CANADIAN FORCES COLLEGE / COLLÈGE DES FORCES CANADIENNES
JCSP 35 / PCEMI 35

MASTER OF DEFENCE STUDIES RESEARCH PROJECT

EVALUATING CANADA'S CYBER SEMANTIC GAP

By /par LCol/lcol Francis Castonguay

Abstract

This dissertation examines the Cyber environment from a Canadian perspective and argues that the Canadian Forces (CF) must deliver the Cyber Operations capabilities required to support the Canada First Defence Strategy (CFDS). In evaluating Canada's Cyber semantic gap, a comprehensive overview of the Cyber environment is outlined, including a detailed discussion of terminology and doctrinal issues, computer network operations, the threats, vulnerabilities, risks and trends relating to public infrastructure, the military, businesses and individuals. In assessing the roles and responsibilities across the various Government of Canada (GC) departments, a historical perspective is given of the progress since the publishing of the 2004 National Security Policy. The slow start in establishing clear governance structures, developing policies and implementing effective proactive solutions to the Cyber threat in Canada is shown to have a new sense of urgency for the GC. Related to policy difficulties, the operational and criminal legal issues highlight the complexities and immaturity of understanding of the Cyber environment and its regulation. The Canadian Forces Network Operations Centre (CFNOC) role and mandate is clearly outlined as a valuable and essential capability for the GC as a national Computer Network Defence (CND), Computer Network Exploitation (CNE) and Computer Network Attack (CNA) capability. However, additional resources will be required to fully execute its mandate of proactive Cyber Operations as required by the CFDS.

Table of Contents

In the old days, people robbed stagecoaches and knocked off armoured trucks. Now they're knocking off servers. ~Richard Power

Some people can hack it, others can't. ~Author Unknown

CHAPTER I – INTRODUCTION

The advent of networked devices in the fabric of modern society dates back only two decades.[1] Prior to this, technology grew in relatively independent streams that did not mix until modems and packet-switching protocols (TCP/IP & OSI) entered the scene commercially in the early 1990's.[2] This innovation connected standalone computers into networks that piggy-backed onto the extensive and reliable 100 year old circuit-switched telephone networks. Since this initial marriage of technologies, information technology and telecommunications have reached a new level of integration and are now collectively called Information and Communications Technology (ICT). In fact, they have fused to such an extent that it created a 180 degree shift from the initial paradigm of voice-only to data-only networks. Computer networks have proliferated globally to such a degree that they no longer rely upon modems or telephone lines to operate. Telephone appliances have even transformed into software appliances through the innovation of Voice over Internet Protocol (VoIP). VoIP software can be installed onto a laptop that is connected wirelessly to the Internet and your plain old hardware telephone is now replaced by an application riding on a computer network. The

---

[1]Leonard Kleinrock, "Information Flow in Large Communication Nets", http://www.lk.cs.ucla.edu/LK/Bib/REPORT/PhD/; Internet; accessed 3 Mar 2009. The thesis of TCP first was published by Leonard Kleinrock on 31 May, 1961 as part of his PHD thesis at MIT He developed this more efficient transfer protocol to improve on the throughput of that used by circuit-switched telephone networks. However, publically-available Internet services became widespread only in the early 1990's with the creation of Simple Mail Transfer Protocol (SMTP) which enabled e-mail as we know today.

[2]Vint Cerf, Internet Society. "A Brief History of the Internet"; 10 December 2003. http://www.isoc.org/internet/history/brief.shtml; Internet; accessed 8 April 2009.

implications of this convergence have raised the spectre of an entire new set of previously impossible outcomes including having voice networks be vulnerable to computer network attacks. This is only one of the many implications from a defence and security perspective that needs to be addressed.

This growth in scale of ICT has also been matched by increased reliance upon communications and information systems. The enabling power of ICT has created synergies and power at the individual level that used to be reserved to state organizations. Low cost and highly mobile wireless devices riding over global Internet infrastructure have created the so-called information age, characterized by billions of highly interconnected devices and people. One source defines complexity as the sum of interdependencies plus change.[3] Computer networks that provide interconnectivity overlaid with collaboration and social networking tools have revolutionized how and with whom we communicate, collaborate and generate knowledge. This, in turn, has elevated our expectations and the pace of innovation on these new Internet tools. This complexity has also meant that regulatory and governance issues continue to lag behind this innovation. Despite the mounting evidence of Cyber-based destructive attacks, businesses and governments are still only at the stage of creating Business Continuity Plans (BCP) and Critical Infrastructure Protection (CIP) plans dealing primarily with physical outages or disruptions to IT infrastructures.[4] The need for the development of plans to mitigate or respond to the potential debilitating effects in the Internet or Cyber environment has yet to be integrated in Canadian BCP and CIP planning. The level of

---

[3]Myriam Dunn Cavelty, *Cyber-Security and Threat Politics : US Efforts to Secure the Information Age* (Milton Park, Abingdon, Oxon ; New York: Routledge, 2008), 17.

[4]Government Operations Centre Business Continuity Planning guidelines. http://www.publicsafety.gc.ca/prg/em/gds/bcp-eng.aspx; Internet; accessed 2 March 2009.

complexity associated with defining the linkages and dependencies of government and critical services upon the Cyber infrastructure is not a trivial task, particularly as more Internet-enabled devices with greater functionality permeate our society.

The interdependencies between technology and the conduct of daily business activities are inextricably linked and increasingly have direct impacts to our individual lives. One such example is Ontario's power distribution system which is being converted to a Smart Grid system. This system will connect homes, power meters and electrical appliances over the Internet, enabling homeowners to adjust their power consumption remotely via the web.[5] The power company will also have the ability to adjust individual household thermostat settings automatically in order to reduce the overall load on the power grid in times of peak demand. This level of interconnectivity and feedback between devices and networks can be characterized as complex and adaptive.[6] The complexity arises from the number of connections between devices in the network as well as the potential for previously unexploited uses and permutations of this interconnectivity. The deduction of this example is a new paradigm in which the power grid can regulate the thermostat, not just the opposite. This shift in the relationship between supplier and customer can lead to many new possible outcomes, both with positive and potentially negative effects. The additional convenience for consumers to control their electric bills remotely or for power companies to prevent blackouts using the Internet infrastructure also comes at the risk of potential Cyber-based attacks and exploitation.

---

[5]Forum Independent Electricity System Operator, "Enabling Tomorrow's Electricity System: Report of the Ontario Smart Grid Forum", http://www.ieso.ca/imoweb/pubs/smart_grid/Smart_Grid_Forum-Report.pdf; Internet; accessed 18 February 2009).

[6]Yaneer Bar-Yam, *Making Things Work: Solving Complex Problems in a Complex World*. Cambridge, MA, USA; NECSI, 2004, 71.

As we gradually gain an appreciation of the complexity and consequences of this dependence upon the Internet in our daily lives, our understanding of the implications of information age technology in matters of national security and national defence is also nascent. One of the first true Cyber events that highlighted our dependencies to ICT across public and private sectors was the Year 2000 (Y2K) issue.[7] Operation ABACUS was the Canadian Forces (CF) proactive response to prepare for any Y2K-induced critical infrastructure failure scenario requiring special assistance beyond the resources of first responders.[8] The lack of Y2K doomsday failures was largely due to the concerted, world-wide efforts on the part of both the public and private sectors to commit significant, and in many cases, disproportionate resources to address this issue in a timely manner.[9] With the absence of Y2K catastrophes, this raises the question of whether the next planned Cyber-based event will be taken as seriously or if there will be scepticism related to the return on investment to protect against new Cyber threats.

One foreseeable event that will certainly affect the Internet in a fundamental way will be the future implementation of Internet Protocol version 6 (IPv6).[10] This will implement a

---

[7]Bill Gates made an efficiency choice of allocating only two digits in memory to represent the calendar year in the initial versions of the Microsoft operating system software, but it was not until 1995 that the Y2K problem was recognized. Extensive effort and money was spent world-wide to update all software applications that relied on the Microsoft Windows date field. Entire software businesses thrived for several years leading up to January 2000 to certify software and hardware platforms as "Y2K compliant". Media coverage of the doomsday scenarios such as planes falling out of the sky never materialized.

[8]Canada. Department of National Defence. "Backgrounder CDS / DM Message Op ABACUS Successes Go Beyond Year 2000", http://www.forces.gc.ca/site/news-nouvelles/view-news-afficher-nouvelles-eng.asp?id=59; Internet; accessed 2 March 2009.

[9]Ed Yourdon. Y2K success lessons. *Computer World*. http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=Default&articleId=40853&taxonomyId=0&pageNumber=1; Internet; accessed 8 Apr 2009.

[10]ICANN. "ICANN Strategic Plan July 2008 – June 2011", 8. http://www.icann.org/en/strategic-plan/strategic-plan-2008-2011.pdf; Internet; accessed 20 March 2009. ICANN is the organization responsible for the technical rollout of IPv6. The planned upgrade from 2008 to 2011 to the current IP address scheme will

new standard format for IP addresses which will allow the increase of the total number of IP-connected devices. IPv6 will affect the entire architecture of the Internet and necessitate infrastructure hardware replacement and software application updates. The challenge will be to implement this major change while remaining compatible with existing devices and applications that use the current IPv4 standard whilst ensuring throughput, reliability, availability and integrity.[11] The deductions from this change include new opportunities to exploit vulnerabilities during the transition period and an increase in complexity due to the increasing number of devices connected to the world-wide-web. "Metcalfe's Law states that the value of a communication system grows as the square of the number of users".[12] The implication of this law for the Internet is that IPv6 will be vital in enabling the expansion of the number of networks, nodes and links. Raising attention to Cyber security issues that fall out from the increasing growth and complexity in the Cyber environment remains a challenge, but various shocking cyber-based events serve to raise the level of awareness among decision makers regarding upcoming challenges and threats.

Multiple incidents of consumer profile and credit card information theft from unprotected retail store databases have exposed millions of customers to fraud.[13] Some businesses such as banks have also been attacked, but many incidents, when detected are not

---

expand the number IP addresses, similar to the move of telephone dialing plans from seven to 10-digit dialing with one large difference, telephone switches already knew how to route calls with 10 digits.

[11]Doug Beizer, "IPv6: 3 more big steps to the promised land", *Federal Computer Week*, 6 February 2009. http://fcw.com/Articles/2009/02/09/IPv6-Next-Steps.aspx; Internet; accessed 18 February 2009.

[12]Myriam Dunn Cavelty, *Cyber-Security and Threat Politics : US Efforts to Secure the Information Age* (Milton Park, Abingdon, Oxon ; New York: Routledge, 2008), 17.

[13]Michigan Department of State. "Information for TJ Maxx Customers". http://www.michigan.gov/sos/0,1607,7-127-1640_9150-165939--,00.html; Internet; accessed 8 April 2009.

reported for fear of losing public and shareholder trust.[14] Likewise, there are classified examples against the US military and other government agencies that are not normally publicized for security reasons.[15] One notable Cyber incident in the April-May 2007 timeframe focused Distributed Denial of Service (DDoS) attacks against the state of Estonia, crippling businesses and government operations for several weeks.[16] This incident has raised questions about the legal definition of an attack, the use of force and cross-border or jurisdictional issues as they apply to the Cyber environment. Initial questions arose as to whether the true intent of the attack was military, criminal or simply online activism. "However, intent is often very difficult to determine and, without knowing it, intent is very hard to defend against."[17] This lack of knowledge of the intent or the true source of the attack emphasized the problem of blurring lines between security and defence sectors. It took almost two years to clarify; only then could charges be laid against four individuals for what is being termed as online rioting, not an attack.[18] Back in 2007, no one knew if the alleged attack was state-sponsored and this caused serious concerns for the North Atlantic Treaty Organization (NATO) regarding its responsibility to intervene in the defence of an Alliance member under

---

[14]Robert Vamosi, "World Bank under cyberattack?", *cnet news*, 10 October 2008. http://news.cnet.com/8301-1009_3-10063522-83.html; Internet; accessed 8 April 2009.

[15]Security Focus, "U.S. military flags China cyber threat", *SecurityFocus.com*. http://www.securityfocus.com/brief/696; Internet; accessed 8 April 2009.

[16]Gadi Evron, "Battling Botnets and Online Mobs Estonia's Defense Efforts during the Internet War", *Science & Technology*. (Winter/Spring 2008) [journal online]; available from http://www.ciaonet.org/journals/gjia/v9i1/0000699.pdf; Internet; accessed 19 February 2009.

[17]Orrick White, *Understanding the Human Dimension in 21st CenturyConflict/Warfare: The Complexities of Human-with-HumanRelationships* DRDC Corporate TR 2008-004, , vii. August 2008 http://pubs.drdc.gc.ca/inbasket/owhite.080826_0858.p529860.pdf; Internet; accessed 3 March 2009.

[18]Gadi Evron, "Battling Botnets and Online Mobs Estonia's Defense Efforts during the Internet War", *Science & Technology*. (Winter/Spring 2008), 128. [journal online]; available from http://www.ciaonet.org/journals/gjia/v9i1/0000699.pdf; Internet; accessed 19 February 2009.

the provisions of Article V.[19] NATO responded in 2008 by agreeing to stand-up the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn Estonia, in an attempt to be better prepared for the future.[20] The Cyber Defence Management Agency (CDMA) was also created in Casteau, Belgium.[21]

The lesson learned from this Cyber event was that a highly Internet-connected country, when attacked, was unable to halt this highly focused Cyber attack on its own. Shutting-down the attacks required not only the assistance of Estonian Internet Service Providers (ISPs) and telecommunications companies, but also that of other countries.[22] A contributing factor in the Estonia case was an architecture based upon foreign-based ISPs, limited number of Internet access points and the large number of unprotected personal computers in Estonia with broadband Internet access. Canada could benefit from Estonia's lessons which they have captured and applied through their Cyber Security Strategy.[23] Some Canadian security experts

---

[19]North Atlantic Treaty Organization, *The North Atlantic Treaty*, Washington D.C., 4 April 1949. http://www.nato.int/docu/basictxt/treaty.htm; Internet; accessed 2 March 2009. Under NATO's Charter, Article V stipulates that "…an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area."

[20]NATO, "NATO opens new centre of excellence on cyber defence". www.nato.in/docu/update/2008/05-may/e0514a.html; Internet; accessed 15 April 2009.

[21]IBLS, "Internet Law - NATO Agrees to Create Cyber Defence Management Authority", 15 May 2008. http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=2054; Internet; accessed 19 February 2009.

[22]Gadi Evron, "Battling Botnets and Online Mobs Estonia's Defense Efforts during the Internet War", *Science & Technology*. (Winter/Spring 2008), 124. [journal online]; available from http://www.ciaonet.org/journals/gjia/v9i1/0000699.pdf; Internet; accessed 19 February 2009.Four Computer Emergency Response Teams (CERT) from Estonia, Germany, Finland and Slovenia and other global contacts were involved.

[23]Estonia, "Estonia Cyber Security Strategy" http://www.mod.gov.ee/static/sisu/files/Estonian_Cyber_Security_Strategy.pdf; Internet; accessed 19 February 2009.

have independently concluded that the only way to effectively defend against hostile Cyber attacks requires a proactive posture, not just a defensive or passive approach.[24] Research at the Royal Military College (RMC) has also argued that "a reactive-oriented network defence policy based solely on perimeter defences is not sufficient to properly safeguard IT infrastructure".[25] As it will be demonstrated, identifying and determining the intent of an attacker prior to an actual attack are essential and requires special Cyber capabilities.

For Canada, there is much work yet to be accomplished to address Cyber security across all government departments. The Canadian government has launched several national-level policy and Cyber-security initiatives to better deliver secure online services to Canadians.[26] However, this is only a small aspect among a host of Cyber issues. There is an intent to develop a National Cyber-security Strategy[27] and parliamentary committees have started the process of establishing a Cyber plan, but Canada has been slow at creating a policy that can be translated into actual capabilities.[28] The lack of investment in Cyber-related initiatives is a telling indicator of the maturity level of our current thinking about the Cyber environment. This has only recently changed with the release of the Canada First Defence

---

[24]David McMahon, "Proactive Cyber Defence - Forecasting the Perfect Storm", 23 November 2008.

[25]Sylvain Leblanc and Scott Knight, "Engaging the Adversary as a Viable Response to Network Intrusion", Workshop on Cyber Infrastructure Emergency Preparedness Aspects, Ottawa, 21-22 April 2005; http://tarpit.rmc.ca/knight/papers/IO%20Counter-measures.doc; Internet; accessed 20 January 2009.

[26]Public Works Government Services Canada, "Secure Channel." http://www.tpsgc-pwgsc.gc.ca/apropos-about/fi-fs/cvcp-sc-eng.html; Internet; accessed 2 March 2009. Secure Channel's primary goals are to provide citizens and businesses with secure, private and high-speed access to all federal government's on-line services, and to provide an environment that enables and encourages departments to integrate with federated common services.

[27]Chris Conrath, "Ottawa Commits to cyber-security strategy", *IT World*, 14 May 2004. http://www.itworldcanada.com/a/ComputerWorld/df89791d-97aa-4b4a-b3f4-b4963ba0f0b5.html; Internet; accessed 11 March 2009.

[28] Canada. Privy Council Office, *Securing an Open Society : One Year Later : Progress Report on the Implementation of Canada's National Security Policy* (Ottawa: Privy Council Office, 2005), 53, 58, xv.

Strategy (CFDS) in June 2008 which, for the first time, explicitly made the link between the Canadian military and the core capabilities required in defending against cyber attacks:

> 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. [29]

CFDS is a major reinvestment in modernising the CF over the next 20 years to procure replacement capabilities for the Army, Navy and Air Force, but has yet to identify any Cyber capabilities. Fortunately, there will be follow-on opportunities to refine the list of capability requirements when CFDS is revisited within the next two years. This leaves very little time to provide sound military advice for future Defence investments in Cyber Operations capabilities.

Cyber Operations capabilities have been categorized in various military concepts and doctrines; these are commonly associated with terms such as Computer Network Operations (CNO) or Cyber Operations. This paper argues that the CF must deliver the Cyber Operations capabilities required to support the CFDS strategy in the Cyber environment. In support of this thesis, Chapter II, serves as a primer to demystify and clarify the Cyber environment in a Canadian context. Chapter III addresses governance issues, the responsibility for Cyber Operations and raises some key legal issues associated with the conduct of Cyber Operations; it highlights the shared, multi-departmental and multinational nature of conducting Cyber Operations. Cyber Operations capabilities will be shown as essential to determining the adversarial intent and hence determining the appropriate government department to address specific Cyber threats. Chapter IV identifies the CF's role in the Cyber environment against the six core missions assigned to the CF in the Canada First Defence Strategy (CFDS) and

---

[29]Canada. Department of National Defence, "Canada First Defence Strategy", June 2008, 7. http://www.army.forces.gc.ca/DLCD-DCSFT/pubs/sdca/June18_0910_CFDS_english_low-res.pdf ; Internet; accessed 19 February 2009.

addresses force generation and sustainment issues for the CF with respect to establishing Cyber Operations capabilities. Chapter V concludes that there must be a strong CNO capability within the CF that is integrated with the CND and CNE capabilities that are resident across the various GC departments, international partners and industry so as to enable an effective CNA capability. It also recommends that a similar study of the Cyber environment be completed at the classified level to ensure that a complete Cyber environment assessment.

CHAPTER II - THE CYBER ENVIRONMENT

Terminology

Military concepts relating to the use of Information and Communications Technology (ICT), also referred to as Communications and Information Systems (CIS) [30] are relatively new and terminology that has emerged has suffered a lack of precision and divergent meanings. As with many newer concepts and technologies, an initial low level of general understanding and a high potential for misinterpretation is quite normal. Time and experience is required before the necessary maturity of new terms settles into a coherent set of definitions and concepts in popular language.

NATO, Australia, Canada, the UK and the US have created Information Operations doctrine that are at different stages of maturity and consequently do not all agree in spite of efforts to increase interoperability and standardized terminology. In the Defence Research and Development Centre (DRDC) – Toronto report, their findings point out that the incongruence between various US doctrinal documents add to the confusion surrounding the concepts of Information Operations and Influence Operations. They note that within NATO, the conceptual basis of Influence Operations is British, with American implementation.[31] In Canada, the lack of CF resources dedicated to doctrine development has resulted in many cases in opting to defer to NATO whenever our doctrine was lacking:

> While the new Canadian Land Force doctrine provides an immediate solution to the lack of Canadian doctrine on influence operations, the practice of adopting alliance or

---

[30]NATO AAP-6 defines CIS as a collective term for communication systems and information systems.

[31]Keith Stewart. DRDC Toronto. "Influence Operations: Historical and Contemporary Dimensions", DRDC Toronto CR-2007-126, 31 July 2007. http://cradpdf.drdc.gc.ca/PDFS/unc69/p528894.pdf; Internet; accessed 15 April 2009.

other nations' doctrine without a careful analysis of one's national experience has its risks.[32]

The NATO terminology publication, the AAP-6 is the product of the Alliance's consensus and is a key source used for many CF-wide definitions. The Canadian Department of National Defence's (DND's) official source of military terminology is the Defence Terminology Databank (DTB); unfortunately, DND has yet to populate its databank with terminology relating to Cyber. For this paper, Canadian Cyber definitions were therefore drawn from select draft Canadian documents and the Concise Oxford dictionary.[33]

The US DoD has developed the concept of the Information Environment, which differs from the Cyber Environment. As articulated by Neil Chuka, the theoretical construct of the Information Environment has its problems because it limits Information Operations to the physical domain and omits the psychological dimension.[34] Unfortunately, NATO does not even offer a definition for Information or Cyber, so there is an evident need to bring clarity to the term Cyber.[35]

Let us first contextualize the concept of Cyber Environment through its origin and modern interpretation. The morpheme Cyber derives from the word cybernetics, a 1948 concept that drew upon another new concept, that of systems theory. Considered the precursor

---

[32]*Ibid,* 8.

[33]The Concise Oxford Dictionary is the primary source of terminology for the CF whenever there is no NATO-agreed term.

[34]Neil Chuka, "Confusion and Disagreement: The Information Operations Doctrine of the US, the US, AUS, CA and NATO", September 2007, 7.

[35]NATO, "NATO Glossary of Terms and Definitions", AAP-6. http://www.nato.int/docu/stanag/aap006/aap-6-2008.pdf; Internet; accessed NATO AAP-6 mentions the word cyber only once as a note within a definition: A computer network attack is a type of cyber attack.

to the current complexity theories, cybernetics is a theory of communications and control of regulatory feedback in living beings and machines built by humans.[36] Clearly, cybernetics means something entirely different than what it represents today. Cyber very commonly refers to all things related to ICT or CIS, but there are narrower interpretations that connect it strictly to computers or computer networks.[37] So the common denominator appears to be computers, but as Internet users grow familiar with connecting other devices to the Internet, the common meaning of Cyber is likely to expand[38]. Despite the gap in usage and meaning of Cyber[netics], its pervasive use in common language garners a growing understanding that is irreversible. The second word in the compound term, environment, the DTB simply copied the NATO definition, "The surroundings in which an organization operates, including air, water, land, natural resources, flora, fauna, humans, and their interrelation."[39] The definition is somewhat wanting if it is to consider other domains such as Cyber or Space. A remedy could be to replace the word "surroundings" with either "medium" or "area of operation", it would then be applicable to the Air/Land/Maritime physical domains as well as other physical areas of military significance such as Space and Cyber. The Concise Oxford offers a computing version of the word environment: "the overall structure within which a user, computer, or program operates".[40] Given the current state of these definitions, the combination of Cyber

---

[36]Myriam Dunn Cavelty, *Cyber-Security and Threat Politics : US Efforts to Secure the Information Age* (Milton Park, Abingdon, Oxon ; New York: Routledge, 2008), 16.

[37]Concise Oxford Dictionary Online. http://www.askoxford.com/concise_oed/cyber?view=uk; Internet; accessed 3 March 2009. Definition of Cyber: **combining form** relating to information technology, the Internet, and virtual reality: *cyberspace.*

[38]A growing number of consumer electronics are IP-addressable or have a USB connector that enables connectivity to computers that are on the Internet. Some examples include digital and video cameras, music players, interactive multi-player games, alarm systems, remote monitoring systems - biometric and mechanical, positioning systems, etc…

[39]Canada. Department of National Defence. Defence Terminology Databank http://terminology.mil.ca/index-eng.asp; Internet; accessed 3 March 2009.

with Environment as a unique or separate domain, medium or environment in its own right is somewhat imprecise. Despite the potential for debate, there is still merit in pursuing the intellectual discussion to elevate our collective understanding and reach a consensus regarding the Cyber Environment.

Defining the Cyber Environment

The Chief of Force Development (CFD) as the lead joint concept developer for the CF has articulated the concept of Cyber along with Space, Special Operations, Air, Maritime and Land environments in which to conduct operations.[41] CFD has yet to define the term Cyber Environment, but it is imperative for the Cyber concepts to become grounded on sound intellectual foundations. Because it is a relatively new conceptual term for the CF, it will likely not be accepted for doctrinal[42] use for some time however, the first step would be to insert a definition into the DTB. The new definition would need to account for the physical component as well as the influence component. Without the physical assets or platform(s) upon which to operate, it could hardly qualify as an environment, so the network hardware devices, cabling, routers, servers, software, etc. should be inherent components of the Cyber Environment. Why is it even necessary to consider it as an environment rather than just an enabler to existing environments? Just as it is possible to conduct operations strictly in the Air,

---

[40]Concise Oxford Dictionary Online. http://www.askoxford.com/concise_oed/environment?view=uk; Internet; accessed 3 March 2009. Definition of Environment.

[41]Chief Force Development (CFD) presentation by MGen Beare given to JCSP 35, CFC Toronto, 10 November 2008.

[42]Canada. Department of National Defence. CF Doctrine. http://www.cfd-cdf.forces.gc.ca/sites/page-eng.asp?page=834; Internet; accessed 25 February 2009. In the CF, doctrine is defined as the "fundamental principles by which military forces guide their actions in support of objectives. It is authoritative but requires judgment in application." In general, doctrine describes the factors involved and provides the broad "how" to plan and execute operations or military activities.

Land or Maritime environment, operations can also be conducted entirely within the Cyber realm, with no assistance from the other environments. To capture the doctrine and techniques associated with this environment requires a conceptual framework for the Cyber Environment.

