treasury Board of Canada Secretariat. "Welcome to the Chief Information Officer Branch." Last accessed 2 April 2013. http://www.tbs-sct.gc.ca/cio-dpi/index-eng.asp.

Carr, Jeffrey. *Inside Cyberwarfare*. Sebastopol, CA: O'Reilly Media Inc., 2010.

Carter, Rosemary M. Brent Feick, and Roy C. Undersander. "Offensive Cyber for the Joint Force Commander: It's Not That Different." *Joint Forces Quarterly* 66 (3rd Quarter 2012): 22-27.

CBC News. "Cybersecurity bill fails to pass in U.S. Senate." Last accessed 2 April 2013. http://www.cbc.ca/news/technology/story/2012/08/02/tech-cybersecurity-bill-us.html

CBN News. "Israel Building 'Digital Iron Dome'." Last accessed 13 February 2013. http://www.cbn.com/cbnnews/insideisrael/2012/October/Israel-Building-Digital-Iron-Dome/.

Chui, Michael Markus Löffler, and Roger Roberts."The Internet of Things." Last accessed 2 April 2013. http://www.mckinseyquarterly.com/The_Internet_of_Things_2538.

Clarke, Richard A. and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It.* New York: Harper Collins Publishers, 2010.

Combined Communications Electronics Board. *ACP 190(C). Guide to Spectrum Management in Military Operations*. September 2007. Last accessed 2 April 2013. http://jcs.dtic.mil/j6/cceb/acps/acp190/ACP190C.pdf

Conference Board of Canada. "It's All About You: Building Capacity in Cyber Security." September 2011. Last accessed 2 April 2013. http://www.conferenceboard.ca/e-library/abstract.aspx?did=4434.

Conti, Gregory, and David Raymond. "Leadership of Cyber Warriors: Enduring Principles and New Directions." *Small Wars Journal* 7, no. 7 (11 July 2011). http://smallwarsjournal.com/jrnl/art/leadership-of-cyber-warriors-enduring-principles-and-new-directions.

Conti, Gregory, J., Caroland, T. Cook, and H. Taylor. "Self-Development for Cyber Warriors." *Small Wars Journal* 7, no. 11 (10 November 2011). http://smallwarsjournal.com/jrnl/art/self-development-for-cyber-warriors.

Conti, Gregory, and Jen Easterly. "Recruiting, Development, and Retention of Cyber Warriors Despite an Inhospitable Culture." *Small Wars Journal* 6, no. 7 (29 July 2010). http://smallwarsjournal.com/jrnl/art/recruiting-development-and-retention-of-cyber-warriors-despite-an-inhospitable-culture.

Cornish, Paul, Rex Hughes, and David Livingstone. *Cyberspace and the National Security of the United Kingdom: Threats and Responses*. London: Chatham House (Royal Institute of International Affairs), 2009.

Council of Europe. *Convention on Cybercrime* CETS no. 185. Last accessed 2 April 2013. http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG.

Cutts, Andrew. "Warfare and the Continuum of Cyber Risks: A Policy Perspective." In *The Virtual Battlefield: Perspectives on Cyber Warfare*, edited by Christian Czosseck and Kenneth Geers, 66-76. Fairfax, VA: IOS Press Inc., 2009.

Czarnecki, Jonathan E. "Operational Command and Control in Age of Entropy." Paper for Twelfth International Command and Control Research and Technology Symposium, Naval War College, 2007. Last accessed 2 April 2013. http://www.dtic.mil/dtic/tr/fulltext/u2/a481372.pdf.

Darnton, Geoffrey. "Information Warfare and the Laws of War." In *Cyberwar, Netwar, and the Revolution in Military Affairs*. Edited by E. Halpin, P. Trevorrow, D. Webb and S. Wright, 139-153, New York, NY: Palgrave MacMillan, 2006.

