CANADIAN FORCES COLLEGE 2009 – 2010

NATIONAL SECURITY PROGRAMME – 2

MPA 500 DIRECTED RESEARCH PAPER

"A JOB FOR THE TROOPS, THE COPS OR THE SPOOKS: Canada's Cyber-Security Challenge"

By / par Chris McMillan

21 May 2010

This paper was written by a student attending the Canadian Forces College in Fulfillment of one of the requirements of the Course of Studies. The paper is a scholastic document, and thus contains facts and opinions, which the author alone considered appropriate and correct for the subject. It does not necessarily reflect the policy or the opinion of any agency, including the Government of Canada and the Canadian Department of National Defence. This paper may not be released, quoted or copied except with the express permission of the Canadian Department of National Defence.	*La présente étude a été rédigée par un stagiaire du Collège des Forces canadiennes pour satisfaire à l'une des exigences du cours. L'étude est un document qui se rapporte au cours et contient donc des faits et des opinions que seul l'auteur considère appropriés et convenables au sujet. Elle ne reflète pas nécessairement la politique ou l'opinion d'un organisme quelconque, y compris le gouvernement du Canada et le ministère de la Défense nationale du Canada. Il est défendu de diffuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense nationale.*

Table of Contents

List of Figures

Abstract

This paper addresses several related questions: to what degree is cybersecurity a serious problem for the government of Canada; to what extent is Canada adequately prepared to meet this cybersecurity challenge; and, what if anything should the government of Canada do about it? It will test the hypothesis that addressing the threat to Canadian national security in the cyberspace domain is a serious security challenge for which Canada is not yet adequately prepared.

The manner in which cybersecurity challenges are currently being addressed in Canada is examined, in terms of which stakeholder groups or organizations have been given the authority and the means for assuming responsibility for aspects of Cybersecurity. The question of whether or not these organizations are adequately empowered and equipped, either individually or collectively, to carry out their responsibilities is then explored.

It is argued that the novelty and severity of the challenge is such that it warrants substantial institutional change at both the national and international levels. In particular it is argued that the government of Canada should create and empower a major new national organization which is dedicated to ensuring that the Canadian government, Canadian citizens and the Canadian corporate private sector are all working together under an integrated national regime (ultimately part of an international regime) to provided adequate cybersecurity for Canadians.

1 Introduction

Imagine a day, or a week, without the Internet.

Now imagine a month or a year without the Internet.

The first thought may seem like a vacation. The second would be something very different. Some can reach back into their memory to do this. For them the thought, though perhaps unsettling, would not be shocking. For others, who have grown to depend on the Internet, the thought could be quite frightening, and for those who have grown up with the Internet, the thought could be almost unimaginable. As this paper hopes to demonstrate, the reality of losing the Internet, on a national scale, would be even much more disruptive than most imagine.

The questions that this paper will address are: to what degree is cybersecurity a serious problem for the government of Canada; to what extent is Canada adequately prepared to meet this cybersecurity challenge; and, what if anything should the government of Canada do about it? The hypothesis will be that addressing the threat to Canadian national security in the cyberspace domain is a serious security challenge for which Canada is not yet adequately prepared. It will be argued that the novelty and severity of the challenge is such that it warrants legislative action and substantial institutional change at both the national and international levels. In particular it will be argued that the government of Canada should take a leadership role in creating and empowering a major new national organization which is dedicated to ensuring that the Canadian government, Canadian citizens and the Canadian corporate private sector are all working together under an integrated national regime (ultimately part of an international regime) to provided adequate cybersecurity for Canadians. The government of Canada should also engage the international community in a very serious discussion of multi-lateral measures that will ultimately be needed.

First we should clarify the hypothesis by agreeing on some basic definitions. For example cyberspace is a fairly recent addition to the English language[1] and an even more recent addition to the military lexicon. According to a recent NATO Advanced Research Workshop on Cyberwar-Netwar[2], the word cyberspace first appeared in a Joint Publication in 2001 (in JP 1-02) where it was defined as "the environment in which digitized information is communicated over computer networks". It has since been updated (as of 18 Dec 2009) to read:

> A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[3]

While we are not only concerned here with the military perspective, this NATO definition, as far as it goes, seems quite adequate for general use. From this definition, one could deduce that the most important aspects of cyberspace are the information and the connectivity that it provides. Many users today would probably find this definition inadequate however, because it fails to convey the many social uses that are made of the Internet. The sociologist Manuel Castells for example, while he doesn't use the term cyberspace, has certainly described in detail the profound impact that it is having on our society, which goes well beyond what one would imagine from the rather sterile definition above, and is in fact leading to "the emergence of a new social structure", which he call Informationalism.[4] No doubt the "official" definition of cyberspace will continue to evolve along with the manner in which it is used.

The next question is what is meant by "cyber security". The same on-line dictionary provides a useful definition of security: "A condition that results from the

[1] The term actually originates from the science fiction writer William Gibson. See: William Gibson, "Burning Chrome", in *OMNI*, July 1982.

[2] Ferdinand Duarte Carvalho and Eduardo Mateus da Silva editors, *Cyberwar-Netwar, Security in the Information Age*, NATO Security through Science Series, IOS Press, Amsterdam, Netherlands, 2006. (3)

[3] Joint Publication 1-02 Department of Defence Dictionary of Military and Associated Terms, http://www.dtic.mil/doctrine/dod_dictionary/, Internet, accessed 29 March 2010.

[4] Manuel Castells, *The Information Age: Economy, Society & Culture, Volume I: The Rise of the Network Society* (Malden, MA: Blackwell Publishing, 2000), 26.

establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences."[5] This may seem clear when applied to personal security, or even to a particular state's security, provided that state has a clear and uncontestable sense of what would constitute a hostile act or influence, as defined for example by its laws and customs. However, as Arnold Wolfers explored in his article: *National Security as an Ambiguous Symbol*, there are important nuances to this issue, such as who defines what is in need of securing (what exactly is in the national interest), and the character and extent of security measures that would be appropriate. He defines security, not as a binary quality that either exists or doesn't, but a quantity which, "in an objectives sense, measures the absence of threats to acquired values, in a subjective sense, the absence of fear that such values will be attacked." [6] Specifically he concludes "that normative admonitions to conduct a foreign policy guided by national security interests … to be meaningful ... would have to specify the degree of security which a nation shall aspire to attain and the means by which it is to be attained in a given situation."[7] He further warns against simplistic solutions, such as the total reliance on either coercive power (hard power) or "moralism" (soft power) alone.