Unfortunately, the term Cyber can be confused with the term virtual because definitions of virtual combine physical and non-physical entities rather than focussing on the non-physical.[43] For example, the term "virtual keyboard" cited in the Merriam-Webster dictionary fails to meet the definition of virtual. In the case of a software-based touch-screen replica of a hardware keyboard, it is still technically a hardware keyboard as opposed to a simulation only, it is just another hardware and software combination.[44] Likewise, activities in the Cyber Environment may appear to be strictly ethereal (virtual) when the actual physical aspects are ignored. Take for example video conferencing over the Internet using an application such as Skype.[45] Many would describe a remote video connection as virtual; however, there are various layers of physical hardware and software between the two video connections. Hence, it would be more accurate to describe the video conference as a Cyber connection than a virtual one.[46] A more purist or precise definition of the term virtual for computers would limit its scope to computer simulations or representations that have no physical manifestation, such as

---

[43]Merriam-Webster Dictionary Online. http://www.merriam-webster.com/dictionary/virtual; Internet; accessed 25 February 2009. Defines Virtual as : being on or simulated on a computer or computer network <print or virtual books> <a virtual keyboard>: as a: occurring or existing primarily online <a virtual library> <virtual shopping> b: of, relating to, or existing within a virtual reality <a virtual world> <a virtual tour>.

[44]A simulated keyboard would use a touch-screen as hardware instead of actual keys and software would replicate the functionality of the keys.

[45]www.skype.com

[46]Concise Oxford Dictionary Online. http://www.askoxford.com/concise_oed/virtual?view=uk; Internet; accessed 2 March 2009. Definition of **Virtual**: not physically existing as such but made by software to appear to do so.

avatars in the online game Second Life.[47] This distinction in definition is important to properly classify the nature of the Cyber Environment and to appreciate the methods of attack and influence. Finally, beyond the challenge of defining and explaining new terms, CFD faces the organizational resistance that is typical when new technologies and associated concepts are introduced to an organization.

The US Strategic Command is currently going through the growing pains of developing a common understanding of what is meant by Cyber as a separate domain. General Kevin Chilton, Air Force commander of the Strategic Command has equated the introduction of the Cyber domain to that of the Space domain 15 years ago. He highlighted the importance of including Cyber operations and concepts in schools to pass the knowledge to a wider community than just Cyber professionals. He added that "this is a warfighting domain everyone needs to understand … where we are going to fight jointly."[48] Another example of resistance that challenged the US Air Force prior to WW II captures the essence of the issues for the Cyber Environment:

> Picture the three-sided challenge of developing the concept of air power that Maj. Gen. Hap Arnold was faced within the years just prior to World War II. The first was controlling the air domain, which required an understanding of the science of flight and the atmosphere. The second was developing technology to operate in that domain, which necessitated an understanding of aerodynamics. The third was operating locally and projecting power through that domain, which led to an infrastructure of airfields, refueling stations and navigational capabilities. Air Force Cyber Command has similar challenges today, and its own trident of challenges to overcome. Same for space command – how to convince the existing elements that the technological innovation has created a new environment? Dedicated and robust conceptual work and collaboration with all stakeholders, experimentation & exercises with other services/environments.[49]

---

[47] http://secondlife.com/whatis/ The game Second Life would be an example of a virtual environment.

[48] Sean Gallaghar, "The Right Stuff for Cyber Warfare",*Defense Systems*, 20 October 2008. http://defensesystems.com/Articles/2008/10/The-right-stuff-for-cyber-warfare.aspx; Internet; accessed 16 February 2009. A Defense Systems interview with General Chilton.

The US DoD Cyber concepts are still immature and broader in scope than in Canada, but are a step forward in spite of a lack of joint guidance on cyberspace operations. The current US definition of cyberspace is:

> a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange data via networked systems and associated physical infrastructures. Cyberspace is a domain like land, sea, air and space and it must be defended.[50]

The US have adopted the term cyberspace rather than Cyber Environment to emphasize the territorial/physical analogy to other environments. For all intents and purposes, the two expressions are synonymous and if cyberspace more easily communicates the concept, perhaps DND should consider adopting this term. But this will require further intellectual rigor and debate to avoid the pitfall of adopting another nation's concepts without considering the Canadian context and linguistic nuances. Specifically, the danger in the US approach is that it "defines Information Operations in terms of competition for the domination of cyber-space",[51] since there is yet no proof that cyberspace domination is actually possible or even desirable.

Another area of concern is the broad reach of the US definition, although it reflects the trend in convergence of technologies and fields of expertise; it loosely combines the electromagnetic spectrum with electronics under the auspices of cyberspace. In Canada, this may have implications on existing organisations, authorities, jurisdiction and policies and further research would be required to determine if this should be the approach for the CF.

---

[49]Barry Rosenberg, "Cyber warriors". C4ISR Journal of Net-centric Warfare, Vol. 6, No. 7., pp. 30-3. http://www.isrjournal.com/story.php?F=2859662; Internet ; accessed 16 February 2009.

[50]United States Air Force. http://www.afcyber.af.mil/library/factsheets/factsheet.asp?id=10784; Internet; accessed 16 February 2009. USAF Fact Sheet Cyberspace 101 Understanding the cyberspace domain.

[51]Keith Stewart. DRDC Toronto. "Influence Operations: Historical and Contemporary Dimensions", DRDC Toronto CR-2007-126, 31 July 2007. http://cradpdf.drdc.gc.ca/PDFS/unc69/p528894.pdf; Internet; accessed 15 April 2009.

Cyber Operations

To understand Cyber Operations and CNO, it is useful to place it in context with the concept of Information Operations (IO), which in Canada has been defined as:

> actions taken in support of political and military objectives which influence decision makers by affecting other's information while exploiting (fully utilizing) and protecting one's own information.[52]

Within NATO, the IO concept is currently still in a state of flux, confounded by immature and imprecise taxonomy, which hampers the achievement of national, and to a greater extent, NATO-wide agreement. [53] This lack of agreement should at a minimum call for some measure of caution in the development of doctrine and serves as an indicator that more work and discourse is required.[54] This should not however deter the DND from having the intellectual debate that will tease out the important ideas contained at the core of this Information or Influence Operations concept. Furthermore, the debate should not be exclusively military, as argued by Sylvain Leblanc and Dr. Scott Knight:

> While originally conceived in a military context, information operations are equally relevant to the new global threat environment and can find application in critical infrastructure protection, counter-intelligence, and contending with organized criminal activity.[55]

So rather than be stymied by the ongoing IO debate, this paper makes the assumption that regardless of the outcome of the IO concept, there is a need to develop certain Cyber

---

[52]Canada. Department of National Defence. CF Information Operations B-GG-005-004/AF-010, 1998-04-15, 1-2.

[53]Neil Chuka, "Confusion and Disagreement: The Information Operations Doctrine of the US, the US, AUS, CA and NATO", September 2007, 2.

[54]Concepts are forward-looking new ideas, while doctrine is experience-based on true and tried tactics, techniques and procedures.

[55]Sylvain Leblanc, Scott Knight, "Engaging the Adversary as a Viable Response to Network Intrusion", Workshop on Cyber Infrastructure Emergency Preparedness Aspects, Ottawa, 21-22 April 2005; http://tarpit.rmc.ca/knight/papers/IO%20Counter-measures.doc; Internet; accessed 20 January 2009.

capabilities. These Cyber capabilities are encompassed in the concept of Cyber Operations, or CNO, to create tactical, operational and strategic effects in response to both the emerging and continually evolving technology that is available to both our foes and our allies. Although IO concepts are still evolving,[56] one common conclusion among NATO nations is the recognition that among the capabilities or enablers that support IO, Computer Network Operations (CNO) is a fundamental and increasingly important capability.[57] It has been argued, that although the importance of protecting the Internet infrastructure is an easy case to make, the militarization of the Internet may require further debate to expand our collective understanding of what is meant by CNO. [58] The term Computer Network Warfare (CNW) has also been proposed to describe this militarization of the Internet, using the parallel framework of existing Electronic Warfare (EW) doctrine.[59] This approach is interesting since it draws upon a mature discipline of EW operations for which procedures and policies exist. Although this is worth exploring, this paper will limit itself to the term CNO and its associated sub-disciplines, as it is being discussed within the CF currently.

Understanding begins with a common lexicon; however, the CF definition for CNO has yet to be published. A draft, unpublished, policy document provided by J6 CNO, defines CNO

---

[56]Neil Chuka,"Confusion and Disagreement: The Information Operations Doctrine of the US, the US, AUS, CA and NATO", September 2007, 8. See Neil Chuka's dissertation for a full discussion on Info Ops, which he defines as "not foremost about technology or disrupting the ability of an adversary to conduct operations; at their most basic, Info Ops, as a coordinating and integrating function, are about conceiving and synchronizing activities, both physical and psychological, to create desired effects that influence the perceptions of the target audience and affect behaviour in a desired manner."

[57]*Ibid.*, 2.

[58]Ron Smith and Scott Knight, "Applying Electronic Warfare Solutions to Network Security", Canadian Military Journal, Vol. 6, No. 3, RMC, Kingston, Autumn 2005. http://tarpit.rmc.ca/knight/papers/Applying%20Electronic%20Warfare%20Solutions%20to%20Network%20Security%20-%206%20Apr04.doc; Internet; accessed 20 January 2009.

[59]*Ibid.*, 1.

as "the phrase used to define the combined disciplines of Computer Network Defence (CND), Computer Network Exploitation (CNE), and Computer Network Attack (CNA)."[60] CND is defined as:

> an activity conducted through the use of one's own computer networks to protect, monitor, detect, analyze, and respond to unauthorized activity within computers or computer networks. [61]

CNE is defined as:

> a directed, covert activity conducted through the use of computer networks to remotely enable access to, collect information from, and / or process information on computers or computer networks.[62]

Finally, CNA is defined as:

> a directed activity conducted through the use of computer networks to intentionally disrupt, deny, degrade, or destroy adversary computers, computer networks, and / or the information resident on them.[63]

Interestingly, NATO only defines CNA[64] and CNE[65], they have no definition for CND or the overarching term CNO.

---

[60]Draft CNO Policy, 22 Apr 08 version. Attached to the CNO definition is the following Note: To ensure clarity and precision, the phrase Computer Network Operations (CNO) shall not be applied to any single subordinate CNO discipline (i.e. - to CND, CNE, and / or CNA). Rather, the phrase shall only be used to describe activities involving two or more of the subordinate CNO disciplines. When an activity falls exclusively within the scope of a particular discipline (i.e. CND, CNE, or CNA), the appropriate phrase shall be employed.

[61]*Ibid* (Draft CNO Policy, 22 Apr 08 version.) Attached to the CND definition is the following Note: Any and all computer network activity, including a CND activity, that initiates intrusive contact (transcending the level of contact available on a public access basis) with other computers or computer networks, without the permission of the owner / operator of those computers or computer networks, constitutes CNE or CNA, depending upon the form of the contact, and falls under the governance framework of the corresponding activity.

[62]*Ibid.*

[63]*Ibid.*

[64]NATO AAP-6 defines Computer Network Attack as: Action taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer network, or the computer and/or computer network itself. Note: A computer network attack is a type of cyber attack.

In light of the trends toward the convergence of technologies, it may be prudent to extend the definitions for CNO, CND, CNE and CNA beyond the current limiting realm of computers and be more inclusive of the expanding array of devices that can be interconnected with the Internet. Not only computers or ICT devices can connect directly or indirectly to the Internet, even wireless appliances should be considered in the mix.[66] Therefore, consideration should be given in the future to change the Canadian definition from Computer Network Operations to Cyber Network Operations. Since CNO is still a burgeoning concept, it will continue to be subject to intellectual debates for years to come before there is consensus on what is meant by the acronym CNO, Cyber Network Operations, Computer Network Operations or even simply Cyber Operations. This debate should not detract from the requirement for military capabilities to defend Canada within the Cyber environment. To appreciate the need to move forward with Cyber capabilities, it is useful to be aware of the trends in Cyber threats.

---

[65]NATO AAP-6 defines Computer Network Exploitation as: Action taken to make use of a computer or computer network, as well as the information hosted therein, in order to gain advantage.

[66]Increasingly, multi-function devices such as cellular telephones and audio players contain flash drives and small, high-storage hard drives that enable the easy portability of large amounts of data. The result is an expansion of the network endpoint, since unauthorized devices can be connected to enterprise systems and authorized devices can be connected to unauthorized systems and networks. This has resulted in an increased attack surface and a higher number of potentially viable entry points for malicious code and attacks. A recent survey has suggested that over 43 percent of enterprises have little or no measures in place to address permissions or restrictions on removable media within their networks. Moreover, less than 17 percent use endpoint security measures to address the issue.40 With increases in data theft and data leakage, these devices represent a viable attack vector for attackers as they attempt to steal as much information from as many sources as possible.

Threats, Vulnerabilities and Risk

The topic of threats is tightly coupled to capabilities and therefore, before determining what capabilities are required, there is an intermediary step of assessing the threats[67] and vulnerabilities within a risk framework. Risk will always exist, the key is to balance even the most dangerous and disastrous scenario against the appropriate and realistic potential of actual occurrence. Despite the vast library of potentially calamitous threat scenarios surrounding the Cyber Environment; it is important to focus on realistic, not just sensationalistic outcomes. Crying wolf with respect to Cyber issues only serves to dilute the attention and response that this environment requires to protect individuals, businesses and governments. To determine whether a Cyber threat is imminent or whether it is a high risk, it is necessary to have knowledge of a potential attacker's identity and preconditions or intent prior to the attack.[68] As will be shown, determining the attacker's identity and intent prior to an attack is the only way to assign the appropriate resources in time to provide Cyber protection.[69] High on the priority list should be the mitigation of zero-day threats that are not detectable by security products at the network edges.[70] The importance of this capability is developed in Chapter III. Finally, an important ingredient in assessing a threat is the ability to classify the threats into categories.

Threats can be categorized into a number of available attack methods, these are described by Solce as cyber weapons, but two broad categories prevail: semantic and

---

[67]Threat = capability + intent.

[68]Symantec Internet Security Threat Report Trends for July–December 07, Volume XIII, Published April 2008, 30.

[69]David McMahon, "Proactive Cyber Defence – Forecasting the Perfect Storm", April 2008.

[70]Bell Canada. "Carrier Grade Threat and Vulnerability Intelligence", December 2008, 1.

syntactic.[71] Semantic threats are those which affect the content and accuracy of information while syntactic threats target the applications or operating system software vulnerabilities. Both semantic and syntactic threats can occur simultaneously in a single attack. A third layer must also be considered, the physical elements that comprise the Cyber Environment and the associated threats and vulnerabilities surrounding the hardware elements.[72] The hardware elements constitute the physical layer in the form of devices such as routers, network cards, computers, wires and even electromagnetic or wireless devices. The physical components differ from the other threats in they way they can be attacked – through semantic and syntactic means, but also through physical means. In large measure, the nature of the attack is dependent upon the systems being targeted. The targets of highest interest to a state traditionally are the public and private critical infrastructure, but as was learned in the Estonia attacks of 2007, business and individual home computers and networks can play a significant role and should be considered in any state threat assessment.

Trends

Symantec, an enterprise security company, has observed in their 2008 Internet Security Threat Report that the "current security threat landscape is predominantly characterized by four major trends".[73] These four trends are explored individually below to better understand the direction Cyber threats have taken in the recent past.

---

[71]Natasha Solce, "The Battlefield of Cyberspace: The Inevitable New Miltary Branch – The Cyber Force". *Albany Law Journal of Science and Technology*. #18-2008, 305.

[72]Martin C. Libicki and Rand Corporation, *Conquest in Cyberspace : National Security and Information Warfare* (Cambridge: Cambridge University Press, 2007), 8.

[73]Symantec, "Internet Security Threat Report Trends for July–December 07", Volume XIII, Published April 2008, 2.

Malicious activity has become Web-based. Attackers have adopted stealthier, more focused techniques, particularly targeting trusted social networking sites such as Facebook and MySpace.[74] They either steal user credentials or launch mass attacks which can propagate quickly through the user's social networks. Cross-site scripting vulnerabilities tend not to be patched by system administrators – only 473 of the 11,253 cases reported, making this a highly open exploit.[75] Browser plug-in vulnerability exploitation through ActiveX plug-ins is used increasingly to modify website home pages and install malicious phishing software.[76] Malicious phishing, mimicking legitimate sites with intent to extract user's personal information, such as bank account numbers and passwords increased 167% during 2007. Globally, 66% of the phishing servers were located in the US.

Attackers target end users instead of computers. Motivated by financial gain, keystroke loggers are used to extract user credentials and sensitive information rather than compromise the machine per se. Data relating to identities, credit cards, and financial details accounted for 44 percent of the information advertised on underground economy servers.

---

[74]Glenn Chapman, "Cyber crooks stalk users of social networks.", Agence France-Presse, 4 March 2009. http://www.canada.com/Technology/Cyber+crooks+stalk+users+social+networks/1351029/story.html; Internet; accessed 25 Mar 09.

[75]CGI Security. http://www.cgisecurity.com/xss-faq.html; Internet; accessed 16 April 2009. Cross site scripting (also known as XSS) occurs when a web application gathers malicious data from a user. The data is usually gathered in the form of a hyperlink which contains malicious content within it. The user will most likely click on this link from another website, instant message, or simply just reading a web board or email message. Usually the attacker will encode the malicious portion of the link to the site in HEX (or other encoding methods) so the request is less suspicious looking to the user when clicked on. After the data is collected by the web application, it creates an output page for the user containing the malicious data that was originally sent to it, but in a manner to make it appear as valid content from the website. Many popular guestbook and forum programs allow users to submit posts with html and javascript embedded in them. If for example I was logged in as "john" and read a message by "joe" that contained malicious javascript in it, then it may be possible for "joe" to hijack my session just by reading his bulletin board post. Everything from account hijacking, changing of user settings, cookie theft/poisoning, or false advertising is possible. New malicious uses are being found every day for XSS attacks.

[76]Gregg Keizer, "ActiveX bugs pose threat to Vista, Microsoft reports", *IT World.* 3 November 2008. http://www.itworld.com/windows/57174/activex-bugs-pose-threat-vista-microsoft-reports; Internet; accessed 16 April 2009.

Underground economy consolidates and matures. Outsourcing of malicious code production has become the way to efficiently exploit this underground economy. Symantec detected 711,912 new threats in 2007 compared to 125,243 threats in 2006, an increase of 468 percent, bringing the total number of malicious code threats identified as of the end of 2007 to 1,122,311. Practically two-thirds of all malicious code threats currently detected were created during 2007; a feat made possible by the emergence of organizations employing dedicated malicious code programmers. Multivariate and bulk pricing for various stolen information such as bank accounts ($10-$1000 each) or credit card numbers (($0.40-$20 each) indicates a level of market sophistication and maturity; and

Rapid adaptability of attackers and attack activity. The increased use of firewalls has limited the ability of network worms to propagate and effective file attachment blocking has reduced the popularity of mass-mailing worms. However, with the increase in the use of removable media in both at home and at the office, USB drives are a popular means to transfer files that are too large to e-mail or that consume too much bandwidth over the network. USB devices are now prime targets for virus propagation, such as the Conficker worm.[77] USB exploits such as the USB Hacksaw make it possible for data to be stolen or e-mailed from a system connected to an infected USB device.[78] Research at RMC is also exposing a novel way

[77]Felix Leder, and Tillmann Werner, "Know Your Enemy: Containing Conficker. To Tame a Malware." Last modified 7 April 2009 (rev 2), *The Honeypot Project*. http://www.honeynet.org/files/KYE-Conficker.pdf; Internet; accessed 18 April 2009. A vulnerable Windows system is generally infected with the Conficker worm via the MS08067 vulnerability, using exploit shellcode that injects the DLL into the running Windows server service. Other possible infection vectors are accessing network shares or USB drives where the malicious DLL is started via the rundll32.exe application. Once infected, Conficker installs itself as a Windows service to survive reboots.

to further misuse USB devices by using unintended two-way communications channels within the USB protocols which create a potential exploitation vector for any USB peripheral.[79]

Government attack trends reported by Symantec lists the telecommunications sector as the top target, accounting for 95 percent of all critical infrastructure attacks, up from 90 percent over 2007. Twenty-one percent of the total attacks targeting the government sector originated from the US and Denial-of-Service (DoS) attacks were the most common attack type, representing 46 percent of the top ten attacks.[80] These statistics give reason to explore the critical infrastructure threats in more detail.

Public and Private Critical Infrastructure.

According to Public Safety Canada, the list of official critical infrastructures are: Energy and Utilities; Communications and Information Technology; Finance; Healthcare; Food; Water; Transportation; Safety; Government and Manufacturing.[81] There are essentially three basic trends affecting infrastructure: 1) the growing reliance upon ICT for internal use and interaction with external systems, 2) increased complexity with accelerating technology evolution and 3) the interconnectedness of various infrastructures.[82] As a result the divide

---

[78]Tim Wilson, "USB Hacksaw Still Sharp, Expert says". *DarkReading*. 29 April 2008. http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml?articleID=211201471; Internet; accessed 16 April 2009.

[79]The Royal Military College (RMC) post-grad Computer Science research being conducted by Maj. Sylvain Leblanc and Maj. John Clark investigates the risk associated with USB devices. This novel research aims to characterize unintended two-way communications channels within the USB protocol.

[80]*Ibid*., 24.

[81]Public Safety Canada website. http://www.publicsafety.gc.ca/prg/em/nciap/about-eng.aspx; Internet; accessed 27 February 2009.

[82]Myriam Dunn Cavelty, *Cyber-Security and Threat Politics : US Efforts to Secure the Information Age* (Milton Park, Abingdon, Oxon ; New York: Routledge, 2008), 18.

between privately and publicly owned infrastructures is becoming difficult to trace. The interconnectedness permeates several layers including physical, organizational, procedural and informational.[83] All of these facets influence the methods necessary to secure any infrastructure. The security puzzle is further complicated by the varied nature of incidents: failures stem from issues internal to the system; accidents arise from external influences; and attacks upon infrastructure can be either targeted or unintentional.[84] Responses to failures, accidents or attacks will vary and demand different resources to address each one.

With the proliferation of Internet-based services connecting many aspects of Canadian affairs, arguably, the Internet infrastructure has become the hot topic in the critical infrastructure protection discourse.[85] When the Blackberry e-mail servers in Waterloo go off-line, one can argue that government and businesses alike are severely affected, if not crippled. One such incident lasted for three hours on 11 February, 2008, affecting almost all major North American mobile service providers (AT&T, Rogers, Bell, Telus, etc.) and their subscribers.[86] The impact of such outages clearly highlights just how dependent Canadian society and DND has become on their smart phones.[87] The range of services, not just physical infrastructure, is

---

[83]The physical linkages between information systems is easily appreciated, particularly when the Internet provides connectivity to infrastructure control systems as well as administrative computer networks. What is less obvious are the informational and contextual relationships and interdependencies across systems. For example, the organizational and procedural regulations and practices between utility companies from province to province or even cross-border with the US. If one company programs its distribution network to divert overflow electricity to another company's network, this has to be done through common, agreed-to procedures.

[84]*Ibid*., 20.

[85]Bell. Security, Intelligence, Law Enforcement, Public Safety and National Defence Research Bell has recorded 14,000 attack/incidents in one month directed primarily at financial and government infrastructures in Canada from the Russian Business Network (RBN) criminal organization.

[86]Stephen Lawson, "Outage knocks BlackBerry users offline". *Inforworld.com*, 11 February 2008. http://www.infoworld.com/article/08/02/11/Outage-knocks-BlackBerry-users-offline_1.html; Internet; accessed 27 February 2009.

expanding as increased functionality and availability of mobile services becomes imbedded into the fabric of our society.[88] This further reinforces not only the interdependencies but also the growing complexity of protecting the ICT infrastructure.

Within the realm of Critical Infrastructure Protection (CIP), the most visible government departments and organizations responsible for emergency services come to mind: police, ambulance and fire departments. They depend upon reliable and available ICT services in times of crisis. The CF also has the responsibility to assist in domestic emergencies, upon request, which occurs when the situation is beyond the capacity of the primary emergency organizations. This levies even higher demands for the level of robustness, availability and resilience of the ICT services that the CF depends upon. Since the mid-1990's, the push to reduce costs and receive more services using the alternate service delivery approach, DND has shifted much of its telecommunications service delivery responsibility to the private sector. First, the Telecommunications Services Renewal Project (TSRP) contract was awarded to Bell Canada in June 2000. Following TSRP was the Global Defence Network Services (GDNS)

---

[87]As of 24 March 2009, 76 Comm Gp reports (via e-mail) that there are 10,949 Blackberry devices issued to DND users, 4,554, or 41.6% are assigned to the 6,339 personnel in the NCR (number of personnel provided by CFSU(O)), the National Defence Headquarters (NDHQ). The ratio of Blackberry devices to personnel in NDHQ is 1:1.4, in other words, 71.8% of the NDHQ staff have Blackberry devices. Given that each user has to justify the operational requirement and a director of a department has to approve each demand, it is clear that these numbers indicate a significant amount of dependence on these devices.

[88]Paul Budde, "2008 Canada – Telecoms, Wireless and Broadband." 20 February 2008. http://www.marketresearch.com/product/display.asp?productid=1687223&g=1; Internet; accessed 2 April 2009.
"Forecast wireless subscribers, penetration and revenue growth - 2008 - 2013
Year / Subscribers / Penetration / Revenue ($ billion)
2008 / 21,300,000 / 64% / 16.6
2009 / 23,200,000 / 69% / 19.0
2010 / 25,300,000 / 74% / 21.6
2011 / 27,600,000 / 80% / 24.6
2012 / 30,100,000 / 86% / 28.1
2013 / 32,800,000 / 93% / 32.0"

contract which was competed and awarded to Telus on June 22nd, 2007.[89] The major change that these projects pioneered was a gradual shift of service delivery responsibility away from DND and more heavily toward contractor-provided services. This was done to decrease costs and still allow for technology upgrades by allowing the contractor to propose new solutions rather than to impose designs and hardware onto them. The obvious implication of this approach was a greater reliance on the contractor to provide, on behalf of DND, the security to these ICT infrastructures. Services and hardware previously housed within the protection of DND premises are now on contractor premises. Additionally, the dual use of the technology solutions utilised result in the sharing of platforms and facilities between DND, industry and private consumers. Our mobile services and basic communications links ride on common commercial links and platforms as opposed to dedicated services and facilities. This is not necessarily better or worse than the previous arrangement, but it represents an element of risk that requires a different mitigation and risk management strategy. To meet the demands of DND's missions, we therefore levy very high security, availability and quality demands on our service providers. We must also be vigilant regarding which new technologies are offered by the contractor and be cautious in avoiding the leading edge of technologies that have not been adequately tested to meet the stringent demands required of our mission.[90] [91]

---

[89]The Maple Leaf, Vol. 10, No. 29 http://www.forces.gc.ca/site/commun/ml-fe/article-eng.asp?id=3780; Internet; accessed 5 March 2009.