Demchak, Chris. "Cybered Conflict, Cyber Power, and Security Resilience as Strategy." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World,* edited by Derek S. Reveron, 121-136. Washington, DC: Georgetown University Press, 2012.

Erbschloe, Michael. *Implementing Homeland Security for Enterprise IT*. New York, NY: Elsevier Digital Press Inc., 2004.

Fidler, David P. "Inter arma silent leges Redux? The Law of Armed Conflict and Cyber Conflict." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World,* edited by Derek S. Reveron, 71-87. Washington, DC: Georgetown University Press, 2012.

Flynn, Charles A., Wayne W. Grigsby Jr. and Jeff Witsken "Fighting in the Clouds: The Network in Military Operations" *Army* (May 2012). http://www.ausa.org/publications/armymagazine/archive/2012/05/Documents/Flynn_0512.pdf.

Follath, Erich and Holger Stark. "The Story of 'Operation Orchard': How Israel Destroyed Syria's Al Kibar Nuclear Reactor." Last modified 2 November 2009. http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html.

Francis, Ed. "Electromagnetic Spectrum Operations: The Path to Net-Centric Warfare." *Army Communicator* 33, no. 1 (Winter 2008): 2-6. http://www.signal.army.mil/ocos/ac/Edition,%20Winter/Winter%2008.pdf

Fryer-Biggs, Zachary. "Navy Looking to Use EW as Part of Cyber." Last accessed 2 April 2013. http://blogs.defensenews.com/intercepts/2013/03/navy-looking-to-use-ew-as-part-of-cyber/.

Friar-Biggs, Zachary. "DoD Looking to 'Jump the Gap' Into Adversaries' Closed Networks." Last accessed 2 April 2013. http://www.defensenews.com/apps/pbcs.dll/article?AID=2013301150010.

Gash, Jim. "Physical Operating Environments: How the Cyber-Electromagnetic Environment Fits." *Canadian Military Journal* 12, no. 3 (Summer 2012): 28-34. http://www.journal.forces.gc.ca/vol12/no3/page28-eng.asp

Gendron, Angela and Martin Rudner. *Assessing Cyber Threats To Canadian Infrastructure: Report Prepared For The Canadian Security Intelligence Service*. Ottawa: Canadian Security Intelligence Service, March 2012. http://www.csis-scrs.gc.ca/pblctns/cdmctrch/20121001_ccsnlpprs-eng.asp#a.

Gibbs, Mark. "SigInt in Afghanistan – Task Force Afghanistan 5-10" *C&E Branch Newsletter* 54 (1 December 2010): 31-32. http://www.commelec.forces.gc.ca/inf/new-bul/vol54/doc/newslett-bulletin-vol54-eng.pdf.

Goodman, Glenn. "Dismounted Counter-IED: Size, Weight and Power Limits," *Soldier Mod* 2 (January 2009): 38-39. http://soldiermod.com/volume-2/pdfs/articles/dismounted-jamming.pdf.

Gorman, Sean P. *Networks, Security, and Complexity: The Role of Public Policy in Critical Infrastructure Protection*. Northampton, MA: Edward Elgar Publishing Inc., 2005

Gorman, Siobhan and Julian E. Barnes. "Cyber Combat: Act of War." *Wall Street Journal*, May 30, 2011. Last accessed 2 April 2013. http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html?KEYWORDS=cyber+combat.

Grauman, Brigid. *Cyber-Security: The Vexed Question of Global Rules (An Independent Report on Cyber-Preparedness Around the World.* Brussels: Security & Defence Agenda, 2012.

Greenemeier, Larry. "The Fog of Cyberwar: What Are the Rules of Engagement." Last accessed 2 April 2013. http://www.scientificamerican.com/article.cfm?id=fog-of-cyber-warfare.