In the case of cyberspace however, which is transnational in nature, the situation is even less clear for a number of reasons. Firstly because cyberspace, in a very real sense, is a shared resource that no country owns and is not divisible, and secondly because behaviour in cyberspace that is legal and acceptable according to one country may not be so in the view of another. From Canada's perspective, a clearer understanding in this context will only come after examination of the vulnerabilities and threats in cyberspace, which is the subject of the following section and chapter respectively.

[5] Joint Publication 1-02 Department of Defence Dictionary of Military and Associated Terms, http://www.dtic.mil/doctrine/dod_dictionary/, Internet, accessed 29 March 2010.

[6] Arnold Wolfers, "National Security as an Ambiguous Symbol", *Political Science Quarterly*, Vol. 67, No. 4. (Dec., 1952), pp. 481-502, 485. http://www.google.ca/url?sa=t&source=web&ct=res&cd=1&ved=0CAYQFjAA&url=http%3A%2F%2Finstituty.fsv.cuni.cz%2F~plech%2FWolfers_BS.pdf&ei=qA_PS4C1JsGBlAexgNmhCw&usg=AFQjCNE6TEnly-UNGJ9YJS9tMqhqGBRwPQ; Internet, accessed 25 April 2010.

[7] Ibid. 502.

We should also be clear in specifying which aspects of cybersecurity this paper will focus on. The most recent national security policy document, *Policy on Government Security*[8], published by the Treasury Board and in effect since 1 July 2009, calls upon government departments to manage their security requirements by continuously assessing risks and implementing, monitoring and maintaining appropriate internal management controls involving:

1. Prevention (mitigation),
2. Detection,
3. Response and
4. Recovery.

This is essentially identical to the four 'pillars' of Information Technology Security that are described in the *Government Security Policy*[9] of the Chrétien government in 2002 and this is also quite similar to the components of an integrated security system as described by the Martin government in 2004, in *Securing an Open Society: Canada's National Security Policy*[10]:

1. Threat Assessment
2. Protection and Prevention
3. Consequence Management
4. Evaluation and Oversight

While the 2009 and 2002 policy documents are focussed solely on the security of government information and services, the 2004 policy document covers the much broader national security requirements. It is interesting to compare these Canadian government objectives to the American equivalents: when the White House announced the creation of a "Chief of Cybersecurity" in 2009, it was stated that the purpose was to coordinate and harmonize the US efforts to:

1. Deter,

[8] Canada: *Policy on Government Security*, http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578&section=text; Internet; accessed 15 January 2010.

[9] 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 27 March 2010.

[10] Canada: *Securing an Open Society: Canada's National Security Policy*; April 2004, (10).

2. Prevent,
3. Detect and
4. Defend

against cyberattacks[11]. The significant difference here is the first objective, which is perhaps more in character for a superpower such as the US than it is for Canada, but it does highlight another important aspect that should not be ignored.

For the purpose of this paper, the focus will be on the manner in which all of these aspects of cybersecurity are currently being addressed in Canada. This will be described in terms of which stakeholder groups or organizations have been given the authority and the means for assuming responsibility for aspects of Cybersecurity. This paper will examine the question of whether or not these organizations are adequately empowered and equipped, either individually or collectively, to carry out their responsibilities, and whether the sum of these responsibilities actually adds up to cyber-security for Canadians. The argument will be that the answer to both questions is no.

Attention will then turn to the question of how to remedy the situation. The options will be discussed and a case made for the creation of a new entity with new authorities to provide the needed capability.

In order to support this hypothesis (that addressing the threat to Canadian cybersecurity is a serious challenge for which Canada is not yet adequately prepared), this paper will start with a brief background on the origins and history of cybercrime and cyber terrorism and then provide ample evidence of Canada's vulnerability to them, based on our increasing dependence upon cyberspace.

Chapter two will provide detailed evidence of the seriousness of the various threats to Canada's cybersecurity, describing the scale and the impact of these threats, and will argue that to date we have not been sufficiently successful in dealing with them.

[11] John Markoff. "Obama to Name Chief of Cybersecurity", *New York Times*, 22 December 2009, http://www.nytimes.com/2009/12/22/technology/internet/22cyber.html; Internet, accessed 15 April 2010.

Here we will also provide a brief, non-technical discussion of the various types of threats in cyberspace, and the types of measures that are required to defend against them. This will be needed to understand the challenges that we face in providing cyber security.

Chapter three will explain several dilemmas that confront us in cyberspace, to further our understanding of the difficulty in defending against these threats: their technical nature and relatively recent emergence, and the fact that the historical organization and jurisdictional authorities of our existing institutions, both national and international, are no longer appropriate for providing security in cyberspace.

Chapter four will describe the current Canadian efforts to defend against these threats, in terms of the responsibilities and capabilities of the various stakeholders, including the various federal government agencies and departments, non-federal government organizations, private corporate sector stakeholders and private citizens. It will be evident then, that these stakeholders are currently unable, either individually or collectively, to provide national cybersecurity for Canada.

Chapter five will briefly broaden the discussion to the international realm, where the ultimate solution must lie. Here we summarize the approaches being taken by our two largest and closest allies, the US and the UK, and discuss the current status of the very important efforts in the multi-lateral sphere.

Chapter six will critically examine some options available for providing this security. It will be argued that the current approach is inadequate and that a more fundamental reorganization will be needed. A recommendation for a way ahead will be provided, that includes an urgent call for the creation of new institutions with new authorities and powers to ensure that Canada is provided with an integrated and coherent security solution.

Finally this will be summarized in the conclusion.

1.1 Origins, history

Crime and terrorism, as explained by Phil Williams[12] are simply the continuation of business and politics by criminal means or through the use of indiscriminate violence (respectively). When the technology of the Internet opened up new avenues of opportunity for business and politics to be conducted, it should not be surprising that organized crime and terrorists followed suit. This is simply another unfortunate side-effect of the globalization that technology is driving.