[90]DoD Instruction 8100.3, Department of Defense Voice Networks. http://www.dtic.mil/whs/directives/corres/pdf/810003p.pdf; Internet; accessed 16 April 2009. The CF operates in the harshest, most austere and extreme scenarios where mission failure is not an option. To coordinate such a large and geographically dispersed organization as the CF requires fail-safe ICT services. DND also operates an extension of two US voice networks, the Defense Services Network (DSN) and the Defense Red Switch Network (DRSN) in Canada and under the MOU agreement with DISA http://www.state.gov/documents/organization/111449.pdf ; Internet; accessed 29 March 2009, DND must comply with policies and interoperability standards of this network. Rigorous testing is performed on all equipment connected to these networks in accordance with DISA Information Assurance Test Plans http://www.disa.mil/dsn/webfiles/DISA_Information_Assurance_Test_Plan_(IATP)v3_1March_2005.pdf; Internet; accessed 16 April 2009.

The US DoD has adopted a more traditional and cautious approach of going back to having the highest level of ownership and physical control over their ICT services. The Global Information Grid (GiG) Bandwidth Expansion (BE)[92] project not only built excess growth capacity to every site but also added redundant and dual-route services located on US military-controlled installations in order to enhance survivability and the security of the infrastructure in times of crisis or hostility. Whether this additional level of expense and precaution will prove to be worthwhile can only be tested in an actual crisis; but from a preparedness perspective, their level of ambition reflects a more risk-averse approach than Canada's. It could be argued that they are just as much at risk as we are since they do not own every metre of fibre optic cable or every central office, satellite, cellular tower and Internet service provider that supplies services to their bases. The point being that the dual-use of ICT services makes the distinction and separation between government and private infrastructure practically impossible. The implication of this is the need to develop with industry a strategy that can meet the peak and extreme demands of the military. This in turn benefits all ICT users and clients given the overall increased level of service and protection that is built-into the design of ICT solutions, since the main network infrastructure pieces are common to all ICT customers. The challenge for the government is to have enough insight into proprietary solutions to know their true level of exposure to risk at the physical, semantic and syntactic layers.

---

[91] Intelfusion. "British Intelligence Warns British Telecom about its Huawei Equipment." http://intelfusion.net/wordpress/?p=558; Internet; accessed 1 April 2009.
"Intelligence chiefs have warned that China may have gained the capability to shut down Britain by crippling its telecoms and utilities."

[92] GlobalSecurity. "Global Information Grid (GIG) Bandwidth Expansion (GIG-BE)". http://www.globalsecurity.org/space/systems/gig-be.htm; Internet; accessed 16 April 2009.

Classification

Another reality regarding threats is the classified and undisclosed nature of threat and vulnerability information that prevents a better understanding among a larger audience. Select individuals, specialists, government officials and senior managers are aware and entrusted with the details of breaches, attacks, vulnerabilities and other Cyber-related problems; however, these are rarely disclosed for public consumption. The reasons are easy to appreciate, they range from national security concerns to business survival and profit. Nevertheless, this reality creates a dilemma for Cyber security practitioners, i.e., how to convince senior management and governments to spend resources on Cyber security when incidents are rarely exposed. There may be little to redress this situation and certainly, for governments and their departments, secrecy surrounding threat levels and our vulnerability to these threats will likely remain classified or on a need-to-know basis, but with the right reporting mechanisms, the decision makers can be briefed accordingly. In Canada, these reporting mechanisms and divisions of responsibility are just beginning to be explored. This paper will not delve into classified matters; however, some sensitive topics will be discussed whenever evidence is available from open sources.

Military Mandates and Missions

The nature of the National Defence role, particularly for a middle power nation such as Canada, entails that our military forces are highly connected and interdependent with its alliance partners. The CF benefits from strong relationships ranging from bi-national MOUs and treaties such as for NORAD to treaties such as with the UN and multinational alliances of

various types including ABCA[93] and NATO. This highlights the wide-ranging networks, both physical and social, which connect us around the world. By extension, much like the principle of the weakest link in a chain, this network of nations carries the information sharing advantages and the disadvantage of increased exposure to risk from multiple sources. Any one partner in the chain that lowers its level of protection or is somehow compromised, places all those connected to them to greater risk of exploitation or disruption.

The ICT infrastructure is so critical to the global reach and success of modern military missions that its Confidentiality, Integrity and Availability (CIA) is paramount. Hence, to ensure non-repudiation, protect confidentiality and avoid unauthorized access or disruption, military satellite projects design government-grade (Type 1) encryption for the up-links and down-links (syntactic links) as well as the data links (semantic links). However, the same is not necessarily true of commercial systems, where the level of encryption may not be to the same calibre. Since the CF relies upon commercial communications satellites to support its global operations, there is an additional layer of protection that must be applied. We normally address this by engineering the data links with our own Type 1 end-to-end encryption to protect our links from a semantic & syntactic perspective. There is still a residual syntactic risk that commercial satellite up-links become victims of Cyber attacks, in which case the denial of these satellites could be problematic.

As introduced in the public infrastructure section, DND's decision to outsource the delivery and management of is Global ICT requirements in the TSRP and GDNS projects had some technical risk attached. Another risk was of exposing our entire communications and

---

[93] http://www.abca-armies.org/History/Default.aspx; Internet; accessed 21 April 2009. **ABCA** stands for American, British, Canadian and Australian. Since 1965, New Zealand has also been part of this program.

security requirements to any firm wishing to bid on the contract. This was controlled through various measures to protect sensitive location data and other information from the general public by controlling the distribution and classifying certain annexes in the statement of work. A higher level of security-screening of employees and companies that bid on the contracts was also implemented to manage the risk. Business entities therefore have a duty to protect sensitive and classified information they store on their premises.

Businesses

Exploitation of customer databases and pilfering of sensitive and proprietary corporate information by both insider and external actors can spell the end to even the most reputable companies overnight.[94] The volatility of the stock exchange is another direct risk vector which is highly dependent upon the Internet to function. The protection of private sector activities rests with the private sector, but the survivability and continuity of markets quickly become the government's concern if the problem is large enough. Hence, there needs to be a strong relationship between government and industry to collaborate and ensure the highest level of Cyber protection. The key stakeholders in threat mitigation and management are the telecommunications service providers that own and operate national carrier networks as well as the Internet Service Providers (ISPs). Their ability to detect trends and collect information positions them as unique proactive security agents.[95]

---

[94]http://www.eimagazine.com/xq/asp/sid.0/articleid.5CE830BB-4E47-4488-A245-90A8E4140C69/qx/display.htm; Internet; accessed 16 April 2009.

[95]Bell Canada. Carrier Grade Threat and Vulnerability Intelligence, December 2008, 1.

Software industry and information security companies are also key stakeholders to the management and mitigation of vulnerabilities. Ensuring that software and firmware code is written with security in mind throughout the design is essential to foil attempts to corrupt or hijack software applications. Bill Gates recognized that consumer trust in Microsoft products was their centre of gravity. He invested in the training of all Microsoft software developers in the importance of security issues since 2002.[96] However, even software that has been developed with security in mind can still represent the Achilles heal of any corporate network.[97] The interaction of disparate applications using different security settings makes the management of different system configurations a major endeavour to secure. Graduate level collaboration between RMC and Queen's university has developed promising automation techniques to improve the testing of software. These initial successes have helped identify and pave the way for additional research in the testing of Windows file sharing protocol and VoIP protocols.[98] This academic initiative would benefit from private industry support to market these solutions.

Hardware is just as susceptible to exploitation as software and the US Cyber Security Policy takes aim at preventing hardware from tampering by foreign or hostile entities.[99] The

---

[96]Bill Gates. "Gates memo: 'We can and must do better'", *cnet news*. http://news.cnet.com/Gates-memo-We-can-and-must-do-better/2009-1001_3-817210.html?tag=mncol;txt; Internet; accessed 2 March 2009.

[97]Microsoft. "Written Direct Testimony of Jim Allchin.", 3 May 2002. http://www.microsoft.com/presspass/legal/allchin.mspx; Internet; accessed 8 April 2009. "We recently instituted a new program to increase the security of our Windows operating systems and are devoting substantial development resources to the task. We see this as a necessity because customers are demanding greater security in our software products to protect their data, their computing networks and their intellectual property."

[98]S. Marquis., T. Dean, and S. Knight, "SCL: A Language for Security Testing of Network Applications", CASCON '05 (IBM Centers for Advanced Studies Conference), Toronto, Oct 2005. http://tarpit.rmc.ca/knight/papers/SCL.pdf; Internet; accessed 20 January 2009.

[99]Symantec Internet Security Threat Report Trends for July–December 07, Volume XIII, Published April 2008, 30. While the risks associated with Internet-connected devices are well documented, the risks of malicious

counterfeiting of CISCO routers that were installed on US military networks has underscored the feasibility of this method of penetrating or exploiting military networks.[100] This has also shaped how the US government procures hardware and how they certify equipment for use on their networks. Other incidents involving backdoors imbedded in integrated circuitry for critical DoD weapon systems have prompted the Defense Advanced Research Projects Agency (DARPA) to launch an initiative called the Trust in Integrated Circuits program.[101] Canada has established a Cyber Protection Supply Arrangement (CPSA) through Public Works Government Services Canada (PWGSC), which is aimed only at obtaining specialized Cyber professional services for GC departments; it does not address any IT hardware protection issues.[102] This CPSA process essentially pre-screens or qualifies service providers against pre-established standards and provides all departments a level of quality from the suppliers. A CPSA could also be established to certify hardware suppliers and their products, as the US has implemented.

---

code being introduced during the manufacturing process of these devices are not. Symantec is concerned that attackers could introduce malicious code at one or more points during their manufacture and distribution. Media players, cellular phones, and other digital devices with storage mediums may have various components created by different manufacturers before final assembly and shipping. The longer the manufacturing supply chain during this process, the greater the opportunity for malicious code to be embedded in the devices directly. In some instances, the transfer of malicious code to storage media could accidentally occur from an infected PC at a manufacturing facility. It is also possible that attackers could deliberately target machines at a manufacturing facility to enhance the chances that, once final assembly and delivery is completed, their malicious code will be delivered to the end user out-of-thebox. A recent example is a number of digital picture frames that were found to contain an older Trojan program and distributed by a major U.S.-based retailer. In another case, some units of a media player manufactured in China and imported by a Dutch company were found to have the Fujacks worm.

[100]Slashdot, "FBI Concerned About Implications of Counterfeit Cisco Gear". http://hardware.slashdot.org/article.pl?sid=08/04/22/1317212; Internet; accessed 2 March 2009.

[101]Sally Adee, "The Hunt For The Kill Switch", Spectrum IEEE, Vol. 45, Isssue 5, May 2008. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4505310; Internet; accessed 8 April 2009.

[102]PWGSC. "Cyber Protection Supply Arrangement", http://www.tpsgc-pwgsc.gc.ca/app-acq/amac-cpsa/index-eng.html; Internet; accessed 12 March 2009.

Individuals

The Cyber events in Estonia in 2007 revealed that the attacks were facilitated by thousands of infected home computers without the knowledge of their owners.[103] A lesson learned in the prevention of these types of DDoS attacks requires the vigilance and cooperation of individuals around the world to keep their systems updated with the latest firewalls, AV and security updates. Preventing unauthorized access and use of home computers by Botnet infections can be an essential Internet security prerequisite.

Conversely, there are projects that have attempted to make use of excess computing capacity for the good of not-for-profit scientific research, such as World Community Grid (WCG).[104] Individuals can donate excess computing capacity by becoming part of a Grid Computing network. The user's personal computer and Internet connection are linked to millions of other computers in a way that generates massive computing power. This computing power is made available to research projects that could not otherwise acquire this amount of computing resources. By joining this Grid, a home computer's unused computing capacity effectively comes under the control of the equivalent of a botnet that distributes computing tasks into small tasks to millions of computers. The user is unaware of what processes or information traverses the home computer. The difference with such an endeavour and malicious botnets is that this organisation has the permission of the system owners who "donate" their excess computing capacity. Given the beneficial use of Grid Computing, and its

[103]NATO Parliamentary Assembly. Sub-Committee on Future Security and Defence Capabilities, NATO and Cyber Defence (Draft Report). 12 March 2009, 1. http://www.nato-pa.int/default.Asp?SHORTCUT=1782; Internet; accessed 8 April 2009.

[104]World Community Grid, http://www.worldcommunitygrid.org/ ; Internet; accessed 2 March 2009.

similarity in concept of operation as maliciaous botnets, any steps taken to mitigate or prevent the malicious botnet problem shall account for, and protect from disruption, initiatives such as the WCG.

Cyber Environment Summary

The Cyber Environment, by its very nature, represents a unique and specialized environment or domain that stands separate from the Air, Land and Maritime environments. If the Space environment is any indication, it benefits of a 50+ year history and it is just now being considered by CFD as a separate environment. The Cyber environment, with its short 20 years of history has one major difference with Space, it is accessible to any individual for only a few hundred dollars or even for free at a local library. In Canada, we are just in the process of developing the concepts and terminology that focus attention to the Cyber Environment and its relative infancy comparatively to other environments makes its recognition and application into doctrine an ongoing challenge. The definition of CNO, refers to two or more of the three sub-disciplines: CND, CNE and CNA. In terms of military operations, the shield function (CND) and the sense function (CNE) are always prerequisites to any act function (CNA), all three are symbiotic and reinforcing capabilities. Publishing a Canadian set of definitions and concepts surrounding CNO is essential to the advancement of CNO in Canada. The evolving trends in threats and vulnerabilities indicate continued growth and economic focus, with increased exploitation of social networking sites and increased outsourcing of malicious programmers. Additionally, the protection of public and private infrastructure continues to be of concern with the increased complexity due to the greater level of interconnectivity between the Internet and internal control networks. The CF relies heavily upon commercial ICT

infrastructure, which it must secure from Cyber threats. Businesses are being targeted for their customer information, hardware suppliers have not been able to provide the necessary levels of protection from tampering, and software companies still sell products filled with vulnerabilities. Therefore, the requirement to develop usable Cyber policy and capability to protect our military and national interests is increasingly urgent.

CHAPTER III - DETERMINING WHO HAS RESPONSIBILITY FOR CNO

In Canada, the issue of responsibility for IT security has been developing since 2002. The Government Security Policy published on February 1st, 2002 underscored the growing reliance upon IT to provide government services and recognized the rapidly evolving threats. It specifically identified potential threats to the "confidentiality, integrity, availability, intended use and value" of government information systems and identified that an Information Technology Security (ITS) strategy was required.[105] Four pillars were raised in this policy statement that covered prevention, detection, response and recovery. The strategy was quite vague and basic, offering little specifics other than imposing IT system accreditation processes and Business Continuity Plan (BCP) development. The immaturity of the document is further revealed by this example of imprecise language regarding the detection pillar (reproduced in its entirety below):

> Since services may rapidly degrade due to computer incidents, ranging from a simple slowdown to a complete halt, departments must continuously monitor the operations of their systems to detect anomalies in service delivery levels.[106]

To suggest that network users can perceive threats by noticing system slowdowns is at best a weak strategy. The most useful aspect of this Government Security Policy was the detailed appendix listing the responsibilities by Federal Government department. The Treasury Board Secretariat (TBS) was identified as the central agency for security and service delivery issues and ten lead departments were assigned government-wide responsibilities. Originally, the Royal Canadian Mounted Police (RCMP) was assigned the role of developing the ITS standards and technical documentation as it relates to malicious software whereas the

---

[105]Public Safety Canada. *Government Security Policy*. 1 February 2002. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12322&section=HTML; Internet; accessed 12 March 2009.

[106]*Ibid*, para 10.12.2.

Communications Security Establishment (CSE) was identified as the cryptology and ITS technical authority relating to networks and hardware accreditations. The Canadian Security Intelligence Service (CSIS) was assigned the role of investigating and analysing cyber threats to national security. The Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP), now renamed Public Safety Canada (PSC), was responsible for the protection of critical networks, information systems and other critical assets of the Government of Canada (GC). Finally, DND was strictly responsible to provide advice to departments on military intelligence for threat and risk assessment purposes.

Integrated Security Strategy

This level of fragmentation of the roles was in keeping with the various departmental mandates, as assigned by the various Acts of Parliament such as the CSIS Act and the National Defence Act; however, it in no way offered an integrated means of combating cyber threats. This policy was superseded by the April 2004 policy statement, *Securing an Open Society: Canada's National Security Policy.*[107] which adopted an integrated approach to security issues across all government departments. It created the Integrated Threat Assessment Centre (ITAC)[108] on October 15th, 2004 and saw investments in the order of $690 million toward several initiatives, including a Government Operations Centre (GOC) that would support all departments and oversee all forms of national emergencies on a 24/7 basis.[109] Specific

---

[107]Canada. Privy Council Office. *Securing an Open Society: Canada's National Security Policy*. April 2004. http://www.pco-bcp.gc.ca/docs/information/Publications/natsec-secnat/natsec-secnat-eng.pdf; Internet; accessed 11 March 2009.

[108]Canada. CSIS. "The Integrated Threat Assessment Centre (ITAC)." http://www.csis.gc.ca/nwsrm/bckgrndrs/bckgrndr13-eng.pdf ; Internet; accessed 12 March 2009.

[109]AFCEA OCIPEP report. http://afceaottawa.ca/uploads/JunReport2003.pdf; Internet; accessed 12 March 2009. The main operational functions of the Cyber Protection Division (CPD) are incident handling,

guidance was introduced to increase the capacity of the Government to predict and prevent Cyber-security attacks against its networks and the development of a National Cyber-security Strategy. Additionally, on the international scene, the CF was tasked with the requirement to be flexible, responsive and combat-capable for a whole range of operations and able to work with our allies. Although there was no specific assignment of Cyber-security roles for the CF, the Canadian Forces Network Operations Centre (CFNOC) was already operating 24/7 since 2002.[110] The fact that CFNOC enjoyed multiple international relationships in the realm of Cyber-security uniquely positioned the CF to play a key role for the entire Government.[111] In Figure 1 below, the notion of overlapping personal, national and international security sectors was introduced. Unfortunately, Cyber-security is shown only to intersect National Security and International Security sectors, when in fact Cyber-security intersects all three sectors, including Personal Security. The resultant deduction remains that the security policy highlights the requirement for some unique Cyber capabilities that have national and

---

vulnerability assessment, special projects, cyber practices, and the OCIPEP Information Protection Centre (IPC). It operates in four constituent areas: the internal IPC, the GoC Cyber Incident Response Centre (CIRCC), the national provincial/territorial governments and critical infrastructure sector owners and operators, and internationally with other governments, their national cyber security response teams and other watch & warning networks.

[110]AFCEA. http://www.afceaottawa.ca/uploads/CNO%20Briefing%2011Jan05.ppt; Internet; accessed 7 April 2009.

[111]Bill C-7: The Public Safety Act, 2004, c.15 http://laws.justice.gc.ca/en/ShowFullDoc/cs/N-5///en (Accessed 12 Mar 09). Clause 78 of this bill, which received royal assent on 6 May 2004, aimed in part at modifying the National Defence Act by creating a new Part v.2 of the NDA dealing with interceptions of communications involving the Department of National Defence (DND) or Canadian Forces computer systems. This new provision ensures that DND and the Canadian Forces have the authority to protect their computer systems networks and the information they contain from attack or manipulation. The vulnerability of computer systems to interference and outright attacks has been a growing concern in recent years, especially within military forces, which are increasingly dependent on information technology for success on the battlefield and for carrying out other operations. Although various measures have been taken to protect the computer systems used by the department and the Forces from intrusions from outside sources, protection is also needed against actions from within the department or Forces that can accidentally or deliberately damage the systems. The new section 273.8 allows the Minister of National Defence to authorize in writing public servants in the department or persons acting on behalf of the department or the Forces who operate, maintain or protect computers and networks to intercept private communications. Sections 273.7(1) and (2) in Bill C-42 described the private communications as "originating from, directed to or transiting through any" computer system or network. Sections 273.8(1) and (2) in Bill C-55 and now Bill C-7 go into greater detail, since they state that these communications are "in relation to an activity or class of activities specified in the authorization, if such communications originate from, are directed to or transit through" any computer system or network.

international reach. When the CF created the CFNOC capability in 2002, it was in fact ahead of its time in responding to the 2004 Government policy.

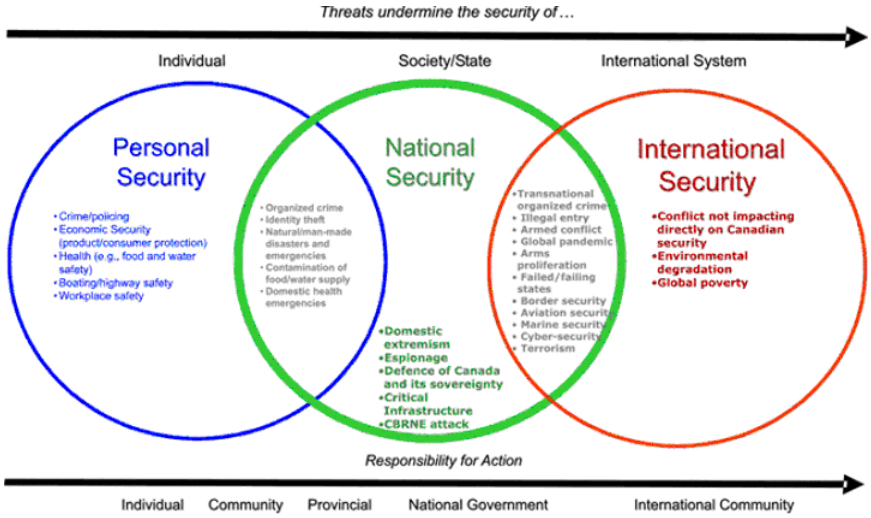

Figure 1 - Overlapping Security Sectors.[112]

Within one year of this new security policy, the Office of the Auditor General conducted a Government-wide audit that was released in February 2005.[113] Although the audit reported an improvement in the co-operation between departments, it also noted that ITS standards still remained to be developed. The only document that had been produced since 2002 was the Management of Information Technology Security (MITS) standard, published in May 2004 and it referred to other standards that were not published until 2006.[114] The lack of interest in ITS is best illustrated by the results of the 2004 TBS survey to 90 departments, in

---

[112]Canada. Government of Canada, Securing an Open Society 2004: Canada's National Security Policy, April 2004, 4. http://www.pco-bcp.gc.ca/docs/information/Publications/natsec-secnat/natsec-secnat-eng.pdf; Internet; accessed 11 March 2009.

[113]Office of the Auditor General Audit, February 1, 2005. http://www.oag-bvg.gc.ca/internet/English/parl_oag_200502_01_e_14921.html; Internet; accessed 16 March 2009.

[114]*Ibid.*, 7. The MITS standard offered guidance on maintaining secure IT systems in the following areas: management controls, risk assessments, dealing with security incidents and weaknesses in systems, auditing security, and business continuity planning. Still missing were Intrusion Detection, Incident Management, Security Training and Awareness, Security in Contracting, Identification and Categorization of Assets, Threat and Risk Assessment, Investigations and Sanctions. Secuirty Screening, Departmental Security Programs, Protection of Employees, Security Outside Canada, and Sharing of Information.

which only 46 responded and of those, only one met the baseline requirements of the security policy. Staff interviews with some departments revealed that a lack of money, people and interest in senior management regarding ITS issues as the reasons behind this inaction. Clearly, the audit provided ample proof that although some basic policy existed, there was no real action behind it, and Canada did not have an integrated ITS posture in 2005. Much more work still remained ahead to address the issues and commitments set out in the 2004 *Securing an Open Society* policy.

The focus of the 2004 policy placed more importance to the Public Safety department and introduced the position of the National Security Advisor. The policy was designed to respond to Canada's core national interests, which have largely remained the same in all Defence White papers since 1964[115]:

1. Protecting Canada and the safety and security of Canadians at home and abroad;
2. Ensuring that Canada is not a base for threats to allies; and
3. Contributing to international security.[116]

This policy document was strongly influenced by the incidents of 9/11 and placed a larger focus on intelligence and information sharing at the international level, making a link that Canadians could best be protected if we looked beyond our borders. Unfortunately, in the realm of Cyber-security, the policy was strictly concerned with Critical National Infrastructure (CNI) protection and failed to address other areas of interest such as business continuity and threat vectors such as espionage, identity theft, intellectual property theft, criminality, terrorism and national security. Although it planned to include both public and private representation in

---

[115]National Defence Policy Archives http://www.forces.gc.ca/admpol/newsite/defence%20policy%20archives.html; Internet; accessed 16 April 2009.

[116]Privy Council Office. *Securing an Open Society: Canada's National Security Policy*. April 2004. http://www.pco-bcp.gc.ca/docs/information/Publications/natsec-secnat/natsec-secnat-eng.pdf, 5; Internet; accessed 11 March 2009.

its national task force to develop a National Cyber-security Strategy, it failed to include private individuals and international representation such as the US, NATO and other security and trading partners; hence it had a very introspective, government-only focus. Although the aim was to reduce Canada's vulnerability to cyber-attacks and cyber-accidents, by limiting its scope to CNI, it was by design an incomplete policy that excluded important parties that could have contributed.

Notably, the CF had already created a national-level organization with the mandate to defend against, monitor and respond to cyber incidents. Although CFNOC's mandate is primarily to defend DND networks, it is also capable of assisting other government departments in the evaluation of their network security. But most of all, CFNOC's reach extends beyond Canadian borders through its work within the 5-eyes community[117] and bilateral arrangements with the US at large through MOUs such as the Combined Defense Information Systems Management in Support of Defense of North America MOU with the Defense Information Systems Agency (DISA).[118] The CF has numerous NATO contacts and involvement with over 28 nations in the development of ITS standards and policies. Much trust-building and collaborative work has been accomplished toward resolving information sharing and network interoperability issues; however, the CF's role in Canada's Cyber-security plans seem to have been marginalized in 2004. In fact, of the four thrusts of the Integrated Security System introduced by the 2004 security policy, the CF's role was limited strictly to two areas: threat assessments, i.e. intelligence; and consequence management as an assisting

---

[117]Another name for the ABCA community, which includes the following nations: AUS/CAN/NZ/UK/US.

[118]Memorandum of Understanding between the Department of National Defence of Canada and the Department of Defense of the United States of America Concerning Combined Defense Information Systems Management in Support of Defense of North America (CANUS CDISM MOU), 6 March 2008. http://www.state.gov/documents/organization/111449.pdf; Internet; acessed 29 March 2009.

force to first responders in response to terrorist attacks or natural disasters. As the only department with any dedicated capability to conduct Cyber Operations, the CF was still regarded only as extra manpower to be called upon in certain limited emergency situations. Granted that CSEC falls administratively under the Minister of National Defence (MND), and has extensive ITS capability, it was only highlighted in the 2004 Policy as receiving additional funding strictly related to its role in the intelligence domain.