Grigsby Jr., Wayne W., J. Garrett Howard, Tony McNeill, and Gregg Buehler. "CEMA: A Key to Success in Unified Land Operations." *Army*. June 2012. http://www.ausa.org/publications/armymagazine/archive/2012/06/Documents/Grigsby1_0612.pdf

Gvosdev, Nikolas K. "The Bear Goes Digital: Russia and Its Cyber Capabilities." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, edited by Derek S. Reveron, 173-189. Washington, DC: Georgetown University Press, 2012.

Hayden, Michael V. "The Future of Things 'Cyber'." *USAF Strategic Studies Quarterly*, Spring 2011: 3-7.

Healey, Jason and Leendert van Bochoven. "NATO's Cyber Capabilities: Yesterday, Today and Tomorrow (Atlantic Council Issue Brief)." Washington, DC: Atlantic Council, 2011. http://www.acus.org/files/publication_pdfs/403/022712_ACUS_NATOSmarter_IBM.pdf

Hollis, David M. "USCYBERCOM: The Need for a Combatant Command versus a Subunified Command." *Joint Forces Quarterly* 58 (3rd Quarter 2010): 48-53.

Howard, Doug and Kevin Prince. *Security 2020: Reduce Security Risks This Decade*. Indianapolis, IN: Wiley Publishing Inc., 2011.

Hughes, Rex. "Towards a Global Regime for Cyber Warfare." In *The Virtual Battlefield: Perspectives on Cyber Warfare*, edited by Christian Czosseck and Kenneth Geers, 106-117. Fairfax, VA: IOS Press Inc., 2009.

Infosecurity Magazine. "RSA 2011: Terrorist groups pose most dangerous cyber threat." Last accessed 2 April 2013. http://www.infosecurity-magazine.com/view/16005/rsa-2011-terrorist-groups-pose-most-dangerous-cyber-threat/.

———. "Security vulnerabilities in critical infrastructure up 600%." Last accessed 2 April 2013. http://www.infosecurity-magazine.com/view/30591/secuirty-vulnerabilities-in-critical-infrastructure-up-600/.

InformationWeek. "Shamoon Malware Might Be Flame Copycat." Last accessed 2 April 2013. http://www.informationweek.com/security/attacks/shamoon-malware-might-be-flame-copycat/240006014.

Inkster, Nigel. "China in Cyberspace." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, edited by Derek S. Reveron, 191-205. Washington, DC: Georgetown University Press, 2012.

International Telecommunications Union. *Digital Dividend: Insights for Spectrum Decisions.* Geneva, Switzerland: International Telecommunication Union, August 2012. http://www.itu.int/ITU-D/tech/digital_broadcasting/Reports/DigitalDividend.pdf.

———. *Exploring the Value and Economic Valuation of Spectrum: Broadband* Series. Geneva, Switzerland: International Telecommunication Union, April 2012. http://www.itu.int/ITU-D/treg/broadband/ITU-BB-Reports_SpectrumValue.pdf.

Jupiter Broadcasting. "Cyber Warfare | TechSNAP 13." July 7, 2011. Last accessed 2 April 2013. http://www.jupiterbroadcasting.com/10096/cyber-warfare-techsnap-13/.

Korns, Stephen W. "Cyber Operations: The New Balance." *Joint Forces Quarterly* 54 (3rd Quarter 2009): 97-102.

Libicki, Martin C. "Sub Rosa Cyber War." In *The Virtual Battlefield: Perspectives on Cyber Warfare*, edited by Christian Czosseck and Kenneth Geers, 53-65. Fairfax, VA: IOS Press Inc., 2009.

Langevin, James R. et al. *Securing Cyberspace for the 44th Presidency*. Washington, DC: Center for Strategic and International Studies, December 2008. http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

Lewis, James. "Cyber: Unclear and present danger." Last accessed 2 April 2013. http://www.lowyinterpreter.org/post/2013/02/19/Cyber-Unclear-and-present-danger.aspx.

Leyden, John. "Israel suspected of 'hacking' Syrian air defences." Last modified 4 October 2007. http://www.theregister.co.uk/2007/10/04/radar_hack_raid/.