It certainly didn't take long for criminal elements to take advantage of new opportunities that arose with the advent of computers and networks of computers. The digital "revolution" that originated in the late 1940's began to see widespread application in the 1970's with the development of integrated circuit technology. This led to its commercial and government adoption, which created digital databases containing valuable information of a personal, financial, commercial or military nature. The ease and rapidity with which these databases could be accessed, modified and transmitted is both an asset and a vulnerability. This ability to economically process and move information, which is of such a great benefit to legitimate users, unfortunately also provided the same benefit to ill-intentioned abusers. Computer crime has existed since those early days, with one of the earliest publications on computer crime appearing in 1976 by Parker[13], which discussed the potentiality of cybercrime well before the birth of the Internet, and warns that "our society is fast becoming dependent on the correct, reliable, and near instantaneous operation by electronic data processing (EDP) personnel of digital computers and data telecommunications". In fact Parker claims to have been aware of this problem since "the mid-1960s" and cites an example of a 1966 incident of a "Computer Expert Accused of Fixing His Bank Account".[14] Parker described the fairly broad range of computer crime that existed in 1976, and accurately predicted that "The pervasive penetration of computers and data communications into the functioning of

[12] Phil Williams. "Strategy for a New World: Combating Terrorism and Transnational Organized Crime." In *Strategy in the Contemporary World*, edited by John Baylis et al. (New York: Oxford University Press, 2007), 192-218.

[13] Donn Parker, *Crime by Computer*. (New York: Charles Scribner and Sons, 1976).

[14] Ibid. x.

society is enough to justify predictions of a growing level of abuse associated with the use of information processing systems". However, he was far off the mark when he considered the future trends in computer crime and hypothesized that the incidence of computer crime would level off and begin to decrease before 2000[15]. Furthermore, nowhere in his lexicon was there any concept of networking, and all that that implies.

However cybercrime itself, as opposed to computer crime, has evolved to exploit the global reach and extreme interconnectedness of the Internet, rather than just the processing power and speed of a computer. This had to await the birth of cyberspace.

It was the development of wide-area-network (WAN) technology in the 1970's, the standardization of protocols (which led to the merger of all such networks into one "Internet"), together with the advent in the late 1980's of the affordable personal computer that led to the rapid expansion of the Internet in the mid-1990's. The original ARPAnet was designed in the 1970's to provide physically robust military communications. However its first widespread use was by scientific and academic users which then spread to commercial users and finally the general public in 1985[16]. This pervasive interconnectivity and the ability to rapidly access and share information over long distances are what give the Internet its unprecedented power. This power is what attracts criminal, terrorist and military interest. The fact that the Internet crosses national and international borders and jurisdictions, has led to the problems of transnational cybercrime as well as cyber-terrorism and cyberattack.

International relations however, are still largely being conducted on the basis of Westphalian sovereignty, as established in 1648, which is based on the two principles of "territoriality and the exclusion of external actors from domestic authority structures"[17]. As we shall see, neither of these principles can be easily applied to the new domain of

[15] Ibid. 293.

[16] James F. Dunnigan, *The Next War Zone: Confronting the Global Threat of Cyberterrorism*, (Kensington Publishing Corp., New York, NY, 2003), 54.

[17] Josef Joffe, "Rethinking the Nation-State: The Many Meanings of Sovereignty"; *Foreign Affairs*, November/December 1999, http://www.foreignaffairs.com/articles/55618/josef-joffe/rethinking-the-nation-state-the-many-meanings-of-sovereignty; Internet; accessed 15 February 2010.

cyberspace, which has greatly complicated efforts to deal with cyberattack (which henceforth will be used in a general sense to also include cybercrime and cyber-terrorism). In fact globalization in general has led some academics to speak of the "Westphalian cartographic illusion" and the emergence of new natural economic zones that don't correspond to state boundaries.[18]

1.2 Recognizing the Vulnerability

The global trend to exploit Information and Communication Technology (ICT) to increase efficiency and effectiveness is being adopted by most sectors of society in virtually all developed and developing nations of the world, including private and public, civil and military. As will be argued herein, this is leading to an ever increasing dependence on the reliable and secure access to a functioning cyberspace, for our economic, social and political well-being.

As the world continues to move to an information-based economy, an ever-increasing proportion of our national wealth and the wealth of other nations will be in the form of intellectual property (IP), which is saved electronically and is stored and moved in cyberspace. In fact a study was conducted by Purdue University's Center for Education and Research in Information Assurance and Security to estimate the loss of IP due to data theft and cybercrime in eight major countries including the US, UK, Japan, Germany and China. By interviewing 800 CIOs, this study estimated that these countries had lost a combined $4.6 billion worth of intellectual property in 2008. Based on these numbers, McAfee Inc. Research was able to project that the worldwide loss of IP by companies was more than $1 trillion that year alone.[19]

[18] Kenichi Ohmae, "The End of the Nation State: The Rise of Regional Economies", New York: Free Press, 1995.

[19] Public Safety Canada web site. http://www.publicsafety.gc.ca/prg/em/cbr/csb-eng.aspx; Internet; accessed 18 March 2010.

Voice, data and video communications are increasingly being carried over the Internet. In fact, according to a leading market research organization[20], among the best performing industries of the last decade (based on accumulative revenue growth from 2000-2009) the top four industries were: Voice Over Internet Protocol (VoIP) Providers; Search Engines; eCommerce and Online Auctions; and Online Dating. Each one of these industries relies entirely on the Internet.

The culture and entertainment industry is going online. Populations are investing more of their working and leisure time in online activities, to the point where the impact of social networking has recently become a new area of sociological research.[21] The result is a "complex, fundamental transformation in the nature of community from groups to social networks."[22]

For efficiency, many physical plants are (or soon will be) also controlled electronically from a remote location, which requires the reliable use of cyberspace[23]. The use of SCADA (Supervisory Control And Data Acquisition) systems has become common place for manufacturing, power generation, fabrication, refining, water management, oil and gas pipeline flow control, electrical power distribution, traffic lights air traffic control, railways and so on. This technology is already in its "third generation", whereby the connections between the sensors, actuators and control are made over the Internet, which makes them vulnerable to cyber-attack[24]. According to the 2008 report from the US Congressional "Commission to Assess the Threat to the United States from Electromagnetic Pulse", *Critical National Infrastructures*:

[20] IBIS*World* press release. "Top 10 Industries of the Decade". http://www.ibisworld.com/pressrelease/pressrelease.aspx?prid=210; Internet; accessed 18 March 2010.