The Cyber-security posture in Canada continued to be wanting for direction for several years, as there is little evidence of progress since the 2005 OAG audit report. Beyond the apathy of most departments for ITS, there were some efforts at the individual level to cooperate between departments, however, the overall government-wide orchestration in a deliberate manner has been lacking. The main accomplishments resulting from the 2004 Policy are the creation of the GOC which serves as the focal point for all emergencies nation-wide.[119] Nevertheless, its role is entirely reactive and spans so many areas of interest related to public safety at large, that it is not specialized in the realm of Cyber-security. Within the GOC resides the Canadian Cyber Incident Response Centre (CCIRC) which is responsible for monitoring threats and coordinating the national response to any cyber security incident. It is primarily concerned with the protection of CNI against cyber incidents.[120] In essence, the service it offers is more informational, their publications are little more than links to anti-virus and software vendor patches. They have a limited scope and although they are prepared to coordinate with the major departments in times of emergencies, in the normal times, there is

---

[119]Public Safety Canada. http://www.publicsafety.gc.ca/prg/em/goc/index-eng.aspx; Internet; accessed 17 March 2009.

[120]Public Safety Canada. http://www.publicsafety.gc.ca/prg/em/ccirc/abo-eng.aspx; Internet; accessed 17 March 2009.

only a superficial relationship between the GOC and the Operations Centres of other departments. This should change now that the CG has published a new IT Incident Management Plan (GCIT IMP).[121]

Also connected to the CCIRC is the Cyber Triage Unit (CTU) which is composed of officials from PSC (the lead department), RCMP, CSIS, TBS CIO Branch, CF and CSEC. The CTU's main function is to analyze the nature of an incident and identify the primary department and supporting departments for the incident.[122] Although this multi-departmental effort appears to be integrating, it actually is only cooperative, in that its only output is to identify a lead department for a particular incident. Although these organizations represent a good start, they are limited in their ability to be effective by the lack of national situational awareness since they are unable to view and monitor the GC's entire inventory of networks and must rely on reports and inputs from Other Government Departments (OGDs). The GOC is only working within existing bureaucratic silos between departments rather than implementing the necessary information sharing and monitoring structures necessary to address the true Cyber-security challenges faced by the GC.

GC Cyber Security Initiatives since 2004

The promise of a National Cyber Security Strategy still remains illusive as reported by the Ottawa Citizen: "Canada still has no strategy to protect critical national infrastructure from

---

[121]Government of Canada. Information Technology Incident Management Plan (GC IT IMP), November 2008.

[122]*Ibid.*

terrorists, natural disasters and other calamities".[123] On May 6th, 2008, Public Safety Canada's Cyber Security Strategy Initiative office released a draft document titled *Working Towards a National Strategy and Action Plan for Critical Infrastructure*. Again, the focus is on the ten critical infrastructure sectors, not the Cyber component *per se*. The timelines for this effort includes a two year timeframe to develop information sharing structures and portals between the various Federal, Provincial and Territorial owners and operators of critical infrastructures. Another document, the GC IT Incident Management Plan (IMP) was released by TBS in November, 2008. The purpose of this document is to comply with the 2002 Government Security Policy in outlining the approach to effectively and efficiently manage IT incidents that impact or may impact the GC.[124] At the core of this plan is a series of reporting channels to seven different layers and committees with the Chief Information Officer Council providing the overall governance and guidance. It also articulates the roles of the various entities in the event of an IT security or Cyber incident. For example, the primary role of the GC Chief Information Officer (GC CIO) is to "approve the disconnection of departmental infrastructures or systems if required to contain an incident".[125] The plan provides a basic incident management framework tailored to government operations and organizations.

That being the case, it is not necessarily efficient, nor is it guaranteed to be effective. The major omission of this plan is a proper proactive posture beyond the basic mitigation activities such as applying security patches. The IMP does however offer enough detail to be

---

[123] Ian MacLeod, "State of emergency: Canada lacks plan to protect critical infrastructure", *Ottawa Citizen*, April 11th, 2008. http://www2.canada.com/ottawacitizen/news/story.html?id=8b1489a0-2dc5-4a79-900f-154e5d51bc33&k=97522; Internet; accessed 17 March 2009.

[124] Canada. Treasury Board Secretariat. *GC IT Incident Management Plan*, draft version 1.6 dated 22 May 2008.

[125] *Ibid.*, 9.

implemented and does a good job of capturing most governance and functional duties in a clear and concise format. It also attempts to provide an integrated approach to handle cross-cutting cyber incidents.

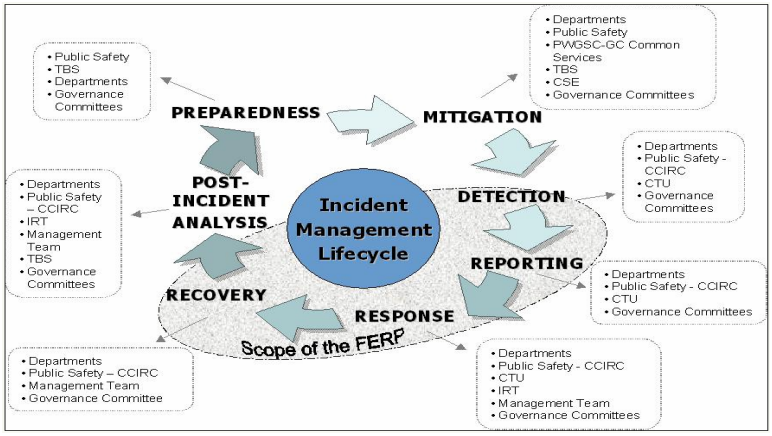

Figure 2 - Cyber Incident Management Plan

Proactive Defence Proposal

Last among the initiatives related to the review of the Government Security Policy is the Proactive Defence Proposal, an evolution of the unpublished ITS Strategy. On June 6th, 2008 the Chief Information Officer for the GC, Ken Cochrane, presented a briefing on a proposal for Proactive Defence. It defined Proactive Defence mainly as a means to assess the Cyber environment and the risks in order to enable the government to take action before issues can affect business IT. He describes the current state of a federated[126] situational awareness as fragmented, of insufficient capacity, with no authority to share information and a focus on post-incident response for recovery from an incident. The target vision aims at consolidating the situational awareness picture into a single GC focal point, with the necessary authorities to share information in view of being proactive.[127] The proposed approach is to develop a

[126]Federate: to organize from a central point, uniting several independently governed entities (such as a federal government system).

roadmap for GC-wide Proactive Defence that covers governance, tools, people and services. The intent is to leverage much of the previous work in policy, the IMP, BCP, and Shared Services.[128] Some of the key activities to be tackled in this effort include the creation of a GC critical systems catalogue, implementing automated tools to build national situational awareness of government IT systems and services, and addressing the legal and policy changes necessary to enable the effect information sharing across departments. Interestingly, CFNOC was highlighted as the only example of a mature and promising federated model to meet these requirements in Canada. In the short term, some high impact initiatives will be pursued which include the reduction of the number of Internet access points, an activity to reduce the number of vulnerabilities by reducing the number of ingress and egress channels to government networks over the Internet, similar to the US Trusted Internet Connections (TIC) Initiative.[129] The GC IT IMP publication was promised and actually published in November 2008, establishing some structures for the governance, reporting and assigning of responsibilities for Cyber incident management. Finally, the third "quick hit" initiative will concentrate on delivering improved threat and vulnerability assessments. The next step in 2009 was to develop a Memorandum for Cabinet in collaboration with PSC and other lead departments to

---

[127]Canada. Treasury Board Secretariat. Proactive Defence presentation by Ken Cochrane given on June 6th, 2008.

[128]Canada. Parliament of Canada. Shared Services: Lower Costs, Improved Services and a Change in Culture. 23 September 2005. http://www.parl.gc.ca/information/library/PRBpubs/prb0532-e.htm; Internet; accessed 17 Marc 2009. Shared Services Organizations (SSO) for Corporate Administration (CA-SSO) and Information Technology (IT-SSO) were created to improve efficiencies and reduce costs of operating government services. IT_SSO would provide shared services in terms of network, office and data centres to all departments and agencies, including CA-SSO, based on shared procedures and standards. In the short term, IT-SSO would apparently form part of Public Works and Government Services Canada.

[129]http://georgewbush-whitehouse.archives.gov/omb/pubpress/2008/071008_tic.html Released July 10th, 2008. Internet; accessed 17 March 2009. "AGENCIES REDUCE SECURITY VULNERABILITIES UNDER THE TRUSTED INTERNET CONNECTION INITIATIVE. Washington, DC — Today, the Office of Management and Budget (OMB) released the *Trusted Internet Connections (TIC) Initiative Statement of Capability Evaluation Report* highlighting the Federal government's rapid progress toward strengthening IT security. This was achieved by reducing external connections, including Internet points of presence from over 4,300 reported in January 2008, to a target of less than one hundred."

move forward the message for the need to recognize cyberspace's urgency and importance to national security.

In summary, some progress is visible on both governance and policy fronts that promise to produce some results, but on balance, some fundamental issues need addressing before any of this work can actually concretize into a responsive, effective and efficient capability. Firstly, as demonstrated in the lull of progress in the Cyber-security realm from 2002 to 2008, the guidance from TBS must be published or announced by the GC and the associated funding must be allocated in parallel across multiple levels of government.[130] The implementation then becomes a bottom-up activity that requires the creation of positions, along with standardized training and education programs to increase the number of personnel across all departments that will execute the Cyber-security policy. Until such time as these specialized resources are in place, there is little hope of a better grade from the next OAG report. As the need and urgency for securing cyberspace becomes more pressing, the CF may be in a position to offer some quick successes for the GC strategy.

The Meaning of Proactive

Another fundamental aspect related to training is having a common lexicon and shared understanding of the objectives; this begins with clarification of terms. The term proactive used in the Proactive Defence Policy Proposal should be clarified to avoid gaps in semantic understanding of the end state. The Concise Oxford English Dictionary defines proactive as

---

[130]Canada. Report of the Standing Senate Committee on National Security and Defence, Vol. 1, Second Session, Thirty-ninth Parliament 2008, Appendix A, 179. This report lists the types of emergency programs funded by the provinces and $0 are allocated to building acyber-attack specific response capability.

"creating or controlling a situation rather than just responding to it." [131] If the policy document is to use proactive in its title, the implication goes beyond simply mitigating and defending GC IT infrastructure in a passive mode.

In a security whitepaper produced by Bell Canada, Proactive Cyber Defence is defined as follows:

> acting in anticipation to oppose an attack against computers and networks. It represents the thermocline between purely offensive and defensive action; interdicting and disrupting an attack or a threat's preparation to attack, either pre-emptively or in self-defence.[132]

The reference to the thermocline can be represented by the diagram in Figure 3 below which depicts the thin and varying boundaries separating Computer Network Defence (CND) from Computer Network Exploitation (CNE) and Computer Network Attack (CNA). To place CND, CNE and CNA into context it is useful to explore the linkages and interdependencies between these CNO activities.

---

[131]Online Concise Oxford English Dictionary http://www.askoxford.com/concise_oed/proactive?view=uk; Internet; accessed 18 March 2009.

[132]Bell Canada. Security, Intelligence, Law Enforcement, Public Safety and National Defence Research: Bell Canada Security Story, no pagination.

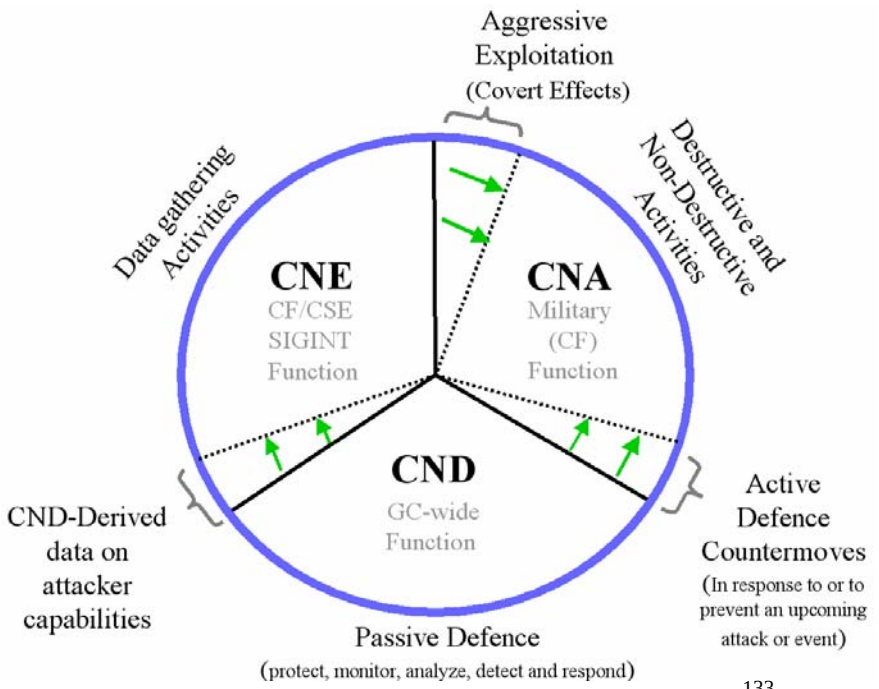

Figure 3 - Computer Network Operations (CNO) Model[133]

Figure 3 illustrates the active defence activities as overlapping the CNA space. Likewise, probing for information about an attacker's capabilities can fall into the CNE category. Finally, aggressive exploitation in a covert manner could be construed as CNA activities.

As delineated in the GSP, currently the task of CND is the responsibility of all federal government departments. CND functions are largely passive in nature; however, to adequately defend against computer network attacks requires more than simply hiding behind a firewall and loading the latest anti-virus updates onto individual computers. CND activities include a host of monitoring and control functions that are enacted by strong and enforceable security policies "to protect, monitor, detect, analyze, and respond to unauthorized activity within

[133]Chart modified from a CFNOC briefing to Information Systems Security Officers Course, Fall 2007, 6.

computers or computer networks." [134] The basic CND functions include system certification and accreditation (C&A), configuration management, IT Infrastructure situational awareness, problem management, incident management, release management, security operations, network defence, open source intelligence, vulnerability analysis and forensic analysis which are all accomplished by CFNOC in support of CND.[135] The note in the draft definition provided by J6 CNO also highlights the notion that CND may constitute CNE or CNA, when intrusive contact with another party's computer or network is affected without their knowledge or consent.

CNE activities are generally covert Signals Intelligence (SIGINT) data gathering activities.[136] CNE, in military terms, represents the intelligence information gathering method for the understanding of adversary's capabilities as well as intents and would be an essential part of any plan to conduct CNA. Due to the aggressive and covert nature of CNE, these activities could be perceived as CNA in nature in the event they were discovered.

CNA activities are offensive by nature; they are aimed at causing destructive damage to information or information systems. As defined by J6 CNO, CNA is:

---

[134]Draft CNO Policy, 22 Apr 08 version. Attached to the CND definition is the following Note: Any and all computer network activity, including a CND activity, that initiates intrusive contact (transcending the level of contact available on a public access basis) with other computers or computer networks, without the permission of the owner / operator of those computers or computer networks, constitutes CNE or CNA, depending upon the form of the contact, and falls under the governance framework of the corresponding activity.

[135]*Ibid.*,15.

[136]Government of Canada. *Statutes of Canada Bill C-36*, (2001): , http://www.parl.gc.ca/37/1/parlbus/chambus/house/bills/government/C-36/C-36_3/C-36TOCE.html; Internet; accessed 10 February 2009. This amendment to the NDA by adding section 273.6 dealing with intercepting private communications under Ministerial Authorization. The CF's role is included at section 263.65 (6) "The Minister of National Defence may issue directions for the Canadian Forces to support the [Communications Security] Establishment in carrying out activities authorized under this section.

> a directed activity conducted through the use of computer networks to intentionally disrupt, deny, degrade, or destroy adversary computers, computer networks, and / or the information resident on them.[137]

Although the formal legal opinions are still being formulated on CNA, there is a possibility that CNA may be regarded as "use of force" with a potential to cause harm;[138] if this is the case, then CNA activities fall within the realm of the National Defence Act (NDA). This would imply that from a legal perspective, CNA activities would primarily be the responsibility of the CF, with OGDs in a supporting role. The relationship between the three CNO functions places the CF in a unique and central role because in addition to the CND role common to all departments, it is also tasked with the active defence role, which borders on being considered CNA. Inherently the CF also bears the intelligence role, which includes the CNE function.

There are also strong functional interdependencies between the three CNO functions. For example, the ability conduct CND against an aggressive adversary relies upon the ability to receive Indications and Warnings (I&W) and other intelligence from CNE activities. Likewise, CND monitoring activities may reveal unusual network activity that can help cue CNE activities toward a particular target. There is also a similar symbiosis between CND and CNA in the case where in the conduct of CND, a defender may have to counter-attack using CNA-type activities in order to protect the network proactively. CND or CNE activities may also reveal an imminent attack to which there are no defences, in which case, a proactive response would be CND in nature but may require CNA techniques. These actions would still

---

[137]Canada. Department of National Defence, Draft Computer Network Operations Policy, 22 April 2008.

[138]Michael N. Schmitt, "Computer Network Attack and the use of Force in International Law: Thoughts on a Normative Framework," *Columbia Journal of Transnational Law* 37 (1998-1999), 886.

fall under the category of CND because they would be reactive to an attack rather than a planned event, but this distinction between the two is important. CNA activities typically would require intelligence support, extensive analysis, detailed mission planning, the development of specialized software code, legal review and finally Ministerial Authorization from the Minister of National Defence (MND). The deliberate rather than reactive nature of CNA requires a higher level of resources and preparedness that exploits the knowledge gained from CND and CNE activities. Sylvain LeBlanc and Dr. Knight from RMC also articulated a strong case in favour of tracking an attacker rather than blocking or shutting down a connection.[139] The value of learning the capabilities, identity, methods and intent of the adversary may be of great value in either defending against or preventing future attacks – this approach would fall under the CNE category.

If the aim of the Proactive Defence Policy is truly to achieve a level of sophistication that will enable the GC to deal with issues before they can impact business in Canada, this involves a higher level of proactive Computer Network Operations (CNO) than we have exercised to date. This will require a clear governance framework and the necessary legal mandate for dealing with cases where CND graduates from passive to active defence, the latter being a CNA-type activity.[140] Based upon the definition of proactive which is necessary to

---

[139]Sylvain Leblanc and Scott Knight, "Engaging the Adversary as a Viable Response to Network Intrusion", Workshop on Cyber Infrastructure Emergency Preparedness Aspects, Ottawa, 21-22 April 2005; http://tarpit.rmc.ca/knight/papers/IO%20Counter-measures.doc; Internet; accessed 20 January 2009.

[140]Elliot Che. "Securing a Network Society" Carleton U-RIEAS113[1], September 2007, 17 http://se2.isn.ch/serviceengine/FileContent?serviceID=10&fileid=FAD521F5-FD15-3D9F-3CAD-71E2629C3127&lng=en,; Internet; accessed 11 March 2009. Passive defence is another name for target hardening, involving the use of technologies such as firewalls or cryptography to protect information technology assets and the data stored within. Active defence seeks to determine the identity of the attacker and possibly initiate a counter-attack.

execute effective CNO activities, a Proactive Defence Policy could only be acted upon by the CF.

Legal Issues

Much analysis into the implications of information operations using computers and the topic of CNA has pointed toward the existing Laws of Armed Conflict (LOAC)[141] and concluded that in times of war, the LOAC are still valid with little or no change.[142] [143] Mark Shulman reinforces this conclusion by advocating that the elements of the Geneva Convention Protocols such as military necessity, proportionality and discrimination still apply to computer attacks.[144] He further suggests that the term Information Operations not be defined, but rather the International Courts should retain the flexibility by building a body of case law over time. The problem of applicability regarding the LOAC is more with the construct of International Law, which rests on the concept of geographical boundaries between states.[145] In the event that a CNA against a state is initiated by or involves a non-state actor, particularly outside the context of war, then the LOAC would not necessarily apply. The interesting point about this conundrum is that it indirectly supports the imperative for states to conduct CNE operations and active defence CND operations in order to make the determination of the source of an attack as being state or non-state. The problems associated with jurisdictional boundaries

---

[141]Directorate of Law Training, ed., *B-GG-005-027/AF-022, Collection of Documents on the Law of Armed Conflict* (Ottawa: Dept. of National Defence, 2005).

[142]Mark R. Shulman, "Discrimination in the Laws of Information Warfare," *Columbia Journal of Transnational Law* 37 (1998-1999), 939.

[143]Cdr Antolin-Jenkins, Vida M., Defining the Parameters of Cyberwar Operations: Looking for Law in all the Wrong Places?, Naval Law Review, Vol 132, 2005, 168.

[144]*Ibid.*, 965.

[145]Peace Treaty concluded at Munster in Westphalia, the 24th Day of October, 1648. http://avalon.law.yale.edu/17th_century/westphal.asp; Internet; accessed 2 February, 2009.

regarding the prosecution of Cyber-crime are complex and are discussed later in this section. The second point is that not all computer attacks will happen in times of declared war, this is where International treaties such as the United Nations Charter can be of use. Again, these are restricted to the signatories that are states, however, states must conduct themselves within the bounds of these agreements to keep any legitimacy on the international stage, Canada included. Hence, as Shulman concludes, "diligent, creative and intelligent application of the these principles [military necessity, proportionality and discrimination] should see LOAC well into the twenty-first century."[146] The challenge remains for states to use established internationally accepted ground rules that were designed to regulate the use of conventional armed force and apply the spirit of these conventions to the Cyber environment. Therefore, the legitimacy of a state's response to Cyber attacks will undoubtedly rely on the UN Charter's concept of self-defence, both in a reactive and pre-emptive manner.

The UN Charter's Chapter VII Article 51 offers states some allowances to act in self-defence:

> Nothing in the present Charter shall impair the inherent right of collective and individual self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security.[147]

---

[146]Mark R. Shulman, "Discrimination in the Laws of Information Warfare," *Columbia Journal of Transnational Law* 37 (1998-1999), 966.

[147]United Nations. Charter of the United Nations. 1948. Chapter VII: Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression, Article 51. http://www.un.org/aboutun/charter/chapter7.shtml; Internet; accessed 18 March 2009. "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security."

The specific reference to an armed attack may appear problematic, since it limits the conditions under which a state could perceive being under attack. However, Chris Richter argues that pre-emptive self-defence has been in existence since the *Caroline* incident of 1837 and that the UN Charter does not supplant such customary laws.[148] Mikael Nabati on the other hand analyzes the rise of terrorism and posits that the UN Article 51 has lost its relevance on two fronts: its ineffectiveness in responding to the terrorist threat; and more poignantly, that Article 51 is no longer a "legitimate restraint on the recourse to force in international relations".[149] Specifically he addressed the reality that under international law, states have no affirmative duties[150] or responsibilities toward non-state actors within their borders to prevent them from conducting terrorism acts. The phenomenon of terrorism places increased pressure on all states to defend themselves pre-emptively from all other states in the traditional environments as well as the Cyber environment. The same legal grey zones that make CNO activities problematic for states to undertake, may in some cases, offer a valid means of retorsion[151] without resorting to armed force. The use of a non-lethal means such as CNO provides states with the ability to deal with both state and non-state Cyber-aggressors within the rules of military necessity,

---

[148]Chris Richter. "Pre-emptive Self-Defence, International Law and US Policy". *Dialogue* (2003) 1:2, 63. http://www.polsis.uq.edu.au/dialogue/vol-1-2-6.pdf; Internet; accessed 19 March 2009. "A right of self-defence that encompasses both actions done in response to an armed attack, and actions done in *anticipation* of an armed attack, are provided by customary international law after the *Caroline* incident."

[149]Mikael Nabati, "International Law at a Crossroad: Self-Defense, Global Terrorism, and Preemption (A Call to Rethink the Sefl-Defense Normative Framework)", *Transnational Law & Contemporary Problems*, Vol. 13, 2003, 775.

[150]http://www.wyolaw.org/Outlines/LaMar%20Jost%20(2002)/lamar_jost_torts_ii.PDF; Internet; accessed 18 April 2009. Generally **the law of affirmative duties** deals with circumstances under which the defendant may owe a special duty of care to the plaintiff. Usually, this will be a duty owed *in addition* to the general duty to due care the defendant owes under the "reasonable person" standard. In other words, the defendant may be liable for
nonfeasance and well as misfeasance in certain situations. (a) *misfeasance:* exists when the defendant is responsible for making the plaintiff's position worse; (b) *nonfeasance:* is found when the defendant has failed to aid the plaintiff through beneficial intervention.

[151]**Retorsion** consists of an unfriendly but legal act of force undertaken with retaliatory or coercive purpose.

proportionality, and discrimination without violating International Law. Given this possibility, the argument follows that CNO activities are even more critical to the defence of any state as a means to react without unduly escalating to armed force, regardless of whether the state is dealing with a non-state or state aggressor. Specifically, CNE and CNA activities then become essential capabilities to enable a state to act pre-emptively in the defence of their national interests.

For those that are unconvinced that pre-emption is justified, Michael Schmitt proposes a new normative framework to clarify the existing UN Charter.[152] In it he considers the case where a CNA occurs and he analyzes how a victim of CNA could interpret this act under the UN framework. He works through the questions of armed vs unarmed attack and whether using CNA in response would be permissible. He argues that, failing all else, Article 42[153] of the UN Charter may be invoked to authorise a forceful response by air, sea or land forces in the event that Article 41 provisions prove inadequate.[154] He does not consider if CNA could be one of the (forceful) means used to respond. But more importantly, the appropriateness of Article 41 is also not fully explored, wherein measures other than armed force could have a more targeted effect. The examples cited in Article 41 mention the interruption of various

---

[152]Michael N. Schmitt, "Computer Network Attack and the use of Force in International Law: Thoughts on a Normative Framework," *Columbia Journal of Transnational Law* 37 (1998-1999), 936.

[153]United Nations. "Charter of the United Nations, 1948." Chapter VII: Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression, Article 42. http://www.un.org/aboutun/charter/chapter7.shtml; Internet; accessed 18 March 2009. "Should the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security. Such action may include demonstrations, blockade, and other operations by air, sea, or land forces of Members of the United Nations.

[154]*Ibid.*, Article 41. http://www.un.org/aboutun/charter/chapter7.shtml; Internet; accessed 18 March 2009. "The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations."

means of communication, which by definition is CNA. It would therefore appear that the UN Charter already has foreseen the role of CNO before the terminology was even in existence. Arguably, as Schmitt indicates, it is unlikely that in 1948 the drafters of the UN Charter envisaged CNO activities in crafting the language of this article.[155] However, even if the provisions of Article 41 were not called CNO specifically, the intent was clearly to seek other options than armed force to change the behaviour of the offending party. Finally, Chris Richter rightly reminds us of the importance for states to justify their actions in a multinational setting, instead of acting pre-emptively in a unilateral manner.[156] In other words, there remains a responsibility on the part of states which act or react without the explicit consent of the United Nations Security Council (UNSC). In cases of self-defence, such as pre-emptive self-defence, the UN Charter provides a large degree of latitude to states when the situation does not permit a debate in the UNSC; but the actions must stand to the scrutiny of such a debate.