Lynn, William J. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs* 89, no. 5 (September/October 2010): 97-108.

Miles, Donna. "Doctrine to Establish Rules of Engagement Against Cyber Attack." October 20, 2011. Last accessed 2 April 2013. http://www.defense.gov/news/newsarticle.aspx?id=65739.

Nethercott, John. "Op ATTENTION Theatre Activation Team Puts It All Together — Literally." Last accessed 2 April 2013. http://www.afghanistan.gc.ca/canada-afghanistan/stories-reportages/2011_06_07.aspx?lang=eng&view=d.

Newmeyer, Kevin P. "Who Should Lead U.S. Cybersecurity Efforts?" *Prism 3*, no. 2 (March 2012): 115-126. http://www.ndu.edu/press/us-cybersecurity-efforts.html

New Zealand. Government Communications Security Bureau. *New Zealand Information Security Manual*. Version 1.01. June 2011. http://www.gcsb.govt.nz/newsroom/nzism/NZISM_2011_Version_1.01.pdf

———. New Zealand Defence Force. *New Zealand Defence Force Statement of Intent 2011-2014*. Wellington, NZ: New Zealand Defence Force, 2010. http://www.nzdf.mil.nz/downloads/pdf/public-docs/2011/soi/nzdf-soi-2011-14.pdf.

———. New Zealand Government. *New Zealand Cyber Security Strategy*. 7 June 2011. http://www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-strategy-june-2011_0.pdf.

———. New Zealand Government. *New Zealand Defence White Paper 2010*. Wellington, NZ: New Zealand Ministry of Defence, November 2010. http://www.defence.govt.nz/pdfs/defence-review-2009-defence-white-paper-final.pdf.

Noonan, S., MGen. "Preparedness at the Operational Level." Lecture, Canadian Forces College, Toronto, ON, January 17, 2013, with permission.

North Atlantic Treaty Organization. AAP-06, *NATO Glossary of Terms and Definitions*. Brussels: NATO Standardization Agency, 2012. http://nsa.nato.int/nsa/zPublic/ap/aap6/AAP-6.pdf.

———. *Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization*. Brussels: NATO Public Diplomacy Division, 20 November 2010. http://www.nato.int/nato_static/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf.

———. *Defending the networks: The NATO Policy on Cyber Defence*. Brussels: NATO Public Diplomacy Division, 4 October 2011. http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf.

———. *NATO 2020: Assured Security; Dynamic Engagement - Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO*. Brussels: NATO Public Diplomacy Division, 17 May 2010. http://www.nato.int/nato_static/assets/pdf/pdf_2010_05/20100517_100517_expertsreport.pdf.

———. "NATO Rapid Reaction Team to fight cyber attack," 31 March 2012. Last accessed 2 April 2013. http://www.nato.int/cps/en/natolive/news_85161.htm.

———. "NATO and cyber defence." Last accessed 2 April 2013. http://www.nato.int/cps/en/natolive/topics_78170.htm.

———. "Strengthening Cyber Security," In *NATO Briefing: Tackling New Security Challenges*, 31 January 2012. Last accessed 2 April 2013. http://www.nato.int/nato_static/assets/pdf/pdf_publications/20120116_new-security-challenges-e.pdf.

North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. New York: Cambridge University Press, 2013. https://www.ccdcoe.org/249.html.

———. "Cyber Defence." Last accessed 2 April 2013. http://www.ccdcoe.org/2.html.

———. “CyCon.” Last accessed 2 April 2013. http://ccdcoe.org/362.html.

Obama, Barack. “Taking the Cyber Threat Seriously.” *Wall Street Journal*, July 19, 2012. Last accessed 2 April 2013. http://online.wsj.com/article/SB10000872396390444330904577535492693044650.html?KEYWORDS=Obama+cybersecurity.