[21] See for example research areas of the Sociology Department at the University of Toronto, http://know.soc.utoronto.ca/index.php?option=com_content&task=view&id=42&Itemid=106; Internet; accessed 25 April 2010.

[22] Barry Wellman. "The Glocal Village: Internet and Community", *the arts* & science re*view* University of Toronto, Autumn 2004 Volume I, Number I, 29.

[23] US Department of Homeland Security, *The National Strategy to Secure Cyberspace*, February 2003, http://www.dhs.gov/files/publications/publication_0016.shtm; Internet; accessed 18 March 2010, (32).

[24] See basic information on Wikipedia at http://en.wikipedia.org/wiki/SCADA. Internet; accessed 18 March 2010.

> SCADAs have emerged as critical and growing elements of a quietly unfolding industrial revolution spurred by the computer age. The accelerating penetration of SCADA systems, along with their electronic cousins, digital control systems (DCS) and programmable logic controllers (PLC), as critical elements in every aspect of every critical infrastructure in the Nation, is both inevitable and inexorable. While conferring economic benefit and enormous new operational agility, the growing dependence of our infrastructures on these omnipresent control systems represents a new vector of vulnerability in the evolving digital age of the 21st century, such as cyber security.[25]

One familiar example of the growth in the use of SCADA is with the so-called "smart meters" that electrical power utilities are beginning to implement for residential customers. These allow remote control of household appliances and heating systems. In 2009 the European Commission conducted a study of the energy supply companies, which found that the energy industry was undergoing a profound change towards becoming an "intelligent utility". This study determined that 70% of the energy supply companies were either already deploying smart meters, were testing them, or were planning to do so in the next two years.[26] Naturally, any large scale unauthorized remote control of these types of systems, broadly distributed across the population, could be extremely dangerous.

Our financial and banking sector, a large and growing sector, relies heavily on the reliable and secure functioning of cyberspace. The retail sector is also moving into cyberspace and healthcare is starting to rely on it as well. Industries in general are becoming increasingly transnational and reliant on a secure and reliable transnational cyberspace for conducting their daily business. A recent Statistics Canada bulletin, analysing the 2007 *Survey of Electronic Commerce and Technology,* indicates that at that time 87% of Canadian private sector enterprises used the Internet, 41% had a web site, 49% purchased online, and 8% sold online, with a total value of online sales exceeding

[25] US Congressional Commission Report to Assess the Threat to the United States from Electromagnetic Pulse, *Critical National Infrastructures*, April 2008, http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf; Internet; accessed 18 March 2010.

[26] European Commission. *7th Synthesis Report of the Sectoral e-Business Watch (2010)*, http://www.ebusiness-watch.org/key_reports/synthesis_reports.htm; Internet; accessed 25 April 2010.

$58bn. What is more: all of these figures were consistently growing every year (starting at 2001).[27]

Cloud Computing is another recent trend that will be of increasing relevance to ICT users. This is the on-line provision, on a pay-as-you-go basis, of ICT services that are immediately scalable. The service provider would typically have a large number of geographically distributed computers and storage devices with high-bandwidth connectivity. The business model is that this allows customers to save on ICT capital costs by leasing capability on an as-needed basis. This paradigm introduces further dependence on cyberspace and introduces additional cyber-security vulnerabilities[28].

Government services are also increasingly being delivered over the Internet. In particular DND has virtually all of its information, tactical, operational and strategic, including sensitive intelligence information, stored in digital form and available on various computer networks (although not necessarily on "the Internet").[29] The conflicting needs to protect critical data while enabling wide access to it creates significant vulnerabilities, which is true in varying degrees to almost all organizations, whether in the public or private sector.

It seems clear, therefore, that significant vulnerabilities exist in both the private and the public sector. This is in spite of the fact that corporations are generally rather reluctant to disclose vulnerabilities, lest they adversely affect shareholder or customer confidence, and in spite of the fact that the government similarly will not wish to reveal any vulnerabilities that could attract the attention of potential criminal or terrorist elements. The protection of government secrets is, of course, one of the most serious

[27] Ben Veenhof and Larry McKeown, "New economy indicators" in *Innovation Analysis Bulletin — Vol. 11, no. 1 (June 2009)*, available from http://www.statcan.gc.ca/bsolc/olc-cel/olc-cel?lang=eng&catno=88-003-X200900110816; Internet; accessed 11 May 2010, 19.

[28] As detailed in the Information Security Briefing provided by the UK Government Centre for the Protection of National Infrastructure (CPNI), available online at http://www.cpni.gov.uk/Docs/cloud-computing-briefing.pdf.

[29] Cyber Operations Science and Technology (S&T) Strategy, draft V0.8, 15 October 2009.

security challenges that the government faces, and therefore many aspects of this problem are classified, which puts them beyond the scope of this paper.

The one common thread in all of these trends is that they are all accelerating. This should not be surprising since the root cause is the growing capability of ICT, which is being driven by Moore's Law (the exponential improvement in technology), which, unless there is some reversal, will eventually lead to an almost complete (and irreversible) dependence on cyberspace.[30] Consider for instance the fact that the current Internet standard (IPv4) can only support about four billion different addresses,[31] which will soon be exhausted by the number of computers and other devices that are being connected to the Internet. The new standard being introduced (IPv6) [32] will be able to support about 3.4×10^{38} addresses[33]. This means that the new "address space" will allow, or about one million devices per square nanometre over the entire surface of the earth (which is about 510 million square kilometres[34] $\approx 5 \times 10^{32}$ square nanometres). In other words there will be practically no limit to the number of nodes that the Internet will be able to support. This is important because, according to Metcalfe's Law[35], the value of a network increases rapidly as new nodes are added (in fact it increases as the square of the number of nodes, since this represents the number of different connections that can be made). In other words, if a single node is added to a network of a million nodes, it immediately becomes available to all million nodes. As the network becomes larger it becomes much more useful, and it will attract more connections, which makes it even more useful and the process snowballs. From a sociological perspective, Manuel Castells describes in detail how this has had and is having a profound impact on society, and leading to a new socio-economic order: Informationalism.[36]

[30] Ray Kurzweil, *The Singularity is Near*, (London: Penguin Books Ltd., 2005), 96.