The notion that computer attacks represent a form of use of force remains a double-edged debate.[157] On one hand, those favouring cautious restraint in the use of CNA by states point to the broad scope and potentially indiscriminate targeting of innocent computer systems. The possibility of Botnets propagating without apparent control and inflicting physical collateral damage, injury or death is perhaps one argument for restraint regarding the use of CNA. However, recent cases such as the Estonia Botnet-based DDoS attack illustrate that attackers can program Botnets to be highly targeted and discriminate. Additionally, the rules

---

[155]Michael N. Schmitt, "Computer Network Attack and the use of Force in International Law: Thoughts on a Normative Framework," *Columbia Journal of Transnational Law* 37 (1998-1999), 912.

[156]Chris Richter. “Pre-emptive Self-Defence, International Law and US Policy”. *Dialogue* (2003) 1:2, 64. http://www.polsis.uq.edu.au/dialogue/vol-1-2-6.pdf ; Internet; accessed 19 March 2009.

[157]Cdr Vida M. Antolin-Jenkins, “Defining the Parameters of Cyberwar Operations: Looking for Law in all the Wrong Places?”, *Naval Law Review*, Vol 132, 2005, 167.

of engagement for UN Member states are codified through various Articles, and restrict them from resorting to indiscriminate attacks of any kind. Because of this, even if CNA is meant to be disruptive and destructive, when conducted by a state, the CNA actions will more likely be limited to legitimately targeted systems and the information contained in these systems. Any Cyber attacker, state or non-state, would be well advised against indiscriminate Cyber attacks for fear that their own systems, due to the interconnectivity of the Internet, would suffer if the attacks were to be launched without proper targeting. Indiscriminate attacks may also raise more attention, or additional responses, from more parties who would be affected than an attacker would want to risk. For states, the LOAC rules still apply to all military operations in terms of the "fundamental principles of military necessity, unnecessary suffering, proportionality, and distinction (discrimination), which will apply to targeting decisions".[158] Targeting is clearly an important element in the crafting of any CNA activity regardless of who perpetrates the attacks or what their motive may be.

Consequently, for any state contemplating the use of CNA, just as any targeting decision currently made in military campaigns, targeting in the Cyber environment would invariably be regulated under the same constraints.[159] Target selection must also be validated by sufficient intelligence analysis prior to being engaged.[160] Whether CNA constitutes the use of force in the traditional understanding is debatable.[161] However, as analyzed by Schmitt, if

---

[158]United States. Department of Defense. *Joint Targeting*. JP 3-60, 13 April 2007, Appendix E-1. http://www.dtic.mil/doctrine/jel/new_pubs/jp3_60.pdf; Internet; accessed 20 March 2009.

[159]Cdr Vida M. Antolin-Jenkins, "Defining the Parameters of Cyberwar Operations: Looking for Law in all the Wrong Places?", *Naval Law Review*, Vol 132, 2005, 168.

[160]*Ibid.*, Appendix D-1.

[161]In International Law, use of force is a clearly determinant for a state to react in self-defence or collective defence. Until more experience is gained through the test of future Cyber attacks, it is unknown how

your intent was not to cause physical damage to tangible objects or injury to human beings, CNA would not constitute use of force legally. Therefore, by limiting CNA activities against data or information, CNA would not be considered use of force. Secondary effects, or collateral damage, to other systems or injury to people would then also be treated in the same manner as for other targeting activities, in which a measure of proportionality[162] is determined prior to the targeting decision. Similarly, from the attacker's perspective, it is concluded by the NATO Cooperative Cyber Defence Centre of Excellence report on legal lessons learned from the Estonia Cyber attacks, that it is possible to limit the nature of the attack such as to elude the triggers for applicability of LOAC.[163] This suggests that a high degree of control of Botnets is possible. The report indicates that the attacks against Estonia (2007), Lithuania (2008) and Georgia (2008) did however have legal consequence in terms of criminal activity which underscores the importance of a cyber crime convention. The linch pin to the effectiveness of such a convention has however been tested and failed in the case of Georgia, given the reluctance of Russia to cooperate in the criminal investigation.

Similar to the Operational Law discussed above, the legal debate regarding criminal or illegal acts conducted over the Internet also must mature to a common-sense approach, as described by, Dr. John C. Klensin.[164] In his a speech to the Internet Governance Forum (IGF)

---

the international community will respond and if armed force would be used in certain cases. In both the Estonia and Georgia cases, allegations have been made that Russia condoned or facilitated the Cyber attacks, using third parties, but to date, no actions have been taken against Russia. As will be discussed later in this paper, the determination of motive or intent as well as access to intelligence resources are essential in providing states with appropriate decision-making information to react in cases of Cyber attacks.

[162]Department of National Defence. *Canadian Forces Operations*, B-GJ-005-300/FP-000, Ch 2 2005-08-15,5-3. **Proportionality**. This principle implies that collateral damage arising from military operations must not be excessive in relation to the direct and concrete military advantage anticipated from such operations

[163]NATO CCDCOE. Cyber Attacks Against Georgia: Legal Lessons Identified, Tallin, Estonia, version 1.0 dated November 2008. http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf; Internet; accessed 8 April 2009.

he articulated that unacceptable and illegal behaviours conducted over the Internet are not technological but antisocial. In other words, it is possible to use existing laws to address what are essentially societal behaviours and technology should not confuse the prosecution efforts. He concluded that:

> Each proposed action that treats an unacceptable behavior differently depending on whether it is committed on the Internet or in some other context should be examined carefully and, I believe, with some suspicion.[165]

He is of the opinion that existing laws need to be used to prosecute Internet-based behaviours that are illegal or criminal in the traditional physical environment. Rafal Rohozinski of the SecDev Group made similar comments about the question of how the Internet is perceived:

> Policy makers have seen Internet as a technical ether rather than an ether of life… We need to see the Cyberspace as an environment in which we engage. Where we engage as a state diplomatically, where we engage as Canadians individually, and where frankly our defence department also engages as a military sphere. This has not happened yet, we still think very reactively about the Internet as things that need to be defended … we don't see it holistically and I think this is where the wakeup call is.[166] [167]

This position is only partially supported by the legal community as being valid in certain cases. The Cyber environment itself is not in a separate jurisdiction, but individuals interacting via the Internet are physically in existing jurisdictions.[168] Jurisdiction comprises several elements, each which have a bearing on which court should hear the case and these non-trivial concerns

---

[164]Biography Dr. John C. Klensin. http://www.icann.org/en/biog/klensin.htm; Internet; accessed 20 March 2009.

[165] John Klensin, "Internet Governance" Address by John Klensin to the opening of the IGF http://www.isoc.org/pubpolpillar/governance/igf-rio_speech_klensin.shtml; Internet; acccessed 3 March 2009.

[166] Munk Centre, University of Toronto. Citizen Lab Press Conference. Posted 31 March 2009. http://hosting.epresence.tv/MUNK/1/watch/104.aspx; Internet; accessed 1 April 2009.

[167]The Citizen Lab and SecDev Group, "Tracking Ghostnet: Tracking a Cyber Espoinage Network", JR02-2009, March 29th, 2009. http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network; Internet; accessed 29 March 2009.

[168] Richard, S. Zembek, "Jurisdiction and the Internet: Fundamental Fairness in the Networked World of Cyberspace", *Albany Law Journal of Science and Technology*, Vol. 6, 1996, 342.

include: personal and subject matter jurisdiction; choice of law; and enforcement - each bringing new complexities to cases involving the Internet.[169] Additionally, Benjamin R. Davis argues that governments have done little to impose a legal framework that enables law enforcement with the tools and information required to prosecute criminal and terrorism cases.[170] In particular he cites how the Patriot Act in the US is not tough enough on ISPs. He points out that the Act provides immunity to ISPs who choose to voluntarily disclose information to law enforcement, and that nobody is obliged to cooperate. He advocates for example that the Internet Corporation for Assigned Names and Numbers (ICANN)[171] and its stakeholders should implement more preventative measures that could enable ISPs and regulators to track and block users that use the Internet to conduct terrorist acts.[172]

Clearly, the from a legal perspective, the distinction between Cyber acts that are criminal, terrorism, hacktivism[173] or acts of war relies upon two important factors: intent and the source. The intent may be easy to trace, based upon on the resulting impact of a computer attack such as the damage or disruption to websites, data, systems or networks. The identification of the source of the attacks may prove more elusive, as revealed by the SecDev

---

[169]Derek Bambauer, John G, Palfrey, Jr., and Jonathan L. Zittrain "A Starting Point: Legal Implications of Internet Filtering" (2004) http://opennet.net/docs/Legal_Implications.pdf; Internet; accessed 20 March 2009.

[170] Benjamin R. Davis, "Ending the Cyber Jihad: Combating Terrorist Exploitation of the Internet with the Rule of Law and Improved Tools for Cyber Governance", *Common Law Comspectus* Vol. 15, 2006-2007, 171.

[171]Internet Corporation for Assigned Names and Numbers, http://www.icann.org/; Internet; accessed 20 March 2009. ICANN was formed in 1998. It is a not-for-profit public-benefit corporation with participants from all over the world dedicated to keeping the Internet secure, stable and interoperable. It promotes competition and develops policy on the Internet's unique identifiers. ICANN doesn't control content on the Internet. It cannot stop spam and it doesn't deal with access to the Internet. But through its coordination role of the Internet's naming system, it does have an important impact on the expansion and evolution of the Internet.

[172]*Ibid.*, 179.

[173]**Hacktivism**, a kind of electronic civil disobedience in which activists take direct action by breaking into or protesting with government or corporate computer systems.
http://www.wired.com/politics/law/news/1998/09/15129

Group and the Munk Centre's Citizen Lab, in their report *Tracking Ghostnet: Tracking a Cyber Espoinage Network*[174] and Greylogic's *Project Grey Goose Phase II Report: The evolving state of cyber warfare.*[175] In both cases, in spite of months of efforts to track and identify the source of the nefarious Cyber activities, they have failed to positively identify the exact source in a conclusive way.[176] There are strong indicators, but they were limited to Open Source Intelligence (OSINT) which resulted in incomplete source determination. What these reports have achieved is a new level of public awareness for these activities, but as Ron Diebert points out in a press conference, in order to make positive attribution in such Cyber cases requires state and military intelligence resources.[177] Legally the Citizen Lab believe they broke no laws but also had no legal mandate and took risks by logging onto the compromised and unsecured GhostNet control server.[178] The team also had no influence in area of

---

[174]The Citizen Lab and SecDev Group, "Tracking Ghostnet: Tracking a Cyber Espoinage Network", JR02-2009, March 20th, 2009. http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network; Internet; accessed 29 March 2009. The Information Warfare Monitor, laid out the findings of a 10-month investigation of alleged Chinese cyber spying against Tibetan institutions. The investigation ultimately uncovered a network of over 1,295 infected hosts in 103 countries. Up to 30% of the infected hosts are considered high-value targets and include computers located at ministries of foreign affairs, embassies, international organizations, news media, and NGOs. The Tibetan computer systems they manually investigated, and from which their investigations began, were conclusively compromised by multiple infections that gave attackers unprecedented access to potentially sensitive information.

[175]Greylogic, "Grey Goose Report Phase II Report: The evolving state of cyber warefare." 21 Mar 09 http://greylogic.us/?page_id=85; Internet; accessed 1 April 2009. This report aims to answer the following questions by examining three different cyber events impacting almost a dozen nations: How effective is Social Network Analysis in Computer Network Exploitation? How critical is the ability to access black (classified) data in a cyber intelligence effort? Is there evidence that points to Russian government involvement in the Georgia cyber attacks of July and August 2008?

[176]John Arquilla and David Ronfledt, *The Advent of Netwar*, 1996, 96. Indeed, the problem of ultimate identification may be a central security dilemma posed by the advent of netwar.

[177]The Citizen Lab press conference, http://hosting.epresence.tv/MUNK/1/watch/104.aspx; Internet; accessed 1 April 2009. Ron Diebert from the Munk Centre at University of Toronto stated that: "state intelligence organisations and military that develop doctrine & strategies to fight and win wars on the Internet… that is their job".

[178]Canadian Broadcasting Corporation, "Podcast #27: exposing the world's biggest cyberspy ring", posted 30 March 2009. http://www.cbc.ca/searchengine/blog/2009/03/podcast_27_exposing_the_worlds_biggest_cyberspy_ring.html#more; Internet; accessed 1 April 2009.

jurisdiction where the servers reside and their work ended when the Chinese government refused to cooperate in the investigation.[179]

To properly triage the potential intents and source(s) of Cyber activity requires advanced Cyber skills but also intelligence information about the perpetrator(s) or attacker(s), a discipline integral to the CF, CSIS, RCMP and CSEC.[180] In other words, some form of advanced notice of an attack or information about the source is necessary to determine intent and to prevent the attack or to prosecute the attackers. In addition to intelligence resources, this demands a full suite of CNO capabilities: including CND and CNE to protect your own systems and prevent attacks, and in the event that prevention fails, CNA capabilities may be required to counter or deter Cyber attacks.[181] From a legal perspective, the CF can conduct CNO activities domestically as well as internationally, and it possesses clear mandates as articulated in the NDA for CND and CNE activities. The CF can also conduct CNA, with its unique mandate to project armed force on behalf of the GC, when so ordered, using the Crown prerogative.[182] Various GC departments have access to international sources of intelligence

---

[179]Canadian Broadcasting Corporation, "Canadian research uncovers cyber espionage network", 29 March 2009. http://www.cbc.ca/technology/story/2009/03/29/internet-spying.html; Internet; accessed 6 April 2009. "It's all a question of jurisdiction. Obviously the Chinese government would have a capability — a legal jurisdiction — to investigate the servers located on their territory. But that is ultimately up to them," he [Rafal Rohozinski] told CBC News.

[180]These various websites indicate the mandates and roles of some key partners that DND could draw upon as needed: Canadian Security Intelligence Service (CSIS) Backgrounder1 http://www.csis-scrs.gc.ca/nwsrm/bckgrndrs/bckgrndr01-eng.asp Accessed 11 Mar 09. Communications Security Establishment Canada (CSEC) http://www.cse-cst.gc.ca/home-accueil/nat-sec/nsp-psn-eng.html (Accessed 11 Mar 09). Royal Canadian Mounted Police (RCMP) http://www.rcmp-grc.gc.ca/fs-fd/index-eng.htm (Accessed 11 Mar 09). Public Works Government Services Canada (PWGSC) http://www.tpsgc-pwgsc.gc.ca/app-acq/amac-cpsa/index-eng.html (Accessed 11 Mar 09). Public Safety Canada (PSC) http://www.publicsafety.gc.ca/prg/em/index-eng.aspx (Accessed 11 Mar 09).

[181]An analogy could be made between CNO activities and any military operation: CND provides the Shield function, CNE the Sense function and CNA the Act function.

[182]The NDA indicates that a Ministerial Authorization is required prior to allowing the CF to conduct CNE activities. No such provisions exist for other departments except CSEC. Where there are no statutes

which are unavailable to the other departments, so sharing of information may prove indispensable to the successful identification of the source of an attack. Once identified, if prosecution was the aim, the RCMP would be the lead since it would involve evidence collection activities;[183] however, to perform CNA activities, the CF would be the lead department with its own Cyber capabilities and mandate.

The Role of National Defence

The Chief of Defence Staff (CDS) and the Deputy Minister of National Defence have articulated the five Defence Priorities for 2009-2010 to be:

> 1. Achieve Operational and Mission Success in Afghanistan; 2. Support the 2010 Winter Olympics; 3. Align Defence Activities with Key Government Priorities (specifically CFDS); 4. Build the Defence Team; and 5. Build Excellence in Defence Management.[184]

The CDS also remarked that:

> Priorities do not define the Defence mandate or on-going duties and responsibilities, which are set out in legislation (the "National Defence Act"), and policy (Defence policy statements, Government announcements/Budgets).[185]

In other words, DND is responsive to the Government of Canada's priorities. Given the extant Cyber Operations capabilities within the CF that have direct applicability to the implementation of a national GC strategy for Cyber-security, it is logical for the CF to occupy

---

specifically enumerating provisions, such as for CNA, the GC's discretion or Crown prerogative can be exercised to grant permission to execute CNA activities on a case by case basis.

[183]RCMP Tech Crime Unit Website http://www.rcmp-grc.gc.ca/fs-fd/tcrime-crimet-eng.htm; Internet; accessed 11 March 2009.

[184]DND. "Defence Priorities (CDS)": http://barker.cfcacad.net/Admin/Goodgen/2008/defpri-2009-10_e.pdf; Internet; accessed 16 March 2009. – Available only on CFC Toronto's Academic Network.

[185]*Ibid*.

a leadership role in CNO at large. The GC CIO also recognized the CFNOC model as a promising one for the GC.[186] Three main reasons further support a leadership role for the CF: 1. the absence of any other comparable capability in the GC; 2. CFNOC's existing and mature capabilities in the realm of CNO; and 3. DND is the only department mandated under the NDA to conduct any form of CNO activity. The CF is also poised to share the expertise it has gained over the past seven years since the creation of CFNOC, this would also fall in line with the GC's priority of providing common shared services.

The GC philosophy of Shared Services Organizations[187] aims to improve efficiencies, reduce costs and standardize common services across government. Because of the economies of scale, larger departments offer an attractive starting point from which to replicate services. DND is one of the largest departments, with proven record of sound IT service management capability and a shared services vision that will be in place by 2010. A strong argument for OGDs to align themselves with DND Cyber structures and mechanisms is the efficiency and economies of scale that it can provide; DND's IM/IT Rationalization will yield $150 million dollars of savings per year.[188] Another salient example is the Global Defence Network

---

[186]Canada. Treasury Board Secretariat. Proactive Defence presentation by Ken Cochrane given on June 6th, 2008.

[187]Canada. Library of Parliament, "Shared Services: Lower Costs,Improved Services And A Change In Culture." http://www.parl.gc.ca/information/library/PRBpubs/prb0532-e.htm; Internet; accessed 16 April 2009. The primary advantage of the shared common services model lies in resource optimization (cost reduction and increased efficiency). In addition, it encourages a shift towards a culture of continuous improvement through performance objectives, in addition to facilitating access to expertise and encouraging innovation and development through "centres of excellence." The model also allows for the establishment, with other internal or external entities, of partnerships that create added value for the organization. Lastly, it allows clients to concentrate on their strategic activities.

[188]The Information Management Group (IMG) manages an IT inventory exceeding 100,000 desktop computers for DND. The IM Gp has initiated an aggressive IT Rationalization Project that will further improve the efficiency of managing such an array of unclassified and classified networks, yielding $150M/year of savings. By 2010, DND will have created a full IM/IT shared services offering. IM/IT Rationalization Presentation – Col Dufour DGIMST (Accessed 16 Apr 09).

Services (GDNS) contract that offers much more than just bandwidth and connectivity options compared to the PWGSC Shared Services Telecommunications Standing Offer. PWGSC's new Government Enterprise Network Services (GENS) initiative appears to try to emulate both of DND's successful managed services contracts (TSRP & GDNS) that have served DND since 2000 and saved ten million dollars annually.[189] As of March 2009, PWGSC's GENS has yet to be contracted and no implementation date is posted.[190]

The CF could also offer a highly secure model to emulate which would provide GC-wide Cyber-security at the highest levels without the overhead of reinventing a solution. DND is also one of the main departments that routinely uses cryptography and secure means to conduct its daily business; information security is at the core of every CF mission.[191] DND is the only department that provides common secure communications for other departments through the Canadian Defence Red Switch Network (CDRSN).[192] The main advantage to other departments is that DND has very high security requirements that they could share with all government departments in a cost-effective way.

---

[189]The savings were in comparison to DND's telecommunications services costs prior to the contracting for the Telecommunications Services Renewal Project (TSRP) in 2000.

[190]Canada. Public Works Government Services Canada. "Government Enterprise Network Services (GENS)." http://www.tpsgc-pwgsc.gc.ca/apropos-about/fi-fs/rceg-gens-eng.html; Internet; accessed 20 March 2009.

[191]Canada. Department of National Defence, B-GG-005-004/AF-010 *CF Information Operations.* Chief of Defence Staff, 1998), 3-7. INFOSEC is the protection of information systems against unauthorized access or information corruption. INFOSEC includes those measures necessary to detect, document, and counter such threats.

[192]Memorandum of Understanding between the Department of National Defence of Canada and the Department of Defense of the United States of America Concerning Combined Defense Information Systems Management in Support of Defense of North America (CANUS CDISM MOU), 6 March 2008. http://www.state.gov/documents/organization/111449.pdf; Internet; accessed 29 March 2009.

More fundamentally, the mandate of Defence assigned to the CF spans an area not assigned to any other department than the CF.[193] Only the CF can go to war or armed conflict for the GC and no other department has the protections under the Geneva Conventions to be a combatant in the event CNO is conducted under the auspices of a state-on-state conflict.[194] Until the debate is settled whether Cyber attacks constitute armed force or use of force, we have to assume the worst case, therefore, no other department than the CF should be tasked with the full CNO mandate that includes all three functions of CND, CNE and CNA. A compelling reason to classify CNA as a weapon, and hence a military matter, stems from the tactical and potentially destructive nature of CNA activities. A telling example of the military use of CNA was witnessed by the simultaneous use of Cyber and physical attacks upon Georgia on August 8th, 2008.[195] The penetrating and potentially disruptive and destructive capability of CNA activities, although technically non-lethal, can have devastating operational and even strategic effects that complement or even substitute conventional operations. Just as Electronic Warfare capabilities can disrupt radar or communications services in a non-lethal manner, CNA should be fully synchronized in certain operations by the CF as another tool to produce desired battlefield effects.[196] It has been argued by Sylvain Leblanc and Scott Knight

---

[193]Canada. *National Defence Act*, Section 14. http://laws.justice.gc.ca/en/ShowFullDoc/cs/N-5///en; Internet; accessed 20 March 2009. Canadian Forces: The Canadian Forces are the armed forces of Her Majesty raised by Canada and consist of one Service called the Canadian Armed Forces. The CF specifically refers to the military portion of DND, in exclusion of public servants.

[194]United Nations. *Protocol I to the Geneva Conventions*, 8 June 1977. Article 43, para 2. http://www.icrc.org/ihl.nsf/FULL/470?OpenDocument; Internet; accessed 19 April 2009. Members of the armed forces of a Party to a conflict (other than medical personnel and chaplains covered by Article 33 of the Third Convention) are combatants, that is to say, they have the right to participate directly in hostilities.

[195]NATO CCDCOE. "Cyber Attacks Against Georgia: Legal Lessons Identified, Tallin, Estonia", version 1.0 dated November 2008, 3. http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf ; Internet; accessed 8 April 2009. Russia responded by military attack and intense international propaganda. Simultaneously, cyber attacks were launched against Georgia's websites oe on August 8, 2008, a large number of Georgian websites, both government and non-government, came under attack.

[196] Intelfusion, "Russia's Chechen Model for its Georgia Cyber Attack" http://intelfusion.net/wordpress/?p=392; Internet; accessed 1 April 2009.

that CNO be used in support of Special Operations Forces (SOF), where CNE could be combined with Signals Intelligence.[197] Because such covert CNE operations can be categorized as CNA, or even directly be CNA in nature, this CNO capability should rest with the CF.[198] This symbiotic relationship between CNE and CNA implies that although technically we can deconstruct the activities into categories, the resultant effects are what matter. The victim of these effects would likely perceive these actions as attacks either under the UN Charter or in legal terms, and therefore could decide to retaliate to these actions. A Russian general provided the most extreme example, by stating they had the right to respond aggressively by military means to any CNA launched against its military forces.[199]

Additionally, with the creation of Canada Command, the CF clearly has added Canada as its Area of Operations (AO) and, at the behest of the GC, is there to respond to national emergencies under the Emergency Management Act (EMA).[200] Despite being in a supporting role to OGDs in the case of domestic emergencies, the CF brings a unique Cyber capability set that is otherwise non-existent within the GC. The CF's Canada Command is also responsible

---

"Cyber warfare as a military strategy is still in its infancy, and Western conceptions of just what cyber warfare is are in sharp contrast to that of Russia and China."

[197]S.P. Leblanc and G.S. Knight," Choice of Force - Special Operations for Canada". Chapter 11: Information Operations in Support of Special Operations. D. Last and B. Horn eds., McGill-Queen's University Press, Montreal, 173-185 (2005). http://tarpit.rmc.ca/leblanc/publications/Leblanc_Knight-IO_in_Support_of_SO.pdf; Internet; accessed 20 January 2009.

[198]See Figure 3 of this chapter for a depiction of the overlapping categories of CNO.

[199]Cdr Vida M. Antolin-Jenkins, "Defining the Parameters of Cyberwar Operations: Looking for Law in all the Wrong Places?", *Naval Law Review*, Vol 132, 2005, 166. General V.I. Tsymbal, in a speech at a Russian-US conference on "Evolving Post Cold War Security Issues", Moscow, 12-14 Sept., 1995 stated: "from a military point of view, the use of Information Warfare against Russia or its armed forces will categorically not be considered non-military phase of a conflict whether there are casualties or not… Russia retains the right to use nuclear weapons first against the means and forces of Information Warfare, and then against the aggressor state itself".

[200]Canada. Parliament of Canada. *Emergency Management Act* Ascented 22 June 2007 http://www2.parl.gc.ca/content/hoc/Bills/391/Government/C-12/C-12_4/C-12_4.PDF; Internet; accessed 11 March 2009.

to support Canada's engagement in the defence of North America through the NORAD agreement.[201] As enumerated within the Bill C-7 of 2002, this amendment to the NDA indicates the possibility of the CF assisting CSEC in the collection of private communications in Canada under certain circumstances.[202] This CNE task, although primarily belongs to CSEC and CSIS, it is also a CF responsibility inherent to the CF mandate, to support OGDs and to effectively and proactively defend DND's networks.

The CND role has been the speciality of CFNOC since 2002 with a capability that is currently unmatched by any other GC department.[203] This experience and expertise is built over many years and the trusted relationships with other military organizations and industry around the world are uniquely available to CFNOC.[204] The information sharing and

---

[201]NORAD Agreement. http://www.treaty-accord.gc.ca/ViewTreaty.asp?Treaty_ID=105060; Internet; accessed 18 April 2009.

[202]Canada. *National Defence Act*, 2004, Section 273.65 (1). http://laws.justice.gc.ca/en/ShowFullDoc/cs/N-5///en; Internet; accessed 20 March 2009. Conditions for authorization: (4) The Minister may only issue an authorization under subsection (3) if satisfied that (*a*) the interception is necessary to identify, isolate or prevent harm to Government of Canada computer systems or networks; (*b*) the information to be obtained could not reasonably be obtained by other means; (*c*) the consent of persons whose private communications may be intercepted cannot reasonably be obtained; (*d*) satisfactory measures are in place to ensure that only information that is essential to identify, isolate or prevent harm to Government of Canada computer systems or networks will be used or retained; and (*e*) satisfactory measures are in place to protect the privacy of Canadians in the use or retention of that information.