OpenNet Initiative. “Country Profiles.” Last accessed 2 April 2013. https://opennet.net/country-profiles.

Organization for Economic Cooperation and Development. *Convergence and Next Generation Networks*. OECD Directorate for Science, Technology, and Industry Committee for Information, Computer and Communications Policy, 2008. http://www.oecd.org/sti/40761101.pdf.

Panetta, Leon E. Speech, Cybersecurity to the Business Executives for National Security, New York City, U.S.A., October 11, 2012. Last accessed 2 April 2013. http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

Pham, Khang. “Cyber Security: Do your part!” *The Maple Leaf* 15, no.2 (February 2012). http://www.forces.gc.ca/site/tml/article-eng.asp?id=1&y=2012&m=02.

Pigeau, Ross, and Carol McCann. "Re-conceptualizing Command and Control." *Canadian Military Journal* 3, no. 1 (Spring 2002): 53-63. http://www.journal.forces.gc.ca/vo3/no1/doc/53-64-eng.pdf.

Porteous, Holly. *The Stuxnet Worm: Just Another Computer Attack or a Game Changer?* Publication No. 2010-81-E. Ottawa: Library of Parliament, 7 October 2010.

Rid, Thomas, and Peter McBurney. “Cyber-Weapons” *The RUSI Journal* 157, no. 1 (29 February 2012): 6-13. http://www.tandfonline.com/doi/abs/10.1080/03071847.2012.664354.

RT. “Erase Israel from the Internet’: Anonymous plots massive cyber-attack.” Last accessed 2 April 2013. http://rt.com/news/anonymous-cyber-attack-israel-241/.

Ruggiero, Paul and Jon Foote. “Cyber Threats to Mobile Phones.” Report for the United States Computer Emergency Response Team. Pittsburgh, PA: Carnegie Mellon University, 2011. http://www.us-cert.gov/sites/default/files/publications/cyber_threats-to_mobile_phones.pdf.

Schreier, Fred. *On Cyberwarfare – DCAF Horizon 2015 Working Paper 7* (Geneva, Switzerland: DCAF, 2012). http://www.dcaf.ch/Publications/On-Cyberwarfare.

Schmidt, Howard A. *Patrolling Cyberspace: Lessons Learned from a Lifetime in Data Security*. N.Potomac, MD: Larstan Publishing Inc., 2006.

Smith, Ron and Scott Knight, "Applying Electronic Warfare Solutions to Network Security." *Canadian Military Journal* 6, no. 3 (Autumn 2005): 49-58. http://www.journal.forces.gc.ca/vo6/no3/electron-eng.asp.

Sokolow, David and Maren Leed. *Seizing the Wireless Advantage: Addressing an Increasingly Congested and Contested Electro-Magnetic Spectrum*. Washington, DC: Center for Strategic and International Studies, October 2010. http://csis.org/files/publication/101018_seizing_wireless_advantage_final2.pdf.

Stavridis, James G. and Elton C. Parker III. "Sailing the Cyber Sea." *Joint Forces Quarterly* 65 (2nd Quarter 2012): 61-67.

The Economist. "Organized Crime Hackers Are The True Threat To American Infrastructure." March 11, 2013. Last accessed 2 April 2013. http://www.businessinsider.com/organized-crime-hackers-are-the-true-threat-to-american-infrastructure-2013-3.

Thompson, Marcus, Brigadier. "The Cyber Threat to Australia." *Australian Defence Force Journal* 188 (2012): 57-67.

Turcotte, Guy. Presentation slides, "DRDC Cyber Defence S&T Program: An Overview." October 9, 2012. Last accessed 2 April 2013. http://www.cyber.st.dhs.gov/wp-content/uploads/2012/10/Day-1.08-Part-1-Canada-Turcotte.pdf.

United Kingdom. Government of the United Kingdom. *A Strong Britain in an Age of Uncertainty: The National Security Strategy*. London, UK: Cabinet Stationery Office, October 2010. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf.