[31] IPv4 uses 32 bits for the address, which allows $2^{32} \approx 4.3$ billion addresses.

[32] Internet Assigned Numbers Authority (IANA) website; http://www.iana.org/numbers/; Internet; accessed 23 April 2010.

[33] IPv6 uses 128 bits for the address, which allows $2^{128} \approx 3.4\times10^{38}$ addresses.

[34] CIA "The World Factbook"; https://www.cia.gov/library/publications/the-world-factbook/geos/xx.html; Internet; accessed 25 April 2010.

[35] Carl Shapiro and Hal R. Varian. *Information rules: a strategic guide to the network economy*, (Harvard Business School Press, 1999), 184.

[36] Manuel Castells, *The Information Age: Economy, Society & Culture, Volume I: The Rise of the Network Society, Second Edition*, (Malden, MA: Blackwell Publishing, 2000), 13-20.

What is critically important is to recognize the increasingly broad, deep and evolving reliance that our society has on the security, reliability and trustworthiness of cyberspace, not only for our economic prosperity, but for our safety and security, as well as our social, cultural and political lives. Cybersecurity can thus be interpreted as meaning the preservation, to the extent possible within our means, of these beneficial characteristics of cyberspace. To understand what measures must be taken to ensure this cybersecurity, it will be necessary to have some understanding of the threats that must be defended against. That is the subject of the next chapter.

Figure 1 below is a visual aid that attempts to illustrate, in a simplified way, the key vulnerabilities as well as the primary stakeholders and their relationships.

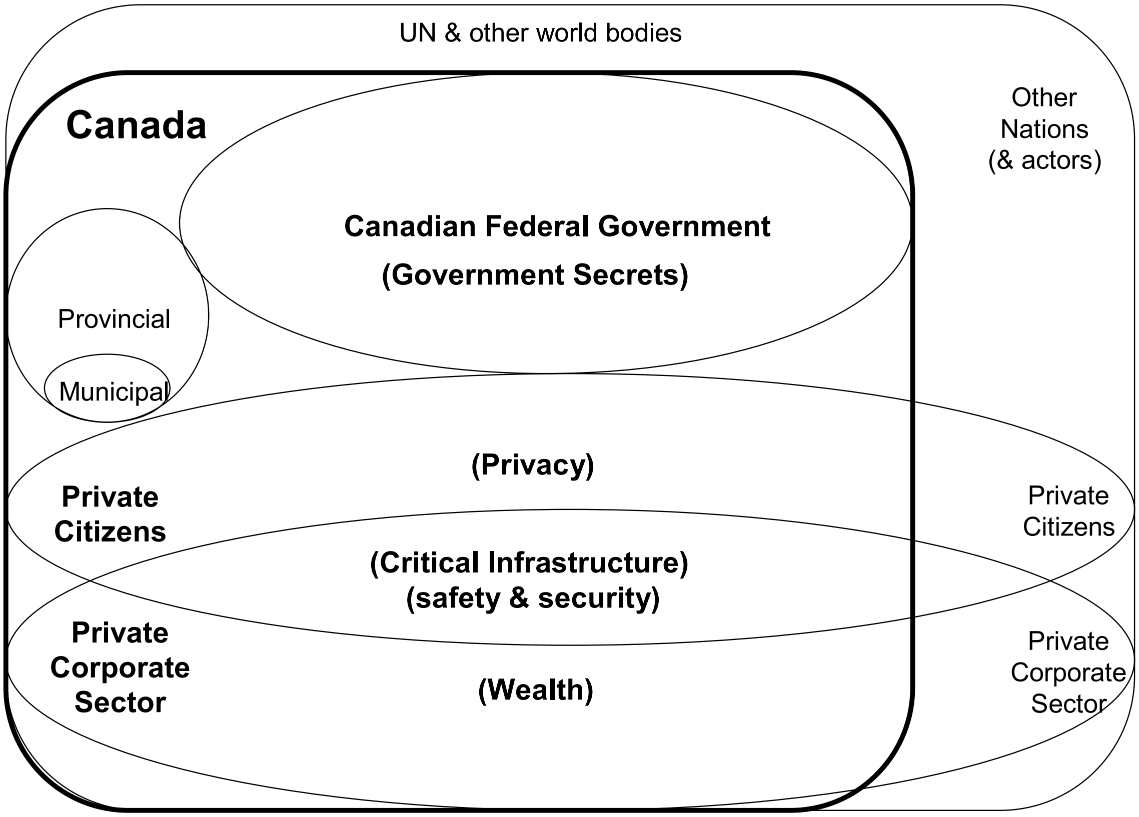


Figure 1. Primary Cyber Stakeholders & Concerns from a Canadian Perspective

This visualization will be repeated below with more detail, to include the threats and the actors engaged in defending against the threats. This is not meant to be taken literally as a strict taxonomy, but it does reflect the fact that the vast majority of the components of cyberspace are owned either by one of the levels of government, by a private corporate entity, or by a private citizen (some of whom are also business owners). For simplicity I have not included institutions or entities that fall outside of these categories, such as NGOs. The figure also represents the important fact that analogous stakeholders exist outside Canada. Finally it attempts to highlight (in parenthesis) a few of their key Cybersecurity concerns, which in most cases are actually shared by all. It must also be realized that many corporations are multi-national, many citizens have dual or multiple citizenship, and that there are world bodies such as the United Nations and other multi-national governance instruments.

2 The Threat to Cybersecurity

2.1 Recognizing the Threat

Ample evidence can be found to support the first part of the hypothesis: that cyber-security is a serious security challenge to Canada in particular, and internationally. For Canada this is reflected in official strategic level documents of the past and current Canadian governments, and has also been recognized by the Canadian police forces, the private sector, the media and academia.