[203] Canada. Treasury Board Secretariat. Proactive Defence presentation by Ken Cochrane given on June 6th, 2008.

[204]Numerous multi-national and bi-national agreements and Memoranda of Agreement regarding technology transfer and information sharing exist between the CF and other military organisations. For example, the International Traffic in Arms Regulations (ITAR) http://www.pmddtc.state.gov/regulations_laws/itar_official.html limit access to procurement programs from the US DoD military inventory. Canada has special access to the telecommunications software and hardware for the Defence Telephone Network (DTN) and the Canadian Defence Red Switch Network (CDRSN) through an MOU with the US Defense Information Systems Agency (DISA): CANUS CDISM MOU, 6 March 2008. http://www.state.gov/documents/organization/111449.pdf (Accessed 29 Mar 09). The NORAD agreement also provides for information sharing regarding the defence of North America. NORAD Agreement. http://www.treaty-accord.gc.ca/ViewTreaty.asp?Treaty_ID=105060 (Accessed 18 Apr 09). As a member of NATO, DND also has many other benefits regarding information sharing, particularly with the newly created Cyber Defence Management Agency (CDMA) in Casteau, Belgium.

interoperability arrangements currently in place with foreign organisations such as NATO are uniquely entrusted to the CF and not easily transferable to any other GC departments that are not military. The CF may not be able to extend these MOUs and agreements to OGDs but has the potential to provide the Cyber security benefits that result from these arrangements.

The CF also benefits from the direct support of the Defence Research and Development Canada (DRDC) and its Network Information Operations (NIO) branch. Several DRDC projects have produced customized software tools to improve the effectiveness of CFNOC. The Joint Network Defence Monitoring System (JNDMS) project has added an impressive capability in the assessment of the impact of a computer attack, or any network degradation, on military operations.[205] The NIO branch has also developed other tools to improve the throughput of CFNOC's Intrusion Detection System (IDS) analysis team. The team of Defence Scientists bring invaluable intellectual capacity and through the Technology Exploitation Network (TEN), harness the power of industry partners as well.[206] DRDC is an impressive and integral capability that is nested within the defence team and enhances the CF's Cyber Operations capability set. Co-located with DRDC is the Canadian Forces Experimentation Centre (CFEC), which supports experimentation on several networks including the Canadian Forces Experimentation Network (CFXNet), the Canadian segment of the Combined Federated Battle Lab Network (CFBLNet).[207] This environment allows the conduct of realistic multi-user, multinational experiments and demonstrations such as the

---

[205]DRDC Ottawa. http://www.ottawa.drdc-rddc.gc.ca/html/nio_201_jndms-eng.html; Internet; accessed 24 March 2009.

[206]DRDC Ottawa. http://www.ottawa.drdc-rddc.gc.ca/html/ten-eng.html; Internet; accessed 24 March 2009.

[207]Canada. Department of National Defence, "Canadian Forces Experimentation Centre (CFEC) Networks." http://www.cfd-cdf.forces.gc.ca/sites/page-eng.asp?page=206; Internet; accessed 24 March 2009.

annual Coalition Warrior Interoperability Demonstration (CWID).[208] The Information Management Group J6 Coordination cell is responsible for the Canadian participation in CWID and CFEC provides the technical support for the networks. Among other activities, the JNDMS was showcased in both CWID 2007 and 2008. This facility, combined with the creativity and reach of the Defence Scientific community, is a powerful resource that positions the CF to be at the front lines of Cyber operations.

Finally, in implementing an Integrated Security Strategy, one must also address the overlapping or converging trends of sectors such as intelligence, security and defence.[209] Having an organization that has experience and mandates in all these domains represents a key enabling factor. Within the Government of Canada, the CF has both the requirement and capacity to meet the unique challenges of CNO. It is important to recognize that the CF cannot and should not be alone in executing CNO tasks, but rather be a leader working in concert with those departments that have a role in intelligence, security and emergency management as well as with businesses that provide services and products in support of CNO.

The Role of Industry

There have been numerous references made to Telecommunications companies and Internet Service Providers (ISPs) in this paper demonstrating the clear relationship industry plays in the security and management of the Information Technology Infrastructure (ITI) and

---

[208]Coalition Warrior Interoperability Demonstration (CWID) http://www.cfd-cdf.forces.gc.ca/sites/page-eng.asp?page=86; Internet; accessed 19 April 2009.

[209]Canada.John Manley, P.C., Independent Panel on Canada's Future Role in Afghanistan. http://dsp-psd.tpsgc.gc.ca/collection_2008/dfait-maeci/FR5-20-1-2008E.pdf; Internet; accessed 20 March 2009. The three lines of operation (security, governance and development) are described as "connected dimensions". In the context of this mission, security refers to the Afghan military and Police forces. The report recommends the purchase of intelligence gathering UAVs which directly support the security mission.

National Critical Infrastructure (NCI). From a legal perspective, there are also pressures being placed upon ISPs to be more involved in the securing of the Internet from illegal and terrorist activities. What remains to consider is how industry can actually make a difference in this complex, anonymous, transnational and highly dynamic maze of relationships that are conducted over the Internet.

An effective enterprise network defence requires the multi-layered protection approach between end users and Tier-1 telecommunications carriers or ISPs. It requires sound CND practices such as enterprise perimeter defences or firewalls and Intrusion Detection Systems (IDS) as well as host-based solutions such as applying software security updates, personal firewalls, Anti-Spam, Anti-Virus (AV) and and Anti-Spyware. In spite of these measures, there are still threats called zero-day[210] threats for which there are no defences or AV signatures available because they are so new on the Internet. Tyson Macaulay of Bell Canada argues that a Tier 1 telecommunications carrier is actually the only entity that can detect zero-day cyber threats and vulnerabilities.[211] In his analysis using real data, it was demonstrated that, relying strictly on perimeter and host-based security using off-the-shelf solutions is insufficient to thwart zero-day threats. The conclusion of this study clearly underscores the value of cooperation with Tier-1 carriers who process the bulk of the Internet traffic and consequently are usually the first to detect these zero-day threats. They are also best positioned to filter these threats from reaching its customers.

---

[210] http://what-is-what.com/what_is/zero_day_exploit.html; Internet; accessed 20 March 2009. The term zero-day refers to the amount of time that systems administrators have to patch susceptible systems after a vulnerability becomes known.

[211] Tyson Macaulay, "Carrier Grade Threat and Vulnerability Intelligence", Bell Canada. December 2008.

The concept of having ISPs provide customers with "clean pipes"[212] or filtering of malicious content, is not new and has been advocated for the purposes of preventing the distribution of pornography or to prevent copyright infringement.[213] Conversely, civil liberties advocates are opposed to such filtering measures. Additionally the forces of the free market economy over the Internet make it difficult to separate malicious Spam from legitimate advertising.[214] The commercialization of the web began in earnest in 1996 when the percentage of .com (commercial) websites rose to 50% and in 2000 reached 78% of all websites, a factor that removes much of the incentive to try to regulate the Internet.[215] Equally, the transnational reality that some destination ISPs may not be subject to the same cultural, legal and customary practices, the enforcement of a law applicable to residents of Canada are not necessarily applicable uniformly across the Internet.[216] Because public law cannot be enforced abroad, ISPs have no incentive to enforce these laws, so the tendency is simply to do nothing.[217] Hence, despite the additional security ISPs can provide by providing its customers

---

[212]Clive Addy, "Cyber Security: An Expert Opinion from Ed Amoroso", *Frontline* Security, Issue #4, Winter 2008/2009. http://www.frontline-canada.com/FrontLineSecurity/index.php?page=109; Internet; accessed 6 March 2009. Dr. Ed Amoroso, AT&T's Chief Security Officer suggests the concept of clean pipes as a mechanism to protect users. "Instead of focusing on protecting multiple millions of guarded bubbles, in millions of homes, I have suggested that we produce a guarded community wherein the providers such as my company or major Canadian providers like Bell, Telus or Rogers be required to "clean the pipes" before sending these dangerous cyber-threats towards you to be screened by a complex and inadequate firewall."

[213]Jonathan Zittrain. "Internet Points of Control". http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2003-01.pdf; Internet; accessed 20 April 2009.

[214]Derek Bambauer, John G, Palfrey, Jr., and Jonathan L. Zittrain "A Starting Point: Legal Implications of Internet Filtering" (2004) http://opennet.net/docs/Legal_Implications.pdf

[215]Jose MA. Emmanuel Caral. *Lessons from ICANN: Is self-regulation of the Internet fundamentally flawed?* International Journal of Law and Information Technology, Vol. 12, No. 1, Oxford University Press, 2004, 28.http://www.heinonline.org/HOL/PDF?handle=hein.journals/ijlit12&collection=journals&id=7&print=31&sectioncount=&ext=.pdf; Internet; accessed 20 March 2009.

[216]New York Times. "Vast Spy System Loots Computers in 103 Countries", 28 March 2009. http://www.nytimes.com/2009/03/29/technology/29spy.html?pagewanted=2&_r=1; Internet; accessed 6 April 2009. Beyond that, said Rafal A. Rohozinski, one of the investigators, "attribution is difficult because there is no agreed upon international legal framework for being able to pursue investigations down to their logical conclusion, which is highly local."

with “clean pipes”, civil rights and free market forces tend to discourage such a control over Internet content. Another obstacle to the use of a “clean pipe” strategy is the lack of customers willing to pay for this service, despite the clear advantages and immediate payoff from a proactive security perspective.[218]

Another way industry could be useful in assisting law enforcement is through longer data retention practices. In the US there are senators pushing for the increase from 90 days to a full two years of user Internet usage data.[219] At this point the intent is to deal with cases of child pornography, but this data could be useful in any legal case. However, as with the question of clean pipes, unless this applies to destination ISPs outside the jurisdiction of this law, this represents only a partial solution. The value of data retention would be to improve our ability to mount effective Cyber operations by having access to several months of history on a particular target. By knowing more about the skills and practices of a potential target, this can provide valuable intelligence about their methods and contacts as well as the victims. It would also greatly assist in the task of identification by providing a more complete picture of which systems an attacker has compromised. Access to such a data store in essence would fulfil an invaluable CNE function for RMCP forensic criminal investigations as much as for CF preparations to mount CND, CNE or CNA operations.

---

[217]Uta Kohl, “The Rule of Law, Jurisdiction and the Internet”. *International Journal of Law and Technology*, Vol 12, No. 3, 2004.

[218]Ed Amoroso, “IT Conversations” Podcast Interview with Sandra Schneider, published 29 January 2006. http://odeo.com/episodes/670129-Ed-Amoroso-Frontline-Security. *Frontline Security*; Internet; accessed 5 March 2009. He argues that the only reason that networked-based security (network in the cloud security) provided by the carriers has not occurred is that nobody is willing to pay for it. He predicts the demise of Demilitarized Zones (DMZs) and security at the edge of networks, i.e. predominant reliance firewalls, will disappear within two years. Filtering of volume perturbations by the ISP/carrier will be more effective at preventing Distributed Denial of Service (DDOS) attacks.

[219]CNN article Pressuring ISP for 2 year data retention. http://edition.cnn.com/2009/TECH/02/20/internet.records.bill/index.html; Internet; accessed 18 March 2009.

ISPs can therefore play a major role on many including protecting consumers against such things as zero-day vulnerabilities and Botnet attacks. Because of this key role, Jennifer Chandler suggests that legal or regulatory action is necessary to force ISPs to better protect their customers from Botnet attacks.[220] She argues that ISPs could be held liable for their role in hosting partly or entirely a Botnet attack. As much as the individual Internet users have a responsibility to protect their computers with up-to-date AV, software security patches and firewalls, they lack the tools to defend against many Botnets, while ISPs could intervene. The 2007 Estonia DDoS attack is a perfect example of how unprotected personal computers have facilitated the Botnets. She suggests that ISPs could have a proactive role by monitoring their end-users' computers and quarantine any infected machines before they cause any harm.[221] Therefore, ISPs can play a significant role, and may have a responsibility in improving Internet security, but it remains to be seen if market forces and/or legal challenges will affect the involvement of ISPs in securing the Internet.[222] Until such time, the burden remains with the end-users to provide the proper host-based protection to their systems.[223] The takeaway for the GC is that Tier-1 Telecommunications providers and ISPs are vital to its CND activities as well

---

[220]Jennifer Chandler, "Liability for Botnet attacks: using tort to improve cybersecurity", *Canadian Journal of Technology Law*. March 2006, 13. http://cjlt.dal.ca/vol5_no1/pdfarticles/chandler.pdf; Internet; accessed 5 March 2009.

[221]*Ibid.*, 14.

[222] David Bizeul, "Russian Business Network study" version 1.0.1, 20 November 2007. http://www.bizeul.org/files/RBN_study.pdf; Internet; accessed 1 April 2009.
"Internet service providers do not want to interfere with their users but if they don't, these users are at risk. ISPs will face this kind of dilemma more and more in a close future and that's why Internet regulators and countries have to enact rules to promote ISP filtering against dangerous zones such as RBN. The world would live better without RBN IP range."

[223]The Conficker worm for example exploits a known Microsoft vulnerability, users can protect their systems simply by applying the security updates issued by the Microsoft Security Bulletin MS08-067 – Critical Published: October 23, 2008. The vulnerability in server service could allow remote code execution (958644) http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx; Internet; accessed 2 April 2009.

as CNE and CNA activities, and individuals with Internet-connected computers can also play a significant CND role.

Responsibility Summary

The role of the GC is to regulate behaviour that maintains order and rule of law. To be effective, they need the assistance of cyber service providers and even individuals to meet this challenge. This effort begins by having the necessary policies and capabilities in place across the GC departments and requires focused planning and funding. Interdepartmental collaboration is required to address unresolved organizational, governance, technical, and jurisdictional issues. PSC's Government Operations Centre (GOC) integrates Cyber incident reports from all departments but lacks the mechanisms to do little more than high-level reporting and limited information sharing. All government departments are responsible for CND of their own networks, while some are mandated in specific areas, Cyber criminality for example is an RCMP responsibility. The CF is the only department with both the mandate and an existing CNO capability to conduct all three functions CND, CNE and CNA. CFNOC was cited in the GC Proactive Defence Proposal briefing as being the only Canadian model available currently with the elements in place to support the GC vision to be proactive rather than reactive; however, this policy is still unpublished and ill-defined. While more work is being accomplished in the policy realm, with the assistance of the CF, integration of existing GC capability remains a challenge to be resolved. The integration of intelligence and CNE capabilities from multiple departments including the CF, CSE, CSIS, RCMP and CSEC is vital to the ability to determine the intent and the source(s) of Cyber attacks. The CF can play a significant role in leading and integrating the implementation of GC Cyber initiatives through

its ability to generate economies of scale in contracting, security posture and requirements, experience in ITSM, access to international intelligence sources, ability to perform R&D in support of CNO, and its extant capability set within CFNOC. The CF is therefore poised to demonstrate leadership in the execution of recent Government announcements surrounding the Canada First Defence Strategy (CFDS) in the Cyber environment.

CHAPTER IV -POTENTIAL CNO CONTRIBUTIONS TO MEET THE CFDS MISSIONS

The recently published CFDS articulated "a clear level of ambition" for the CF, which brought into focus the Cyber environment as a threat vector for which core capabilities were required:

> In such a complex and unpredictable security environment, 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. Indeed, Canadians expect and deserve no less than a highly capable military that can keep them safe and secure while effectively supporting foreign policy and national security objectives.[224]

When the CFDS estimates were requested by the GC prior to its announcement, the Chief Force Development (CFD) had a deadline of May 2008 to perform the detailed work of identifying and estimating the joint requirements for the Air, Land and Maritime Environments[225] for the next 20 years. This impressive amount of work was done on time, by May 2008, which meant that only those items that were easily quantifiable were addressed, notably platform (vice capability) replacements for the three environments. CFD's challenge now is to repeat this exercise for the Space and Cyber environments in a similar timeline. Part of the difficulty will be the funding for any capability, since the large ticket items such as aircraft, ships and other vehicles have consumed most of the allocated funds. The other difficulty will be finding staff who have expertise in Space and Cyber environments to perform this analysis. To date, Space for the CF has been an ad hoc business that relied upon certain individuals who had a personal interest in these environments. Employment in Space has been limited to a few project offices within NDHQ, some exchange positions with NORAD and one

---

[224]Canada. Department of National Defence, "Canada First Defence Strategy", June 2008, 7. http://www.mdn.ca/site/focus/first/June18_0910_CFDS_english_low-res.pdf; Internet; accessed 11 November 2008.

[225]In Canada, the three elements Air, Land and Maritime are called Environments as opposed to "Services" in the US DoD. The NDA stipulates that the Canadian Forces are a unified force.

liaison position with the Canadian Space Agency. For the Cyber environment, the challenge is similar, personnel with education and experience in this environment are mostly those who have been employed at CFNOC, although there are new positions within the IM Gp J6 directorate and within Canada Command there is a J6 Information Protection officer.[226]

The tasks assigned to the CF represent a level of ambition that would see the Forces carrying out up to six different core missions potentially simultaneously. For the purposes of this paper, only the Cyber-related implications to these six missions will be discussed in this chapter:

1. Domestic and Continental Operations

On the domestic front, CFDS places particular focus on Arctic issues such as the surveillance of Canadian territory. The CF is at the centre of several space-based projects involving both commercial and military satellites. In particular, the Polar Communication and Weather (PCW) Satellite Constellation Project has interesting potential Cyber-related capabilities north of the 70 degree latitude.[227] Its communications channels will open the possibility of extending Internet and other communications services in the remotest areas of the Arctic and to provide mobile users access to the Public Switched Telephone Network (PSTN)

---

[226]Baker Spring and Mackenzie Eaglen. "Quarterly Defense Review (QDR): Building Blocks for National Defense." *The Heritage Foundation*, 28 January 2009. http://www.heritage.org/research/nationalsecurity/bg2234.cfm; Internet; accessed 29 March 2009. The QDR is the US equivalent of CFDS and it identified in its **Building Block #10: Deterring, protecting, denying, and attacking in cyberspace** that "the requirements for structuring, manning, equipping, and training U.S. cyber forces are still not well understood. Thus, the first step for the QDR is to affirm the military mission". Therefore the challenge of understanding Cyber requirements is a problem that plagues the US just as much as Canada.

[227]Canada. Department of National Defence, Director Space Development Presentation by Colonel F. Mala to the CFC Toronto JCSP Course 35, January 13th, 2009.

by the year 2016. Having positive control over these links is an important security capability that falls under the CF's CND mandate.

From a continental defence perspective, the CF's close partnership with NORAD through Canada Command is vital to monitor and secure airspace and space traffic. The project Sapphire for the Surveillance of Space will provide a monitoring capability to focus on space objects and debris 6,000-40,000 km above Earth. The Cyber aspect relates to the uplink and downlink encryption. For the integrity of the controls for the satellite, protecting it from unwanted attack or hijacking is vital.

These capabilities also answer the GC's CFDS expectations of delivering excellence at home which:

> requires the Forces to be aware of anything going on in or approaching our territory, deter threats to our security before they reach our shores, and respond to contingencies anywhere in our country.[228]

Both these capabilities not only provide Canada with highly useful monitoring assets, an important feed into the intelligence network, they enable the CF to operate in new areas securely and demand CND, CNE and potentially CNA capabilities.

2. Major International Events

The CFDS announcement specifically identifies the Vancouver 2010 Winter Olympics as an event supported by the CF. The CF plays a supporting role to the RCMP for security and

---

[228]Canada. Department of National Defence. *Canada First Defence Strategy*, June 2008, 21 http://www.mdn.ca/site/focus/first/June18_0910_CFDS_english_low-res.pdf; Internet; accessed 11 November 2008).

the Cyber defences are an important part of this event, similar to the Beijing Olympics.[229] Although the data networks for this event will not be on DND infrastructure, the CF will have its networks operating in the command centre in Vancouver to coordinate any CF or NORAD involvement as required via secure means. To ensure interoperability between government departments and local authorities demands special planning and security measures the Vancouver 2010 Integrated Security Unit (VISU) was created, joining the forces of the RCMP, the CF and the Vancouver Police Department.[230] CFNOC also offers an important capability from a CND perspective.

3. Response to a Major Terrorist Attack

Terrorism can take many forms and threatening the use of force or violence with the intent of coercing people for certain ideological or political reasons has naturally included the Internet.[231] The Internet is a prolific conduit for the exchange of tactics and techniques to facilitate many forms of terrorism, such as how-to manuals on bomb-making and Botnet attacks. The CF has taken over the counter-terrorism operations from the RCMP with the creation of JTF 2 on April 1, 1993; it must therefore address the Cyber threats that can accompany any physical terrorism activity.[232] This is an area of specialization that was proposed as early as 2002 for the implementation of a new SOF capability, including CNE /

---

[229]http://www.byteandswitch.com/document.asp?doc_id=160638; Internet; accessed 26 March 2009.

[230]VISU http://www.canada2010.gc.ca/invsts/srvcs/030202-eng.cfm; Internet; accessed 26 March 2009.

[231]Lech Janczewski, Andrew M. Colarik, and Inc Books24x7. *Cyber Warfare and Cyber Terrorism*. Hershey, PA: Information Science Reference, 2008, 2.

[232]Canada. Department of National Defence, http://www.jtf2.forces.gc.ca/ajt-sfo/index-eng.asp; Internet; accessed 26 March 2009.

CNA, as described by Major (now Lieutenant-Colonel) Allen, the first Commanding Officer of CFNOC, in her paper on CNE/CNA.[233]

4. Support to Civilian Authorities

This particular core mission normally is associated with providing equipment and personnel to assist civilian authorities during natural disasters. Beyond the traditional responses to assist provinces with flooding or ice storms, the CF is poised to provide robust and resilient Cyber services to emergency organisations such as police, fire and ambulance. In the event that natural disasters affect civilian infrastructure, CF networks could be used to provide command and control of these services. Also, as described in Chapter III, the CF's stringent service level requirements levied upon its telecommunications services providers can be implemented by provinces and municipalities simply by emulating the federated model of the CF's CIS services. Finally, the provinces and the municipalities across Canada have no CNO capabilities within their existing services, only IT service delivery organisations.[234] By operating a robust CNO capability, the CF in effect also provides a measure of protection to all of Canada, not just the GC.

[233]Major F.J. Allen, "CN(Eh?) – A Recommendation for the CF to Adopt Computer Network Exploitation and Attack Capabilities." Canadian Forces College, 2002, 6.

[234]http://www.misa-asim.ca/en/news/Launched.html; Internet; accessed 21 April 2009. MISA/ASIM Canada is the collective voice for its member associations on national issues affecting effective delivery of municipal services using information and technology. It is mostly an information sharing forum relating to the effective delivery of municipal services, using information and technology..

5. Lead or Conduct a Major International Operation

The CF is currently involved in leading a major coalition task force in the Kandahar, Afghanistan and the Cyber and intelligence aspects of this mission are an important part of the successful planning and execution of operations. Secure and reliable CIS services in expeditionary operations provide the CF essential capabilities that enable planning, intelligence and coordination tasks. Working within a multinational setting also requires the integration of multi-caveat and multi-level networks such as to enable secure data and e-mail sharing in large headquarters. CFNOC is at the core of the Canadian Cyber protection effort in our deployed operations.

6. Deploy in Response to Crises for Short Periods

Finally, the mobility of CF personnel and equipment is tied to having the necessary communications infrastructure and equipment to link our networks world-wide in the most demanding and austere locations. In the GDNS telecommunications services statement of work, international communications services were added to facilitate the implementation of CIS services anywhere in the world, providing the CF with the necessary reach in a timely manner which is responsive to any expeditionary operational tasking from the GC. Monitoring and protecting these vital links is also a CFNOC responsibility.

More generically, the statement in CFDS about "core capabilities and flexibility required to successfully address both conventional and asymmetric threats, including terrorism, insurgencies and cyber attacks"[235] speaks to having a readiness level that matches the threats. For this to be so, a full

[235]Canada. Department of National Defence, *Canada First Defence Strategy*, June 2008, 21 http://www.mdn.ca/site/focus/first/June18_0910_CFDS_english_low-res.pdf; Internet; accessed 11 November 2008.

365/24/7 operation of CFNOC is clearly required. To meet this demanding standard, there are significant but addressable sustainment challenges to be considered.

CFDS Sustainment Issues

As illustrated, every one of the six core CF missions assigned to the CF by the GC is in some way linked to CNO. Every scenario involves sophisticated CND capabilities and consequently, due to the requirement to be proactive as demonstrated in Chapter III, CNE and CNA activities are also inevitable to successfully protect the CF's networks. Key to enabling the CF with the required tools to effectively "Fight the Networks"[236] is the access to the defence scientific capability of DRDC. The CFDS concludes by underscoring:

> that the global security environment and capabilities required to deal effectively with it will continue to evolve, the Government is committed to reviewing this comprehensive plan on a regular basis to ensure that it continues to meet the needs of the military and Canadians.[237]

With this statement, there is clear intent on the part of the GC to adapt and continuously support the development of the CF's Cyber capabilities to meet the demands of all assigned mission sets. The CF's ability to meet these demands is not a question of mandate but one of resources, in order to sustain a CNO capability. To fully appreciate the requirements of such a Cyber capability, it is necessary to explore the force generation factors for the CF.

---

[236]The motto of the Canadian Forces Network Operations Centre (CFNOC) is "Fight the Networks".

[237]Canada. Department of National Defence, *Canada First Defence Strategy*, June 2008, 21 http://www.mdn.ca/site/focus/first/June18_0910_CFDS_english_low-res.pdf ; Internet; accessed 11 November 2008.

Force Generation Challenges

There are two broad aspects that affect personnel resources, the force generation[238] of personnel and the retention of personnel. Despite its operational successes after seven years of existence, CFNOC suffers from several issues that limit its ability to effectively conduct the full suite of CNO, particularly if the six assigned missions are to be addressed simultaneously. The first obstacle remains staffing, this organisation requires additional resources to truly provide 365/24/7 coverage, with a complement of specialized personnel available for every shift. Since 2004, at its peek CFNOC has had no more than a total of 92 military and civilian positions filled.[239] For CFNOC, posting cycles, promotions, and the current operations tempo have been the primary reasons for the depletion of line resources. CFNOC's actual annual posting cycle replaces on average 28.5% of existing staff, which creates an imposing training demand both in terms of formal courses and staff mentoring.[240] One method of relieving this pressure would be to revisit the tour lengths for military personnel assigned to CFNOC.

The question of limiting the posting frequency was a recommendation by the Defence Scientific Advisory Board (DSAB) in a report that identified a similar issue in retaining sufficient military staff for reasons of interoperability and network readiness.[241] Originally CFNOC was uniquely composed of military members, however, in 2007, ten military positions

---

[238]Force Generation (FG) in the CF generically refers to the capability production cycle. For personnel, this involves recruitment, training and education to produce a qualified military capability. The authorities responsible for the FG function in the CF are the Environmental Chiefs of the Air, Land and Maritime environments.