———. Government of the United Kingdom. *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*. London, UK: Cabinet Stationery Office, November 2011. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

———. House of Commons Committee on Defence. "hc 106 Defence and Cyber-security – Session 2012-13," 18 April 2012. Last accessed 2 April 2013. http://www.publications.parliament.uk/pa/cm201213/cmselect/cmdfence/writev/106/m01a.htm.

———. Minister for the Cabinet Office. "Cyber Security." Last accessed 2 April 2013. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf.

———. Ministry of Defence. *Strategic Trends Programme: Future Character of Conflict.* Shrivenham, UK: Development, Concepts and Doctrine Centre, February 2010.

http://webarchive.nationalarchives.gov.uk/20121026065214/http://www.mod.uk/NR/rdonlyres/A05C6EB5-5E8F-4115-8CD6-7DCA3D5BA5C6/0/FCOCReadactedFinalWeb.pdf.

———. Ministry of Defence. *Global Strategic Trends – Out to 2040*, 4th Edition. Shrivenham, UK: Development, Concepts and Doctrine Centre, 2010. https://www.gov.uk/government/publications/dcdc-global-strategic-trends-programme-global-strategic-trends-out-to-2040.

———. Ministry of Defence. *Joint Doctrine Publication 0-01: British Defence Doctrine*, 4th Edition. Shrivenham, UK: Development, Concepts and Doctrine Centre, November 2011. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/33697/20111130jdp001_bdd_Ed4.pdf.

———. Ministry of Defence. *Joint Concept Note 2-12: Future Land Operating Environment*. Shrivenham, UK: Development, Concepts and Doctrine Centre, May 2012. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/33688/20120829jcn2_12_floc_u.pdf.

———. Ministry of Defence. "Defence Cyber Operations Group." Last accessed 2 April 2013. http://www.google.ca/url?sa=t&rct=j&q=defence%20cyber%20operations%20group&source=web&cd=2&ved=0CDoQFjAB&url=http%3A%2F%2Fwww.science.mod.uk%2Fcontrols%2Fgetpdf.pdf%3F606&ei=JQ_zUJHMBqbc2QWo-oCwBA&usg=AFQjCNHy4kB9a-T6IlEVKybfV_HxZHHnDA&bvm=bv.1357700187,d.b2I.

United States and Canada. Department of Homeland Security and Public Safety Canada. *Canada-United States Action Plan for Critical Infrastructure*. 2010. Last accessed 2 April 2013. http://www.dhs.gov/xlibrary/assets/ip_canada_us_action_plan.pdf

United States. Army Training and Doctrine Command. TRADOC Pamphlet 525-7-8, *Cyber Operations Concept Capability Plan 2016-2028.* Fort Leavenworth, KS: U.S. Army Capability Integration Centre, 22 February 2010. http://www.tradoc.army.mil/tpubs/pams/tp525-7-8.pdf.

———. Army War College. *Information Operations Primer*. Carlisle, PA: US War College, November 2011. http://www.carlisle.army.mil/usawc/dmspo/Publications/Information%20Operations%20Primer%20AY12%20Web%20Version.pdf.

———. Chairman of the Joint Chiefs of Staff. *The National Military Strategy for Cyberspace Operations (Unclassified).* Washington, DC: Department of Defense, December 2006. http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf.

———. Department of Defense. JP 3-0, *Joint Operations*. Washington, DC: Department of Defense, 11 August 2011. http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf.

———. Department of Defense. JP 3-13, *Information Operations*. Washington, DC: Department of Defense, 27 November 2012. http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.

———. Department of Defense. JP 3-13.1, *Electronic Warfare*. Washington, DC: Department of Defense, 08 February 2012. http://info.publicintelligence.net/JCS-EW.pdf.