Canada's most recent national security policy statement, *Securing an Open Society: Canada's National Security Policy,*[37] dates back to April 2004, and came from the previous government, however there has not been a major change in direction on this issue. This document lists eight current security threats, at least three of which have a cyber-security component: Foreign Espionage, Critical Infrastructure Vulnerability, and Organized Crime. However, the policy statement only recognizes the cyber dimension of

[37] *Securing an Open Society: Canada's National Security Policy,* (Ottawa: Privy Council Office, 2004).

Critical Infrastructure Vulnerability. Further, in terms of actual actions to be taken specifically to defend against cyber threats, this document only promises two modest measures, both of which are under "Emergency Planning and Management". They are:

- The Government will increase its capacity to predict and prevent cyber-security attacks against its networks.
- A national task force, with public and private representation, will be established to develop a National Cybersecurity Strategy.

The first measure only protects GoC networks, for which the responsibility and authority already existed within government, as will be described in chapter 3 below. The second was not accomplished before the Martin government fell, however the Harper government has just promised, in its 3 March 2010 Throne Speech, to finally deliver a cyber-security strategy:

> Working with provinces, territories and the private sector, our Government will implement a cyber-security strategy to protect our digital infrastructure.[38]

The current government's national defence strategy, *Canada First Defence Strategy*[39]*,* which is a high level document, only mentions cyber attack in the most cursory way when it describes the threat as follows:

> 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.

According to the fall 2009 Report of the Auditor General (AG) to the House of Commons, in Chapter 7 on Emergency Management, the Minister of Public Safety recognizes that there have been repeated attacks against Canada's computer systems and

[38] Speech from the Throne, 3 March 2010. "A Stronger Canada. A Stronger Economy. *Now and for the Future.",* http://www.speech.gc.ca/eng/index.asp; Internet; accessed 19 March 2010.

[39] Canada. "Canada First Defence Strategy"; available from http://www.forces.gc.ca/site/pri/first-premier/index-eng.asp; Internet; accessed 15 February 2010.

that the "threats to computer-based critical infrastructure, including federal information systems, are evolving and growing."[40] This AG report suggests that these cyber attacks could be coming from either individuals or from groups, and while some may be unintentional or amateur, others may be state-sponsored espionage or even information warfare. It further recognizes that these attacks could cause serious damage to our computer and communications networks which, as previously mentioned, are used to control critical infrastructure components such as the electrical power grid.

In the most recently available Public Report from the Canadian Security Intelligence Service (CSIS) (2007-2008), it is reported that Canada faces some serious threats to Cybersecurity, and that

> Politically motivated cyber-related attacks can originate from a variety of groups, including foreign governments, domestic hackers with an extremist political agenda, or terrorist groups. Open-source reports have also suggested that foreign intelligence services use the Internet to conduct espionage operations….[41]

The private sector, by exploiting IM/IT technology to increase efficiency and effectiveness has developed a serious vulnerability to cyberattack which is widely recognized. For example, according to Dave McMahon of Bell Canada:

> The Canadian national information infrastructure is now decisively engaged in a cyber-war; the telecommunications and financial sectors are fighting on the front lines against transnational crime and state-sponsored campaigns. The national proactive cyber defensive matrix interdicts and disrupts over one-trillion inbound attacks per year in a pre-emptive fashion. … Public and private sector executives in Canada are being successfully targeting by organized crime and hostile intelligence agencies…[42]

[40] Sheila Fraser, "Chapter 7: Emergency Management – Public Safety Canada", *2009 Fall Report of the Auditor General of Canada;* (Ottawa: 2009), 23; Available from http://www.oag-bvg.gc.ca/internet/English/parl_oag_200911_07_e_33208.html#hd3d; Internet; accessed 14 February 2010.

[41] Canada. "CSIS Public Report 2007-2008". Available from http://www.csis-scrs.gc.ca/pblctns/nnlrprt/index-eng.asp; Internet; accessed 16 February 2010. 15

[42] Dave McMahon, http://ca.linkedin.com/pub/dave-mcmahon/4/1b7/510; Internet; accessed 11 February 2010.

Media articles regularly highlight the dangers that lurk in cyberspace. A search on the CBC news web site reveals 7,780 CBC articles related to Internet security, with thirteen in just the previous week.[43] Recently the cyber-attack that Google experienced in China has made headlines[44]. The cyber-attacks by Russia against Estonia[45] in 2007 and against Georgia[46] during their conflict in 2008 were widely reported. Last October, which Public Safety Canada had declared "Cyber Security Awareness Month"[47] the National Post recently ran a more in-depth series of four articles under the banner "Fighting the Virtual War"[48], from 20 to 23 October 2009. These articles described in some detail the growing threat to global security from the actions of Terrorists, Rogue States and organized crime in cyberspace.[49]

[43] CBC Website. http://www.cbc.ca/search/cbc?ie=utf8&site=CBC&output=xml_no_dtd&getfields=description&oe=utf8&safe=high&q=internet+security, Internet, accessed 30 March 2010.

[44] Ariana Eunjung Cha and Ellen Nakashime, The Washington Post, 14 January 2010, "Google China cyberattack part of vast espionage campaign, experts say"; http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html; Internet; accessed 15 February 2010.

[45] BBC News, 17 May 2007, Estonia hit by "Moscow cyber war", http://news.bbc.co.uk/2/hi/europe/6665145.stm; Internet, accessed 19 March 2010. (includes links to other media reports on same topic)

[46] Brian Krebs. "Russian Hacker Forums Fueled Georgian Cyber Attacks", The Washington Post, 16 October 2008; http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html; Internet; accessed 19 March 2010.

[47] Public Safety Canada, "October is Cyber Security Awareness Month," http://www.publicsafety.gc.ca/media/nr/2009/nr20091002-1-eng.aspx; Internet; accesses 15 February 2010.

[48] Mark Dubowitz and Larry Footer, "'The code is mightier than the sword'; Terrorists and rogue states are moving their battle to the Internet," National Post, 20 October 2009.
Milton Maltz, "Turning Power Lines Into Battle Lines; Terrorist groups and rogue states are moving their battle to the Internet," National Post, 21 October 2009.
Vaino Reinart, "Lessons from Estonia: Protecting the West from a computer attack," National Post, 22 October 2009.
Rodney Joffe, "The cyber crime epidemic; Terrorists and rogue states are moving their battle to the Internet. How do we fight it?" National Post, 23 October 2009.