[239]CFNOC Official Historical Reports for unit #6323 for the years 2004 through 2007.

[240]*Ibid*. The percentage of new staff posted-into CFNOC has been 27% (2004), 30% (2005), 34% (2006) and 23 % (2007).

[241]Canada. Defence Science Advisory Board, *Network Readiness Requirements for Interoperability with Allies*,[2008]).

were converted to civilian positions. This was in response to the high unavailability and deployment rates of military members and the annual losses associated with the posting cycle. Although there is no guarantee that the Computer Systems (CS) civilian positions will not suffer from a high turnover rate, the employees are not forced to move away every two to three years or to deploy like the military personnel. Until the proposed CFSCE and RMC training and education programs are in place, the question of force generation will remain difficult since 87% of CFNOC's personnel is military, which creates a significant annual training requirement.

Cyber Training

Cyber training of CFNOC personnel is also expensive, averaging approximately $50,000 per member over a two year period.[242] Recently however, the CF has developed some internal educational resources through a partnership with the Royal Military College's (RMC) postgraduate Computer Science Department.[243] This initiative is vital because it provides higher quality education and training by allowing hands-on laboratory work on a replica of DND's own networks, using the same tools as those used at CFNOC. This is a great improvement over the more generic training available from commercial training firms and it will be much more cost-effective in terms of money and training time. The three key thrusts of the services available from the RMC Computer Security Laboratory (CSL) include:

> a focused postgraduate program for CFIOG sponsored Master's students, regular computer network defence exercises for the CFIOG, CSE, DRDC, RMC community, and specialized training short courses for CFIOG personnel.[244]

---

[242]CFNOC annual business plan FY 07/08 planned $594,000 for training.

[243]Memorandum 3705-1 dated 20 May 2008 from RMC to CFIOG, Subject: OUTCOMES OF THE ONGOING COLLABORATION BETWEEN CFIOG AND THE RMC COMPUTER SECURITY LAB.

[244]*Ibid.*

This is a unique and powerful capability that can deliver value not only for the CF, but also to CSEC, the Defence Research community and possibly other government departments. This initiative is still embryonic however it has already benefited CFNOC in a tangible way:

> Since 2000 the CSL has trained 29 Master's and PhD students (completed study, or currently undergoing study). These 29 PG students are military, are providing awareness and expertise throughout the CF and DND. Of these 29 military students 4 have served [in the Canadian Forces Information Operations Group] CFIOG directly as staff officers.[245]

There are currently nine officer positions at CFNOC providing the leadership and significant technical expertise. Continued efforts are being promoted to ensure that CFIOG creates and sponsors PG positions within its organization to enable greater numbers of future RMC PG-qualified officers to contribute to the CNO task. However, the CF currently cannot meet the training demands of Cyber operators for the cadre of Non-Commissioned Members (NCMs) employed at CFNOC.

The CF technical training establishment for officers and NCMs, the Canadian Forces School of Communications and Electronics (CFSCE) is not currently delivering the necessary courses to accredit "Cyber warriors" or "Cyber Operators". It does produce network and system administrators but CFSCE does not qualify personnel to be assigned to CFNOC with the specialized Cyber Operations training. This is being addressed through initiatives at CFSCE to create a series of new military occupational specialties and courses to meet the CNO demands. In October 2008, CFSCE held a Symposium and created campaign plan to transform CFSCE by rebranding itself as the CF Network Operations Centre of Excellence.[246] The

---

[245] *Ibid.*

Commandant of the School aims to revamp the curriculum of the school to meet the growing demands for Cyber-trained professionals. This is a major endeavour that will take time to accomplish but is vital to the continued sustainment and growth of the CNO resources required by the CF.

Institutional Inertia

In addition to the problem of competing for resources across environments, other important issues are raised by the Land Ops 2021 ADO concept, including the impediments to the force generation process in a military organization such as the CF:

> Institutional inertia and resource constraints will in all likelihood prevent the development of a full complement of capabilities that exceeds those of well-funded adversaries, intent on focusing only on a few niche areas.[247]

Institutional inertia is an insidious factor that permeates organizations that value traditions, such as the military.[248] For the CF, until 2006, there was little incentive to address joint requirements such as Cyber Operations under one authority. With the implementation of the CF Transformation, and the creation of CFD in 2006, joint capabilities are now the responsibility of CFD. This is an important change given that CNO is one of those activities that is considered an enabler and each environment felt they should have a role in its exploitation. Now that CFD has articulated the CF's operational role within the Cyber

---

[246]Canada. Department of National Defence, "Transforming the Network Fight", Canadian Forces School of Communications and Electronics (CFSCE) Network Operations Centre of Excellence. June 2008, 37.

[247]Canada. Department of National Defence. Directorate of Land Doctrine and Concepts. *Land Operations 2021: The Force Employment Concept for Canada's Army of Tomorrow* B-GL-310-001/AG-001, 2007.

[248]David Schmidtchen, *The Rise of the Strategic Private: Technology, Control and Change in a Network Enabled Military*, 2006.

environment, there is a mechanism to enable the growth and expansion of CNO capabilities with a centralized and joint focus.

For the CF, the organisational issues are simplified by the fact that CFNOC has had national responsibility for all DND networks since its inception. Underlying the importance of this centralization is the requirement for interoperability, not only across the CF but also with our national and international partners.

Interoperability

On the subject of interoperability, the DSAB report on *Network Readiness Requirements for Interoperability with Allies* highlights that:

> This leads to a consideration of the current situation concerning a national network enabled capability, which sees the CF working together with other government departments, other levels of government and first responders within Canada. Federalism and inter-governmental dimensions to interoperability are a serious weakness of Canadian governance at present.[249]

Key issues highlighted in the report that deter from achieving effective collaborative arrangements across government departments include: competition for resources, stovepipe management, legal impediments such as limitations on data sharing, the structure of the Canadian government, the ongoing movement of staff, distrust due to resource sequestering, and the erosion over the years of the resources to support IT services. To overcome this laundry list of impediments requires centralized leadership and focus which according to the DSAB report is still a work in progress:

---

[249]Canada. Defence Science Advisory Board, *Network Readiness Requirements for Interoperability with Allies*,[2008], 30.

> There is a clear tension that needs to be resolved regarding overall strategic direction. The Government's Canada First Defence Strategy includes the priority of overseas commitments and operations, and at the same time recognizes the importance of generating strong links with OGD's and other levels of government - preferably links that not generated in an ad hoc fashion during a crisis. As such, it is unclear whether the Government prioritizes interoperability within and across governments in Canada ahead of the current DND focus on achieving a high level of interoperability with US or coalition forces.[250]

The interoperability challenges such as information sharing were also recognized in a Report of the Standing Senate Committee on National Security and Defence regarding Emergency Preparedness in Canada.[251] The common theme is the required effort necessary to improve the current interoperability across all levels of government in Canada, but also internationally such as with key partners such as the US and NATO. For CFNOC, historically, it has been easier to resolve these interoperability issues with other nations than nationally, in large part because of the fifty years of trust and cooperation that has evolved through the CF's participation and collaboration with NATO. Working closely with OGD's in the Cyber environment is still a nascent experience for the CF but the experiences in Afghanistan as well as the preparations for the 2010 Olympic Games has fostered closer ties domestically.

The promising aspect to the challenge of interoperability is that the CF, through its partnerships with various nations has positive experiences to share with OGDs regarding the conduct of Cyber Operations in a federated model. CFNOC has been a successful leader on the international stage, fostering for example the creation of the International Network Analysis Teams (INAT) in five different countries.[252] This highly successful group of teams in

---

[250]*Ibid.,* 37.

[251]Canada. Report of the Standing Senate Committee on National Security and Defence, Vol. 1, Second Session, Thirty-ninth Parliament 2008, 64.

[252]CFNOC briefing to Information Systems Security Officers Course, Fall 2007, 6.

the US, UK, Australia, New Zealand and Canada share the load of work across time zones and share open source information in support of international CND under common procedures and reporting mechanisms.

Finally, interoperability presents a complex problem that requires more centralized direction on the part of the GC for domestic matters but also is key to international collaboration as required under the tasks and roles assigned through the CFDS.

CFDS Summary

For the first time, the role of Cyber is articulated in a Defence paper and demands new levels of performance for the CF to be responsive to a wide range of six potentially simultaneous core missions. Despite the challenges with CFNOC personnel training and staffing requirements, in the past year, several initiatives have sought to redress the shortages of trained personnel. That being said, the CFDS tasks place additional demands upon the existing unit which will definitely need to be augmented. The extent of the personnel gap remains a question to be answered, but the CF's CNO force generation requirements have increased by virtue of the new CFDS, particularly with the increased focus on domestic issues that require more collaboration and integration with OGDs. This may involve posting individuals with OGDs in a liaison capacity.

CHAPTER VI – CONCLUSION

This paper argues that the CF must deliver the Cyber Operations capabilities required to support the CFDS strategy in the Cyber environment. It described the Cyber environment in a Canadian context and Cyber Operations capabilities were shown to be essential in determining the adversarial intent and the identity of Cyber attackers. The lead government department to address specific Cyber threats depends on the intent and the identity of the perpetrators due to the implications as to information gathering and sharing imposed by the various departmental mandates. Because of the complex interconnectivity between the security and defence mandates, a solution to the integration challenges in dealing with Cyber attacks is needed. The CFNOC capability currently is a clear leader in all Cyber functions and the CF is assisting with the task of developing the GC Cyber policy. The Cyber governance and doctrinal issues in Canada are finally receiving the much needed attention, as the public, the military and government senior leadership have an increased awareness of the Cyber threats. The responsibility for Cyber Operations is increasingly pointing toward CFNOC given its track record and immediate availability to respond. Key to quickly harnessing the GC Cyber resources efficiently will be to build upon the existing niche specialization in specific departments and the sharing of existing capacity. CFNOC should therefore concentrate on its prime mission, which is to deal with defending Canada from network attacks, as outlined in the Canada First Defence Strategy (CFDS).

The CF's role in the Cyber environment against the six core missions assigned in CFDS must also be assessed in a quantitative manner to identify the resources required within the CFDS funding envelope prior to the next review cycle. The Chief of Force Development and the Information Management Group have limited time and qualified personnel to provide an

assessment of the capability gap to insert a true CNE and CNA capabilities within CFNOC to complement the existing CND capability. The assessment will need to identify the required increase in staff levels for CFNOC to operate the full complement of CNO capabilities (CND, CNE and CNA) on a 365/24/7 basis. In the meantime, the Cyber training and education plans elaborated by CFSCE and RMC should be implemented immediately to improve the force generation capacity within the CF and eventually aim to also extend it to OGDs, to address their CND capability gap.

The research supporting this paper was based on the limited unclassified data available regarding the Cyber threats and vulnerabilities, the GC may find value in conducting a separate analysis at the classified level to gain a full appreciation of the Cyber environment and its implications beyond those affecting the CF's ability to answer the requirements of CFDS. In summary, Canada's Cyber semantic gap can best be described as lessening. This is due in part to a growing momentum of policy development, financial support, intellectual and legal debate, interdepartmental cooperation and general awareness about Cyber issues. We are however currently not as prepared as we should be to address the existing and growing Cyber threats and should be more proactive, lest we suffer a significant Cyber attack while still determining our capacity. We have not yet learned the hard lessons that states like Estonia have faced, we can still reduce Canada's Cyber semantic gap.

Bibliography

Addy, Clive. “Cyber Security: An Expert Opinion from Ed Amoroso”, *Frontline Security*, Issue #4, Winter 2008/2009, p.19-21. http://viewer.zmags.com/publication/5a3c92e9#/5a3c92e9/189; Internet; accessed 6 March 2009.

Adee, Sally. “The Hunt For The Kill Switch”, Spectrum IEEE, Vol. 45, Isssue 5, May 2008. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4505310; Internet; accessed 8 April 2009.

AFCEA. "Report on OCIPEP Cyber Security Activities." http://afceaottawa.ca/uploads/JunReport2003.pdf; Internet; accessed 12 March 2009.

Allen, F. J., Major. "CN(Eh?) – A Recommendation for the CF to Adopt Computer Network Exploitation and Attack Capabilities."Canadian Forces College, 2002.

American National Standards Insitute. The Financial Impact of Cyber Risk: 50 Questions every CFO should ask**,** 2008 http://webstore.ansi.org/cybersecurity.aspx; Internet; accessed 21 October 2008.

Amoroso, Ed. Podcast Interview on Computer Security, published 29 January 2006. http://odeo.com/episodes/670129-Ed-Amoroso-Frontline-Security. *Frontline Security*; Internet; accessed 5 March 2009.

Antolin-Jenkins, Cdr Vida M., “Defining the Parameters of Cyberwar Operations: Looking for Law in all the Wrong Places?” *Naval Law Review*, Vol 132, 2005.

Arquilla, John and Ronfledt, David. *The Advent of Netwar*, 1996.

Bambauer, Derek, Palfrey, John G, and Zittrain, Jonathan L. “A Starting Point: Legal Implications of Internet Filtering” (2004). http://opennet.net/docs/Legal_Implications.pdf; Internet; accessed 20 March 2009.

Bar-Yam, Yaneer. *Making Things Work: Solving Complex Problems in a Complex World*. Cambridge, MA, USA; NECSI, 2004.

Beizer, Doug, “IPv6: 3 more big steps to the promised land”, *Federal Computer Week*, 6 February 2009. http://fcw.com/Articles/2009/02/09/IPv6-Next-Steps.aspx; Internet; accessed 18 February 2009.

Bell Canada. “Carrier Grade Threat and Vulnerability Intelligence”, December 2008.

———. "Security, Intelligence, Law Enforcement, Public Safety and National Defence Research: Bell Canada Security Story.", 2008.

Bidgoli, Hossein. *Global Perspectives in Information Security : Legal, Social and International Issues*. Hoboken, N.J.: J. Wiley & Sons, 2009.

Bizeul, David. "Russian Business Network study" version 1.0.1, 20 November 2007. http://www.bizeul.org/files/RBN_study.pdf; Internet; accessed 1 April 2009.

Budde, Paul. "2008 Canada – Telecoms, Wireless and Broadband." 20 February 2008. http://www.marketresearch.com/product/display.asp?productid=1687223&g=1; Internet; accessed 2 April 2009.

Byres, Eric and Lowe, Justin. "The Myths and Facts behind Cyber Security Risks for Industrial Control Systems. http://www.tswg.gov/subgroups/ps/infrastructure-protection/documents/The_Myths_and_Facts_behind_Cyber_Security_Risks.pdf; Internet; accessed 6 March 2009.

Bzostek, Rachel. *Why Not Preempt? : Security, Law, Norms and Anticipatory Military Activities*. Justice, International Law and Global Security. Aldershot, England ; Burlington, VT: Ashgate, 2008.

Canada. Canadian Security Establishment Canada. "Cyber Protection Supply Arrangement (CPSA)." http://www.cse-cst.gc.ca/its-sti/services/cpsa-amac/index-eng.html; Internet ; accessed 11 March 2009.

———. "CSEC Information Technology Security Training." http://www.cse-cst.gc.ca/training; Internet; accessed 17 March 2009.

Canada. Canadian Secruity and Intelligence Service. *Integrated Threat Assessment Centre (ITAC)* http://www.csis.gc.ca/nwsrm/bckgrndrs/bckgrndr13-eng.pdf ; Internet; accessed 12 March 2009.

Canada. Department of Justice. Bill C-7: *The Public Safety Act,* 2004, c.15 http://laws.justice.gc.ca/en/ShowFullDoc/cs/N-5///en; Internet; accessed 12 March 2009.

Canada. Directorate of Law Training, ed., B-GG-005-027/AF-022, *Collection of Documents on the Law of Armed Conflict* (Ottawa: Dept. of National Defence, 2005).

Canada. Department of National Defence. "About JTF." http://www.jtf2.forces.gc.ca/ajt-sfo/index-eng.asp; Internet; accessed 26 March 2009.

———. B-GJ-005-300/FP-000, *Canadian Forces Operations.* Ch 2, 15 October 2005.

———. B-GG-005-004/AF-010 *CF Information Operations.* Chief of Defence Staff, 15 April 1998.

———. B-GL-310-001/AG-001. Directorate of Land Doctrine and Concepts. *Land Operations 2021: The Force Employment Concept for Canada's Army of Tomorrow*, 2007.

———. "Canadian Forces (CF) Computer Network Operations (CNO) Policy - Draft for Ratification".

———."Canadian Forces School of Communications and Electronics (CFSCE) Campaign Plan: Transforming the Network Fight." Kingston: CFSCE, 2008.

———. "Canadian Forces Experimentation Centre (CFEC) Networks." http://www.cfd-cdf.forces.gc.ca/sites/page-eng.asp?page=206; Internet; accessed 24 March 2009.

———. "Canada First Defence Strategy", June 2008. http://www.army.forces.gc.ca/DLCD-DCSFT/pubs/sdca/June18_0910_CFDS_english_low-res.pdf ; Internet; accessed 19 February 2009.

———. *Canadian Forces Doctrine*. http://www.cfd-cdf.forces.gc.ca/sites/page-eng.asp?page=834; Internet; accessed 25 February 2009.

———. CFNOC briefing to Information Systems Security Officers Course, Fall 2007.

———. CFNOC Website. http://www.img-ggi.forces.gc.ca/org/cfi-goi/cfnoc-corfc-eng.asp; Internet; accessed 12 March 2009.

———. Chief Force Development (CFD) presentation by MGen Beare given to JCSP 35, CFC Toronto, 10 November 2008.

———. "Coalition Warrior Interoperability Demonstration (CWID)." http://www.cfd-cdf.forces.gc.ca/sites/page-eng.asp?page=86; Internet; accessed 19 April 2009.

———. Computer Network Operations Policy (Draft), 22 April 2008.

———. "Defence Priorities (Chief of Defence Staff)" http://barker.cfcacad.net/Admin/Goodgen/2008/defpri-2009-10_e.pdf; Internet; accessed 16 March 2009. – Available only on CFC Toronto's Academic Network.

———. Defence Terminology Databank http://terminology.mil.ca/index-eng.asp; Internet; accessed 3 March 2009.

———. DGIMST "IM/IT shared services offering." IM/IT Rationalization Presentation by Colonel Dufour; DND Intranet only; accessed 16 April 2009.

———. "DND Newsroom on proposed Bill C-42 BG-002.010." 30 April 2002. http://www.forces.gc.ca/site/news-nouvelles/view-news-afficher-nouvelles-eng.asp?id=329; Internet; accessed 12 March 2009.

———. Memorandum 3705-1 dated 20 May 2008 from RMC to CFIOG, Subject: Outcomes of the Ongoing Collaboration Between Cfiog and the RMC Computer Security Lab.

———. National Defence Policy Archives http://www.forces.gc.ca/admpol/newsite/defence%20policy%20archives.html; Internet; accessed 16 April 2009.

———. The Maple Leaf, Vol. 10, No. 29 http://www.forces.gc.ca/site/commun/ml-fe/article-eng.asp?id=3780; Internet; accessed 5 March 2009.

Canada. Defence Research and Development Canada. "Joint Network Defence and Management System (JNDMS)." http://www.ottawa.drdc-rddc.gc.ca/html/nio_201_jndms-eng.html; Internet; accessed 24 March 2009.

———. "Influence Operations: Historical and Contemporary Dimensions" DRDC Toronto CR-2007-126 http://cradpdf.drdc.gc.ca/PDFS/unc69/p528894.pdf; Internet; accessed 15 April 2009.

———. "Technology Exploitation Network." http://www.ottawa.drdc-rddc.gc.ca/html/ten-eng.html; Internet; accessed 24 March 2009.

Canada. Defence Science Advisory Board. *Network Readiness Requirements for Interoperability with Allies,* 2008.

Canada. House of Commons. "Anti-Terrorism." *Statutes of Canada Bill C-36*. Ottawa: 2001. http://canada.justice.gc.ca/eng/antiter/act-loi/index.html; Internet; accessed 11 March 2009.

Canada. Industry Canada. "Emergency Telecommunications." http://www.ic.gc.ca/eic/site/et-tdu.nsf/eng/Home; Internet; accessed 12 March 2009.

———. "Industry Canada National Cyber Protection." http://www.ic.gc.ca/eic/site/et-tdu.nsf/vwapj/Fact-CTCP-e.pdf/$FILE/Fact-CTCP-e.pdf; Internet; accessed 12 March 2009.

Canada. Office of the Judge Advocate General, ed. B-GG-005-027/AF-021, *The Law of Armed Conflict at the Operational and Tactical Level : Annotated.* Ottawa: Canada. Dept. of National Defence, 2001.

———. *Securing an Open Society: Canada's National Security Policy*. April 2004. http://www.pco-bcp.gc.ca/docs/information/Publications/natsec-secnat/natsec-secnat-eng.pdf; Internet; accessed 11 March 2009.

Canada. Office of the Auditor General, "2005 February Status Report of the Auditor General of Canada." February 1, 2005. http://www.oag-bvg.gc.ca/internet/English/parl_oag_200502_01_e_14921.html; Internet; accessed 16 March 2009.

Canada. Office of the Privacy Commissioner. “Deep Packet Inspection (DPI).” http://dpi.priv.gc.ca/; Internet; accessed 9 April 2009.

Canada. Privy Council Office. *Securing an Open Society : One Year Later : Progress Report on the Implementation of Canada's National Security Policy*. Ottawa: Privy Council Office, 2005.

Canada. Parliament of Canada. *Emergency Management Act* Ascented 22 June 2007 http://www2.parl.gc.ca/content/hoc/Bills/391/Government/C-12/C-12_4/C-12_4.PDF; Internet; accessed 11 March 2009.

———. *National Defence Act*, 2004, Section 14. http://laws.justice.gc.ca/en/ShowFullDoc/cs/N-5///en; Internet; accessed 20 March 2009.

———. *National Defence Act*, 2004, Section 273.65 (1). http://laws.justice.gc.ca/en/ShowFullDoc/cs/N-5///en; Internet; accessed 20 March 2009.

———. "New Public Safety Act Bill C7-Section 13-2002." http://www.parl.gc.ca/common/Bills_ls.asp?Parl=37&Ses=3&ls=C7#part13txt; Internet; accessed 12 March 2009.

———. "New Public Safety Act Bill C-42 First Reading." 22 November 2001, Part 10: *National Defence Act* (Clauses 80-91). http://www.parl.gc.ca/common/Bills_ls.asp?lang=E&ls=c42&source=library_prb&Parl=37&Ses=1#PART%2010; Internet; accessed 12 March 2009.

———. "Parliamentary Review of the Anti-Terrorism Act - Chief CSE Appearance 11 April 2005." http://www.cse-cst.gc.ca/home-accueil/nat-sec/review-ata-examen-lat-eng.html; Internet; accessed 11 March 2009.

———. "Parliamentary Committee Review of the Anti-Terrorism Act." http://www2.parl.gc.ca/content/hoc/Committee/391/SECU/Reports/RP2798914/sterrp07/sterrp07-e.pdf; Internet; accessed 11 March 2009.

———. “Report of the Standing Senate Committee on National Security and Defence”, Vol. 1, *Second Session, Thirty-ninth Parliament*, 2008.

———. *Securing an Open Society : Canada's National Security Policy*. Ottawa: Privy Council Office, 2004.

———. "Shared Services: Lower Costs, Improved Services And A Change In Culture." http://www.parl.gc.ca/information/library/PRBpubs/prb0532-e.htm; Internet; accessed 16 April 2009.

———. *Statutes of Canada Bill C-36*, (2001). http://www.parl.gc.ca/37/1/parlbus/chambus/house/bills/government/C-36/C-36_3/C-36TOCE.html; Internet; accessed 10 February 2009.

Canada. Public Safety Canada. “About Critical Infrastructure.” http://www.publicsafety.gc.ca/prg/em/nciap/about-eng.aspx; Internet; accessed 27 February 2009.

———. “About The Canadian Cyber Incident Response Centre (CCIRC).” http://www.publicsafety.gc.ca/prg/em/ccirc/abo-eng.aspx; Internet; accessed 17 March 2009.

———. "Canada's National Cyber Security Strategy Initiative." http://www.usaservices.gov/intergovt/documents/Session4-Presentation-Cyber-Security-RobertGordonE.PPT#286,1,Canada’s National Cyber Security Strategy Initiative; Internet; accessed 17 March 2009.

———. “Government Operations Centre” http://www.publicsafety.gc.ca/prg/em/goc/index-eng.aspx; Internet; accessed 17 March 2009.

———. *Government Operations Centre Business Continuity Planning guidelines*. http://www.publicsafety.gc.ca/prg/em/gds/bcp-eng.aspx; Internet; accessed 2 March 2009.

———. Information Technology Incident Management Plan (GC IT IMP), November 2008.

———. *Inventory of Government of Canada Cyber Security Activity*, National Cyber Security Initiative, 25 September 2008.

———. *Government Security Policy*. 1 February 2002. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12322&section=HTML; Internet; accessed 12 March 2009.

———. "Part 1 Working Towards a National Strategy-PSC." http://www.publicsafety.gc.ca/prg/em/cip/strat-part1-eng.aspx; Internet; accessed 11 March 2009.

———. "Part 2 Action Plan-PSC." http://www.publicsafety.gc.ca/prg/em/cip/strat-part2-eng.aspx; Internet; accessed 11 March 2009.

Canada. Public Works Government Services Canada. “Cyber Protection Supply Arrangement”, http://www.tpsgc-pwgsc.gc.ca/app-acq/amac-cpsa/index-eng.html; Internet; accessed 12 March 2009.

———. "Government Enterprise Network Services (GENS)." http://www.tpsgc-pwgsc.gc.ca/apropos-about/fi-fs/rceg-gens-eng.html; Internet; accessed 20 March 2009.

———. “Secure Channel.” http://www.tpsgc-pwgsc.gc.ca/apropos-about/fi-fs/cvcp-sc-eng.html; Internet; accessed 2 March 2009.

Canada. Royal Canadian Mounted Police. "RCMP Technological Crime." http://www.rcmp-grc.gc.ca/fs-fd/tcrime-crimet-eng.htm; Internet; accessed 11 March 2009.

Canada. Treasury Board. *Business Continuity Planning*. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12324; Internet; accessed 12 March 2009.

———. *Directive on Departmental Security Program*.

———. *Government of Canada IT Incident Management Plan*, 2008.

———. "Government Security Policy." http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12322&section=HTML; Internet; accessed 12 March 2009.

———. "Operational Security Standard: Management of Information Technology Security (MITS)." http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12328&section=HTML; Internet; accessed 12 March 2009.

———. Proactive Defence presentation by Ken Cochrane given on June 6th, 2008.