———. Department of Defense, JP 6-0, *Joint Communications System*. Washington, DC: Department of Defense, 10 June 2010. http://www.dtic.mil/doctrine/new_pubs/jp6_0.pdf.

———. Department of Defense, JP 6-1, *Joint Electromagnetic Spectrum Management Operations*. Washington, DC: Department of Defense, 20 March 2012. http://www.dtic.mil/doctrine/new_pubs/jp6_01.pdf.

———. Department of Homeland Security. "Cyber Storm: Securing Cyber Space." Last accessed 2 April 2013. http://www.dhs.gov/cyber-storm-securing-cyber-space.

———. Executive Office of the President of the United States. *The Comprehensive National Cybersecurity Initiative.* 2 March 2010. http://www.fas.org/irp/eprint/cnci.pdf.

———. Federal Communications Commission. *Connecting America: The National Broadband Plan*. March 2010. http://www.broadband.gov/download-plan/.

———. Federal Communications Commission. "GPS, WiFi, and Cell Phone Jammers: Frequently Asked Questions (FAQs)." Last accessed 2 April 2013. http://transition.fcc.gov/eb/jammerenforcement/jamfaq.pdf.

———. Government Accountability Office. GAO 10-230T, *Statement for the Record to the Subcommittee on Terrorism and Homeland Security, Committee on the Judiciary, US Senate; Cybersecurity: Continued Efforts are Needed to Protect Information Systems from Evolving Threats.* November 17, 2009. Last accessed 2 April 2013. http://www.defense.gov/home/features/2010/0410_cybersec/docs/d10230t.pdf

———. National Intelligence Council. *Global Trends 2025: A Transformed World*. Washington, DC: Director of National Intelligence, 2008. http://www.aicpa.org/research/cpahorizons2025/globalforces/downloadabledocuments/globaltrends.pdf.

———. National Security Agency. "Declassified UKUSA Signals Intelligence Agreement." Last accessed 2 April 2003. http://www.nsa.gov/public_info/press_room/2010/ukusa.shtml.

———. White House. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. Washington, DC: White House, May 2009. Last accessed 2 April 2013. http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

———. White House. *International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World*. Washington, DC: White House, May 2011. Last accessed 2 April

2013. http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

——— . White House. “President Obama Details Plan to Win the Future through Expanded Wireless Access,” February 10, 2011. Last accessed 2 April 2013. http://www.whitehouse.gov/the-press-office/2011/02/10/president-obama-details-plan-win-future-through-expanded-wireless-access.

Valeriano, Brandon and Ryan Maness. “Persistent Enemies and Cyberwar: Rivalry Relations in an Age of Information Warfare.” In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, edited by Derek S. Reveron, 139-172. Washington, DC: Georgetown University Press, 2012.

Valiquet, Dominique. *Cybercrime: Issues*, Publication No. 2011-36-E. Ottawa: Library of Parliament, 5 April 2011.

Verton, Dan. *Black Ice: The Invisible Threat of Cyber-Terrorism*. Emeryville, CA: McGraw-Hill, 2003.

Weston, Greg. "Fake parts in Hercules aircraft called a genuine risk." (CBC News, 9 January 2013). Last accessed 2 April 2013. http://www.cbc.ca/news/canada/story/2013/01/09/f-vp-weston-hercules-counterfeit-chinese-parts.html.

Wingfield, Thomas C. *The Law of Information Conflict: National Security Law in Cyberspace*. Falls Church, VA: Aegis Research Corporation, 2000.

Wingfield, Thomas C. “Legal Aspects of Offensive Information Operations in Space.” Falls Church, VA: Aegis Research Corporation, n.d. Last accessed 2 April 2013. http://www.au.af.mil/au/awc/awcgate/dod-io-legal/wingfield.pdf.

Yap, Jamie. “South Korea army, university to start cyberdefense major.” Last accessed 2 April 2013. http://www.zdnet.com/south-korea-army-university-to-start-cyberdefense-major-2062300991/.