[49] For example the first article describes how radical Islamists organizations such as as-Sahab (the media wing of al-Qaeda) make extensive use of the internet for propaganda and recruiting. The second states that US National Security officials have documented multiple covert intrusions into the computer systems that control their power lines, which is interpreted as hostile reconnaissance to find weak spots for future exploitation. The third explains the serious transnational cyber attack that Estonia experienced in 2007 and offers some lessons learned from that. The fourth and final article in this series refers to an Interpol press release estimating the losses from phishing alone (one of the most common cyber crimes) to be US$2 trillion worldwide!

There is a growing body of academic literature which describes and analyses this issue, from a military perspective[50], a criminology perspective[51], a sociological perspective[52] and information technology perspective[53], among others.

The Bureau of Justice Statistics (BJS) of the US Department of Justice and the National Cyber Security Division (NCSD) of the U.S. Department of Homeland Security cosponsored the National Computer Security Survey (NCSS) in 2005 which asked 7,818 American businesses "to produce reliable national and industry-level estimates of the prevalence of computer security incidents (such as denial of service attacks, fraud, or theft of information) against businesses and the resulting losses."[54] This extensive survey found that businesses were experiencing high levels of cybercrime, with 67% having detected at least one cybercrime, 60% one or more cyber attacks, 11% a cyber theft and 24% some other cybersecurity incident. About a third of these attacked businesses suffered monetary losses of $10,000 or more. In total 3,247 businesses were aware of having lost a total of $867 million. Of course, the impact of cyberattack is quite likely considerably higher than this study suggests. This survey found that most businesses did not report cyber attacks to law enforcement authorities. Of course this survey, as with all such surveys, does not report undetected attacks. It also doesn't report on the origins of the attacks, which could be domestic or trans-national.

[50] Ferdinand Duarte Carvalho and Eduardo Mateus da Silva editors, *Cyberwar-Netwar, Security in the Information Age*, NATO Security through Science Series, IOS Press, Amsterdam, Netherlands, 2006.

[51] Roderic Broadhurst, "Developments in the global law enforcement of cyber-crime," *Policing: An International Journal of Police Strategies & Management*, Vol 29 no. 3 (2006): 408-433.
Sylvia Mercado Kierkegaard, "International Cybercrime Convention", in *Cyber Warfare and Cyber Terrorism*, edited by Lech J. Janczewski and Andrew M. Colarik, 469-476. (Hershey, New York: Information Science Reference, 2008).

[52] Manuel Castells, *The Information Age: Economy, Society & Culture, Volume I: The Rise of the Network Society* (Malden, MA: Blackwell Publishing, 2000).
Isabelle J. Fagnot, "Behavioral Information Security", in *Cyber Warfare and Cyber Terrorism*, edited by Lech J. Janczewski and Andrew M. Colarik, 199-205. (Hershey, New York: Information Science Reference, 2008).
Vincent Mosco, *The Digital Sublime: Myth, Power and Cyberspace*, (Cambridge Massachusetts: MIT Press, 2004).

[53] Norman F. Schneidewind, "Cyber Security Models", in *Cyber Warfare and Cyber Terrorism*, edited by Lech J. Janczewski and Andrew M. Colarik, 228-240. (Hershey, New York: Information Science Reference, 2008).
Murray E. Jennex, "Cyber War Defense: Systems Development with Integrated Security", in *Cyber Warfare and Cyber Terrorism*, edited by Lech J. Janczewski and Andrew M. Colarik, 241-253. (Hershey, New York: Information Science Reference, 2008).

[54] US Bureau of Justice Statistics website: http://bjs.ojp.usdoj.gov/index.cfm?ty=tp&tid=41; Internet; accessed 29 December 2009.

While most commercial interests are reluctant to reveal the extent of their vulnerability to cyberattack, for fear of discouraging investors or clients, several surveys have been conducted which reveal at least a lower bound on the threat (since the threat is quite likely greater than what they are willing to admit). In 1991 the United Nations Commission on Crime and Criminal Justice conducted a fairly comprehensive survey of 3,000 sites in Canada, Europe and the United States. Of those who responded, 72 percent reported a security incident (this includes internal incidents) in the previous 12 months, of which 43 percent were reported to have been criminal in nature[55]. More recent surveys, while less comprehensive, show much higher incidence rates, with virtually all respondents reporting incidents, and a large proportion reporting a large and increasing number of incidents. For example a 1998 survey found 98.5 percent victimization and 43 percent having had over 25 incidents.[56] In 2004, cybercrime in Germany accounted for only 1.3% of all crime, but 57% of the financial damages arising from criminal activity which amounted to €6.8bn![57]

Several serious cyber attacks have already occurred at the national level, with Estonia being subjected to a major cyber attack from Russian hackers in the spring of 2007[58], leading to significant economic losses in the private sector, and Georgia coming under cyber attack in 2008[59] as an adjunct to the invasion from Russia. These examples clearly illustrate an inability at the international level to secure cyberspace. Since the Russian government disavowed responsibility for these attacks, and proof of such a direct involvement could not be produced, these examples also illustrate the difficulty in distinguishing between crime, terrorism and warfare in cyberspace, state-sponsored or

[55] U.N. Commission on Crime and Criminal Justice. *United Nations Manual on the Prevention and Control of Computer-Related Crime*. (New York: United Nations, 1995).

[56] Carter, D.L. and Katz, A.J.. "Computer Crime Victimization: An Assessment of Criminality in Cyberspace". *Police Research Quarterly* vol. 1, no.1 (1998)

[57] Sylvia Mercado Kierkegaard, "International Cybercrime Convention", in *Cyber Warfare and Cyber Terrorism*, edited by Lech J. Janczewski and Andrew M. Colarik, 469-476. (Hershey, New York: Information Science Reference, 2008), 471.