———. "TBS Security Policies." http://www.tbs-sct.gc.ca/pubs_pol/gospubs/tbm_12a/siglist-eng.asp; Internet; accessed 12 March 2009.

Canada and United States. "Memorandum of Understanding Between the Department of National Defence of Canada and The Department of Defense of The United States of America Concerning Combined Defense Information Systems Management in Support of the Defense of North America." (CANUS CDISM MOU), 6 March 2008. http://www.state.gov/documents/organization/111449.pdf ; Internet; accessed 29 March 2009.

Canada. Vancouver 2010 Integrated Security Unit (VISU). "Security Planning." http://www.canada2010.gc.ca/invsts/srvcs/030202-eng.cfm; Internet; accessed 26 March 2009.

Canadian Broadcasting Corporation. "Canadian research uncovers cyber espionage network (CBC.ca – more on Ghostnet)." http://www.cbc.ca/technology/story/2009/03/29/internet-spying.html; Internet; accessed 6 April 2009.

———. "Podcast #27: exposing the world's biggest cyberspy ring", posted 30 March 2009. http://www.cbc.ca/searchengine/blog/2009/03/podcast_27_exposing_the_worlds_biggest_cyberspy_ring.html#more; Internet; accessed 1 April 2009.

Caral, Jose MA. Emmanuel. *Lessons from ICANN: Is self-regulation of the Internet fundamentally flawed?* International Journal of Law and Information Technology, Vol. 12, No. 1, Oxford University Press, 2004, 28. http://www.heinonline.org/HOL/PDF?handle=hein.journals/ijlit12&collection=journals&id=7&print=31&sectioncount=&ext=.pdf; Internet; accessed 20 March 2009.

Center for Strategic and International Studies (CSIS). "Cyberspace: A New Dimension at our Fingertips." http://www.csis.org/media/csis/events/071128_estonia.pdf; Internet; accessed 19 February 2009.

Cerf, Vint. "A Brief History of the Internet." http://www.isoc.org/internet/history/brief.shtml; Internet; accessed 8 April 2009.

CGI Security. http://www.cgisecurity.com/xss-faq.html; Internet; accessed 16 April 2009.

Chandler, Jennifer. "Liability for Botnet attacks: using tort to improve cybersecurity", *Canadian Journal of Technology Law*. March 2006. http://cjlt.dal.ca/vol5_no1/pdfarticles/chandler.pdf; Internet; accessed 5 March 2009.

Chapman, Glenn. "Cyber crooks stalk users of social networks." *Agence France-Presse*, 4 March 2009. http://www.canada.com/Technology/Cyber+crooks+stalk+users+social+networks/1351029/story.html; Internet; accessed 25 March 2009.

Che. Elliot. "Securing a Network Society Cyber-Terrorism, International Cooperation and Transnational Surveillance." Carleton University RIEAS Research paper No. 113, September 2007. http://se2.isn.ch/serviceengine/FileContent?serviceID=10&fileid=FAD521F5-FD15-3D9F-3CAD-71E2629C3127&lng=en; Internet; accessed 11 March 2009.

Chuka, Neil S. "Confusion and Disagreement: The Infomation Operations Doctrine of the United States, the United Kingdom, Australia, Canada and NATO."Royal Military College of Canada, 2007.

Citizen Lab. http://www.citizenlab.org/; Internet; accessed 1 April 2009.

———. "Everyone's Guide to By-Passing Internet Censorship For Citizens Worldwide." September 2007. http://www.civisec.org/sites/all/themes/civisec/guides/everyone's-guide-english.pdf; Internet; accessed 1 April 2009.

Citizen Lab and SecDev Group, "Tracking Ghostnet: Tracking a Cyber Espoinage Network", JR02-2009, 29 March 2009. http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network; Internet; accessed 29 March 2009.

Citizen Lab press conference, http://hosting.epresence.tv/MUNK/1/watch/104.aspx; Internet; accessed 1 April 2009.

Connor, Gina. "Who Will Guard the Guardians? Legal Aspects of Information Warfare.", 2005.

Conrath, Chris. “Ottawa Commits to cyber-security strategy”, *IT World*, 14 May 2004. http://www.itworldcanada.com/a/ComputerWorld/df89791d-97aa-4b4a-b3f4-b4963ba0f0b5.html; Internet; accessed 11 March 2009.

Davis, Benjamin R. “Ending the Cyber Jihad: Combating Terrorist Exploitation of the Internet with the Rule of Law and Improved Tools for Cyber Governance”, *Common Law Comspectus* Vol. 15, 2006-2007.

Digital Forum. “DPI technology raises concerns says privacy commission.” http://www.digitalhome.ca/content/view/3588/280/; Internet; accessed 9 April 2009.

Directorate of Law Training, ed. B-GG-005-027/AF-022, *Collection of Documents on the Law of Armed Conflict*. Ottawa: Dept. of National Defence, 2005.

Dunn Cavelty, Myriam. *Cyber-Security and Threat Politics : US Efforts to Secure the Information Age*. CSS Studies in Security and International Relations. Milton Park, Abingdon, Oxon ; New York: Routledge, 2008.

Enterprise Information Magazine. “Corporate information theft is rife, according to survey.”. http://www.eimagazine.com/xq/asp/sid.0/articleid.5CE830BB-4E47-4488-A245-90A8E4140C69/qx/display.htm; Internet; accessed 16 April 2009.

Estonia. Ministry of Defence. “Estonia Cyber Security Strategy.” http://www.mod.gov.ee/static/sisu/files/Estonian_Cyber_Security_Strategy.pdf; Internet; accessed 19 February 2009.

Evron, Gadi, “Battling Botnets and Online Mobs Estonia’s Defense Efforts during the Internet War”, *Science & Technology*. (Winter/Spring 2008) Journal online; available from http://www.ciaonet.org/journals/gjia/v9i1/0000699.pdf; Internet; accessed 19 February 2009.

Gallaghar, Sean. “The Right Stuff for Cyber Warfare”,Defense Systems, 20 October 2008. http://defensesystems.com/Articles/2008/10/The-right-stuff-for-cyber-warfare.aspx; Internet; accessed 16 February 2009.

Gates, Bill. “Gates memo: 'We can and must do better'”, cnet news. http://news.cnet.com/Gates-memo-We-can-and-must-do-better/2009-1001_3-817210.html?tag=mncol;txt; Internet; accessed 2 March 2009.

Global Security. “Global Information Grid (GIG) Bandwidth Expansion (GIG-BE)”. http://www.globalsecurity.org/space/systems/gig-be.htm; Internet; accessed 16 April 2009.

Government of Ontario. Emergency Management Ontario. "Emergency Response Plan 2008." http://www.emergencymanagementontario.ca/stellent/idcplg/webdav/Contribution%20Folders/emo/documents/PERP%20Final%20March%202008.pdf; Internet; accessed 11 March 2009.

Greylogic. Project Grey Goose: Phase I Report. "Russia/Georgia Cyber War – Findings and Analysis", 17 October 2008. http://d.scribd.com/docs/2i7t2qyiwv0g63e7l3g.pdf; Internet; accessed 1 April 2009.

———. "Grey Goose Report Phase II Report: The evolving state of cyber warefare.", 21 March 2009. http://greylogic.us/?page_id=85; Internet; accessed 1 April 2009.

Hejazi, Wallid and Allan Lefort. *2008 Rotman-TELUS Joint Study on Canadian IT Security Practices*, 2008.

Huges, Rex B. "NATO and Cyber Defence: Mission Accomplished?" 2009. http://www.atlcom.nl/site/english/nieuws/wp-content/Hughes.pdf; Internet; accessed 8 April 2009.

ICANN. "ICANN Strategic Plan July 2008 – June 2011." http://www.icann.org/en/strategic-plan/strategic-plan-2008-2011.pdf; Internet; accessed 20 March 2009.

Independent Electricity System Operator. *Forum*. "Enabling Tomorrow's Electricity System: Report of the Ontario Smart Grid Forum", http://www.ieso.ca/imoweb/pubs/smart_grid/Smart_Grid_Forum-Report.pdf; Internet; accessed 18 February 2009.

Information Warfare Monitor. http://www.infowar-monitor.net/index.php

Intelfusion. "British Intelligence Warns British Telecom about its Huawei Equipment." http://intelfusion.net/wordpress/?p=558; Internet; accessed 1 April 2009.

———. "Project Grey Goose Phase III: Open call for volunteers." http://intelfusion.net/wordpress/?p=555; Internet; accessed 1 April 2009.

———. "Russia's Chechen Model for its Georgia Cyber Attack" http://intelfusion.net/wordpress/?p=392; Internet; accessed 1 April 2009.

International Telecommunication Union. "Creating trust in critical network infrastructures: Canadian Case Study", 20 May 2002. http://www.itu.int/osg/spu/ni/security/docs/cni.07.pdf; Internet; accessed 12 March 2009.

———. "Working with IMPACT to secure the global information society." *Global Cybersecurity Agenda*. http://www.itu.int/osg/csd/cybersecurity/gca/impact/response.html; Internet; accessed 18 April 2009.

Internet Business Law Services, “Internet Law - NATO Agrees to Create Cyber Defence Management Authority”, 15 May 2008. http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=2054; Internet; accessed 19 February 2009.

Janczewski, Lech, Andrew M. Colarik, and Inc Books24x7. *Cyber Warfare and Cyber Terrorism*. Hershey, PA: Information Science Reference, 2008.

Keizer, Gregg. “ActiveX bugs pose threat to Vista, Microsoft reports”, *IT World.* 3 November 2008. http://www.itworld.com/windows/57174/activex-bugs-pose-threat-vista-microsoft-reports; Internet; accessed 16 April 2009.

Kleinrock, Leonard. “Information Flow in Large Communication Nets”, http://www.lk.cs.ucla.edu/LK/Bib/REPORT/PhD/; Internet; accessed 3 March 2009.

Klensin, Dr. John C. Biography. http://www.icann.org/en/biog/klensin.htm; Internet; accessed 20 March 2009.

———. “Internet Governance” Address by John Klensin to the opening of the IGF http://www.isoc.org/pubpolpillar/governance/igf-rio_speech_klensin.shtml; Internet; acccessed 3 March 2009.

Knight, G. Scott and C. Daicos. "Concerning Enterprise Network Vulnerability to HTTP Tunnelling." Athens, May 2003.

Knight, G. Scott and Ron Smith. "Applying Electronic Warfare Solutions to Network Security." *Canadian Military Journal* 6, no. No. 3 (Autumn 2005).

Kohl, Uta. “The Rule of Law, Jurisdiction and the Internet”. *International Journal of Law and Technology*, Vol 12, No. 3, 2004.

Lackenbauer, P. Whitney. "Arctic Front, Arctic Homeland: Re-Evaluating Canada’s Past Record and Future Prospects in the Circumpolar North."Toronto, www.canadianinternationalcouncil.org; Internet; accessed 30 October 2008.

LaMar, Jost. Torts. http://www.wyolaw.org/Outlines/LaMar%20Jost%20(2002)/lamar_jost_torts_ii.PDF; Internet; accessed 18 April 2009.

Lawson, Stephen. “Outage knocks BlackBerry users offline”. *Inforworld.com*, 11 February 2008. http://www.infoworld.com/article/08/02/11/Outage-knocks-BlackBerry-users-offline_1.html; Internet; accessed 27 February 2009.

Leblanc, Sylvain, and Knight, Scott, “Engaging the Adversary as a Viable Response to Network Intrusion”, Workshop on Cyber Infrastructure Emergency Preparedness Aspects, Ottawa, 21-22 April 2005; http://tarpit.rmc.ca/knight/papers/IO%20Counter-measures.doc; Internet; accessed 20 January 2009.

———. "Choice of Force - Special Operations for Canada". Chapter 11: Information Operations in Support of Special Operations. D. Last and B. Horn eds., McGill-Queen's University Press, Montreal, 173-185 (2005). http://tarpit.rmc.ca/leblanc/publications/Leblanc_Knight-IO_in_Support_of_SO.pdf; Internet; accessed 20 January 2009.

Leder, Felix and Werner, Tillmann. "Know Your Enemy: Containing Conficker. To Tame A Malware", *The Honeypot Project.* http://www.honeynet.org/files/KYE-Conficker.pdf; Internet; accessed 18 April 2009.

Lemos, Robert. "U.S. military flags China cyber threat", *Security Focus.* http://www.securityfocus.com/brief/696; Internet; accessed 8 April 2009.

Libicki, Martin C. and Rand Corporation. *Conquest in Cyberspace : National Security and Information Warfare*. Cambridge: Cambridge University Press, 2007.

MacLeod, Ian. "State of emergency: Canada lacks plan to protect critical infrastructure", *Ottawa Citizen*, April 11th, 2008. http://www2.canada.com/ottawacitizen/news/story.html?id=8b1489a0-2dc5-4a79-900f-154e5d51bc33&k=97522; Internet; accessed 17 March 2009.

Manley, John, P.C., *Independent Panel on Canada's Future Role in Afghanistan.* http://dsp-psd.tpsgc.gc.ca/collection_2008/dfait-maeci/FR5-20-1-2008E.pdf; Internet; accessed 20 March 2009.

Marquis, S., Dean, T., and Knight, S. "SCL: A Language for Security Testing of Network Applications", CASCON '05 (IBM Centers for Advanced Studies Conference), Toronto, October 2005. http://tarpit.rmc.ca/knight/papers/SCL.pdf; Internet; accessed 20 January 2009.

McAllister, Andrew. "Some of OCIPEP's Cyber Security Activities." http://afceaottawa.ca/uploads/JunReport2003.pdf; Internet; accessed 12 March 2009.

McCullagh, Declan. Pressuring ISPs for 2 year data retention, *CNet.com*, published 20 February 2009. http://edition.cnn.com/2009/TECH/02/20/internet.records.bill/index.html; Internet; accessed 18 March 2009.

McDermott, Thomas. "Security Considerations for Avaya ESS Implementation." *SANS Infosec Reading Room.* http://www.sans.org/reading_room/whitepapers/voip/security_considerations_for_avaya_ess_implementation_32984; Internet; accessed 25 February 2009.

Mclean, Jesse and Cooper, Alex. "Glitch bares Ryerson students' information." *TheStar.com*, 24 February 2009. http://www.thestar.com/News/GTA/article/592063; Internet; accessed 24 February 2009.

McMahon, David. "Proactive Cyber Defence - Forecasting the Perfect Storm." 23 November 2008.

Michigan Department of State. “Information for TJ Maxx Customers”. http://www.michigan.gov/sos/0,1607,7-127-1640_9150-165939--,00.html; Internet; accessed 8 April 2009.

Microsoft Corporation. “Microsoft Security Bulletin MS08-067”, published: 23 October 2008. http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx; Internet; accessed 2 April 2009.

———. “Written Direct Testimony of Jim Allchin.”, 3 May 2002. http://www.microsoft.com/presspass/legal/allchin.mspx; Internet; accessed 8 April 2009.

Mills, Elinor. “Microsoft to give partners heads-up on security vulnerabilities.” *Cnet.com*, 5 August 2008. http://news.cnet.com/8301-1009_3-10006325-83.html?tag=txt; Internet; accessed 8 April 2009.

Municipal Information Systems Association. “MISA/ASIM Canada Launched in Ottawa.”http://www.misa-asim.ca/en/news/Launched.html; Internet; accessed 21 April 2009.

Munk Centre, University of Toronto. Citizen Lab Press Conference. Posted 31 March 2009. http://hosting.epresence.tv/MUNK/1/watch/104.aspx; Internet; accessed 1 April 2009.

N-Dimension Solutions Inc. “Cyber Security and the Smart Grid.” http://www.ieso.ca/imoweb/pubs/smart_grid/N-Dimension.pdf; Internet; accessed 18 February 2009.

Nabati, Mikael. “International Law at a Crossroad: Self-Defense, Global Terrorism, and Preemption (A Call to Rethink the Sefl-Defense Normative Framework)”, *Transnational Law & Contemporary Problems*, Vol. 13, 2003.

National Infrastructure Security Co-ordination Centre. “Botnets – The Threat to the Critical National Infrastructure”. 17 October 2005. http://www.cpni.gov.uk/Docs/botnet_11a.pdf; Internet; accessed 11 March 2009.

National Science Foundation. “Scientists Use the ‘Dark Web’ to Snag Extremists and Terrorists Online.” http://www.nsf.gov/news/news_summ.jsp?cntn_id=110040; Internet; accessed 18 February 2009.

New York Times. “Vast Spy System Loots Computers in 103 Countries”, 28 March 2009. http://www.nytimes.com/2009/03/29/technology/29spy.html?pagewanted=2&_r=1; Internet; accessed 6 April 2009.

Newman, M.E.J. "The Structure and Function of Complex Networks." *SIAM Review*, Vol.45, No. 2, pp. 167-256, 2003. http://www.santafe.edu/files/gems/paleofoodwebs/Newman2003SIAM.pdf; Internet; accessed 10 March 2009.

NORAD Agreement. http://www.treaty-accord.gc.ca/ViewTreaty.asp?Treaty_ID=105060; Internet; accessed 18 April 2009.

North Atlantic Treaty Organization. *The North Atlantic Treaty*, Washington D.C. – 4 April 1949. http://www.nato.int/docu/basictxt/treaty.htm; Internet; accessed 2 March 2009.

———. "NATO Opens New Centre of Excellence on Cyber Defence". www.nato.in/docu/update/2008/05-may/e0514a.html; Internet; accessed 15 April 2009.

——. "NATO Glossary of Terms and Definitions", *AAP-6*. http://www.nato.int/docu/stanag/aap006/aap-6-2008.pdf; Internet; accessed 2 October 2008.

——. CCDCOE. Cyber Attacks Against Georgia: Legal Lessons Identified, Tallin, Estonia, version 1.0 dated November 2008. http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf; Internet; accessed 8 April 2009.

——. "NATO Cooperative Cyber Defence (CCD) Centre of Excellence (COE)." (Tallin, Estonnia). http://www.ccdcoe.org/; Internet; accessed 1 April 2009. http://transnet.act.nato.int/WISE/TNCC/CentresofE/CCD; Internet; accessed 1 April 2009. http://www.nato.int/docu/update/2008/05-may/e0514a.html; Internet; accessed 1 April 2009.

——. Parliamentary Assembly. "NATO and Cyber Defence" 027 DSCFC 09 E (Draft Report), *Sub-Committee on Future Security and Defence Capabilities*. 12 March 2009. http://www.nato-pa.int/default.Asp?SHORTCUT=1782; Internet; accessed 8 April 2009.

Neasmith, Colonel David, "Computer Network Operations Consideration for DND/CF Requirements." AFCEA Presenation dated 11 January 2005; available at: http://www.afceaottawa.ca/uploads/CNO%20Briefing%2011Jan05.ppt; Internet; accessed 7 April 2009.

Radcliffe, Jerome. "CyberLaw 101: A primer on US laws related to honeypot deployments." *SANS Institute InfosecReading Room*, 1 February 2007. http://www.sans.org/reading_room/whitepapers/legal/cyberlaw_101_a_primer_on_us_laws_related_to_honeypot_deployments_1746; Internet; accessed 8 April 2009.

RCMP Tech Crime Unit Website http://www.rcmp-grc.gc.ca/fs-fd/tcrime-crimet-eng.htm; Internet; accessed 11 March 2009.

Richter, Chris. “Pre-emptive Self-Defence, International Law and US Policy”. *Dialogue* (2003). http://www.polsis.uq.edu.au/dialogue/vol-1-2-6.pdf; Internet; accessed 19 March 2009.

Rosenberg, Barry. “Cyber warriors”. C4ISR Journal of Net-centric Warfare, Vol. 6, No. 7, 1 August 2007. http://www.isrjournal.com/story.php?F=2859662; Internet ; accessed 16 February 2009.

Sachoff, Mike. “Man Convicted In Estonia Cyber Attack.” Webpronews.com, 24 January 2008 http://www.webpronews.com/topnews/2008/01/24/man-convicted-in-estonia-cyber-attack; Internet; accessed 1 April 2009.

Schmidtchen, David. *The Rise of the Strategic Private: Technology, Control and Change in a Network Enabled Military,* 2006.

Schmitt, Michael N. "Computer Network Attack and the use of Force in International Law: Thoughts on a Normative Framework." *Columbia Journal of Transnational Law* 37, (1998-1999).

Shulman, Mark R. "Discrimination in the Laws of Information Warfare." *Columbia Journal of Transnational Law* 37, (1998-1999).

Simmons, Donna. “Laws of Canada as they Pertain to Computer Crime.” *SANS Institute InfosecReading Room*, May 2002. http://www.sans.org/reading_room/whitepapers/legal/laws_of_canada_as_they_pertain_to_computer_crime_673; Internet; accessed 8 April 2009.

Slashdot, “FBI Concerned About Implications of Counterfeit Cisco Gear”. *SlashDot*, 22 April 2008. http://hardware.slashdot.org/article.pl?sid=08/04/22/1317212; Internet; accessed 2 March 2009.

Solce, Natasha. "The Battlefield of Cyberspace: The Inevitable New Military Branch - the Cyber Force." *Albany Law Journal of Science and Technology* 18, no. 1 (2008).

Spring, Baker and Eaglen. Mackenzie. “Quarterly Defense Review (QDR): Building Blocks for National Defense.” *The Heritage Foundation,* 28 January 2009. http://www.heritage.org/research/nationalsecurity/bg2234.cfm; Internet; accessed 29 March 2009.

Stapelberg, Dr. Rudolph Frederick. “Infrastructure Systems Interdependencies and Risk Informed Decision Making (RIDM): Impact Scenario Analysis of Infrastructure Risks Induced by Natural, Technological and Intentional Hazards.” Griffith University. http://www.iiisci.org/journal/CV$/sci/pdfs/R105SQ.pdf; Internet; accessed 6 March 2009.

Stewart, Keith. DRDC Toronto. “Influence Operations: Historical and Contemporary Dimensions”, DRDC Toronto CR-2007-126, 31 July 2007. http://cradpdf.drdc.gc.ca/PDFS/unc69/p528894.pdf; Internet; accessed 15 April 2009.

Symantec. *Symantec Internet Security Threat Report Trends* for July–December 07, Volume XIII, Published April 2008.

The White House. *The National Strategy to Secure Cyberspace*. Washington D.C.: 2003.

Thomas, Timothy L. "China's Electronic Long-Range Reconnaissance." *Military Review*, Nov-Dec, 2008. http://findarticles.com/p/articles/mi_m0PBZ/is_6_88/ai_n31140190/; Internet; accessed 1 April 2009.

United Nations. Chapter VII: Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression, Article 42. *Charter of the United Nations*. 1948. http://www.un.org/aboutun/charter/chapter7.shtml; Internet; accessed 18 March 2009.

———. Chapter VII: Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression, Article 51. *Charter of the United Nations*, 1948. http://www.un.org/aboutun/charter/chapter7.shtml; Internet; accessed 18 March 2009.

———. *Protocol I to the Geneva Conventions*, 8 June 1977. Article 43, para 2. http://www.icrc.org/ihl.nsf/FULL/470?OpenDocument; Internet; accessed 19 April 2009.

United States Air Force. "USAF Fact Sheet Cyberspace 101 Understanding the cyberspace domain." http://www.afcyber.af.mil/library/factsheets/factsheet.asp?id=10784; Internet; accessed 16 February 2009.

United States. Air Force Association. "Victory in Cyberspace.", October 2007. http://www.afa.org/media/reports/victorycyberspace.pdf; Internet; accessed 1 April 2009.

United States. Department of Defense. DoD Instruction 8100.1 "Global Information Grid (GIG) Overarching Policy." http://biotech.law.lsu.edu/blaw/dodd/corres/pdf/d81001_091902/d81001p.pdf; Internet; accessed 16 April 2009.

———. Department of Defense. DoD Instruction 8100.3, Department of Defense Voice Networks. http://www.dtic.mil/whs/directives/corres/pdf/810003p.pdf; Internet; accessed 16 April 2009.

———. *Joint Targeting*. JP 3-60, 13 April 2007, Appendix E-1. http://www.dtic.mil/doctrine/jel/new_pubs/jp3_60.pdf; Internet; accessed 20 March 2009.

United States. Defense Information Systems Agency (DISA). "Voice Networks Infromation Assurance Test Plan (IATP)version 3.1." 1 March 2005. http://www.disa.mil/dsn/webfiles/DISA_Information_Assurance_Test_Plan_(IATP)v3_1March_2005.pdf; Internet; accessed 16 April 2009.

———. Defense Information Systems Agency (DISA). "IPv6 for the GSCR." http://jitc.fhu.disa.mil/tssi/docs/1_7ipv6_approved6089r6104.pdf; Internet; accessed 16 April 2009.

United States. Executive Office of the President. "Agencies Reduce Security Vulnerabilities Under the Trusted Internet Connection Initiative." http://georgewbush-whitehouse.archives.gov/omb/pubpress/2008/071008_tic.html Released July 10th, 2008. Internet; accessed 17 March 2009.

United States Department of Defense. Secretary of Defense. "National Military Strategy for Cyberspace Operations (NMS-CO)", 11 December 2005. http://www.dod.mil/pubs/foi/ojcs/07-F-2105doc1.pdf; Internet; accessed 29 Mar 2009.

Vamosi, Robert. "World Bank under cyberattack?", *Cnet news*, 10 October 2008. http://news.cnet.com/8301-1009_3-10063522-83.html; Internet; accessed 8 April 2009.

ViruSCAN.org, "Scanning Program Results for: GhOst Rat.exe." http://www.virscan.org/report/7f946853ab104508dbd84330eaef5d2c.html; Internet; accessed 1 April 2009.

What-is-what.com. "What is a Zero Day Exploit?" http://what-is-what.com/what_is/zero_day_exploit.html; Internet; accessed 20 March 2009.

White, Orrick. "Understanding the Human Dimension in 21st CenturyConflict/Warfare: The Complexities of Human-with-HumanRelationships." DRDC Corporate TR 2008-004, August 2008. http://pubs.drdc.gc.ca/inbasket/owhite.080826_0858.p529860.pdf; Internet; accessed 3 March 2009.

Wilson, Tim. "USB Hacksaw Still Sharp, Expert says". *DarkReading*. 29 April 2008. http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml?articleID=211201471; Internet; accessed 16 April 2009.

World Technology Grid. http://www.worldcommunitygrid.org/ ; Internet; accessed 2 March 2009.

Yourdon, Ed. Y2K success lessons. *Computer World*. http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=Default&articleId=40853&taxonomyId=0&pageNumber=1; Internet; accessed 8 April 2009.

Zembek, Richard, S. "Jurisdiction and the Internet: Fundamental Fairness in the Networked World of Cyberspace", *Albany Law Journal of Science and Technology*, Vol. 6, 1996.

Zittrain, Jonathan. "Internet Points of Control", Research Publication No. 2003-01, March 2003. http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2003-01.pdf; Internet; accessed 20 April 2009.