[58] BBC News, 17 May 2007, Estonia hit by "Moscow cyber war", http://news.bbc.co.uk/2/hi/europe/6665145.stm; Internet, accessed 19 March 2010. (includes links to other media reports on same topic)

[59] Brian Krebs. The Washington Post, 16 October 2008, "Report: Russian Hacker Forums Fueled Georgian Cyber Attacks"; http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html; Internet; accessed 19 March 2010.

not. This also illustrates the difficulty of assigning responsibility to defend cyberspace to any of the existing organizations, but this is the subject of chapter 4 below.

Based on the discussion above, the seriousness of the threat to cybersecurity is certainly well recognized by all stakeholders, including, inter alia, the Canadian government, the Police Forces, the private sector, the media, academia, and certainly by DND. The question then remains: are we, as a world and as a nation, adequately prepared to deal with this threat?

This raises many serious questions, which various organizations, both national and international, are struggling to answer. How can we best equip and organize ourselves to deal with these daunting challenges to Cyberspace Security? What is the role of the government in providing this security? What is the role of the commercial private sector? What are the responsibilities of individuals in safeguarding themselves? Can existing security organizations cope by simply coordinating their activities, or is a new organizational structure needed?

2.2 Understanding the Threat

A basic familiarity with the different types of cyber attacks will be useful in understanding how to defend against them. While there is a fundamental difference between cybercrime, cyber-terrorism and a military cyber-attack, most of the open source (i.e. unclassified) literature deals with cybercrime. Fortunately, cyber terrorists and cyber warriors attack systems in much the same way as hackers.[60] Since the attack mechanisms are so similar, we can draw much from the open source literature to understand them.

A threat to cybersecurity can be considered to have two basic dimensions: the person or organization that is using or threatening to use the attack, and the technical

[60] Murray E. Jennex. “Cyber War Defense: Systems Development with Integrated Security”, Chapter XXIX of *Cyber Warfare and Cyber Terrorism*, Information Science Reference, (Hershey, New York, 2008), 241.

means by which the attack is carried out (sometimes called the "threat vector"). Taxonomies for these will be useful in discussing cybersecurity issues.

The Bureau of Justice Statistics (BJS) of the US Department of Justice and the National Cyber Security Division (NCSD) of the U.S. Department of Homeland Security cosponsored the National Computer Security Survey (NCSS) in 2005. This survey used the following taxonomy of cybercrime[61] (which of course doesn't include pure terrorist threats or military/espionage threats from hostile nations, which are not considered criminal activities):

1. Cyber attacks: crimes in which the computer system is the target. Cyber attacks consist of computer viruses (including worms and Trojan horses), denial of service attacks, and electronic vandalism or sabotage.
2. Cyber theft: crimes in which a computer is used to steal money or other things of value. Cyber theft includes embezzlement, fraud, theft of intellectual property, and theft of personal or financial data.
3. Other computer security incidents: such as spyware, adware, hacking, phishing, spoofing, pinging, port scanning, and theft of other information, regardless of whether the breach was successful.

Robert Taylor et al. examine computer crime from a criminological and criminal justice perspective. While they recognize that computer crime is rapidly evolving in response to advances in technology, they do offer a categorization of computer crime into four types[62]:

1. The computer as a target.
2. The computer as an instrument of a crime.
3. The computer as incidental to a crime.
4. Crimes associated with the prevalence of computers.

Unfortunately neither of these taxonomies provides a satisfactory description of specific societal vulnerabilities, nor do they point to possible defensive measures. Taylor

[61] US Bureau of Justice Statistics website: http://bjs.ojp.usdoj.gov/index.cfm?ty=tp&tid=41; Internet; Accessed 29 December 2009.

[62] Taylor, Robert W. et al., *Digital Crime and Digital Terrorism*. (New Jersey: Prentice Hall, 2006), 9.

et al. however do provide a detailed description of the types of crimes and terrorist attacks that are most common. They describe “white Collar Crimes”:[63]

1. Embezzlement.
2. Corporate Espionage.
3. Money Laundering.
4. Identity Theft.
5. Internet Fraud.

While most of these appear to be Police matters, on a larger scale some could easily involve National Security, and clearly most of these often are transnational in nature. Other classes of cybersecurity problems are more directly associated with terrorism, and the same authors provide a brief description of these threats as well, although without such a clear taxonomy. They include:[64]

1. Critical Infrastructure attacks
2. Information Attacks
3. Propaganda and Promotion
4. Information Warfare as an Adjunct Attack

Another simple, but perhaps more comprehensive taxonomy of cyber threat vectors is offered here: (see Appendix 2 for definitions of technical terms):

1. Theft of information (such as identity theft, theft of IP, corporate espionage, national espionage)
2. Corruption of information (spoofing) (defacing a web site, inserting, deleting or changing records such as medical, financial or legal). This can have grave impact if for example it involves the interference with control of devices of critical infrastructure (electrical grid, water supply) or major manufacturing etc.
3. Denial of service (bringing down websites, blocking access to web-based services). When conducted on a large scale, this can become what is called Distributed Denial of Service (DDoS: using a botnet for widespread denial of service).
4. Hijacking of computers (remotely controlling programs that have been surreptitiously loaded onto a computer via the Internet. Sometimes large numbers of such hijacked computers can be marshalled together into a ‘botnet’ and used for DDoS)

[63] Ibid (99).
[64] Ibid (19-33).

For example a hostile state could launch a large scale cyber attack, using any or all of the threat vectors described above. This could be done in conjunction with a conventional attack, such as appears to have happened in Georgia, or as a separate, purely cyber attack, as appears to have happened in Estonia (as described in the previous section).

Most of these attacks are initiated by deceiving or inducing a computer user or program to download a file, with hidden malicious code, over an Internet connection. One significantly different hypothesized threat scenario is the following: somehow a malicious person or organization (or country) embeds latent threats into electronic components that an ICT manufacturer (unknowingly or otherwise) then builds into their computers or other Internet devices, such that these threats can at some future date be remotely activated and used by the malicious entity. This is the "unsecured supply line" scenario.

Another significant aspect of the threat, which largely determines which organization has the authority and responsibility to defend against it, is the human source and their motivation. The human sources of threat can be:

1. criminals (organized or individuals, foreign or domestic),
2. terrorists (foreign or domestic),
3. hostile states,
4. vandals / "hackers" (intentional or accidental, foreign or domestic).

For illustrative purposes, and using the same scheme as figure 1 above, figure 2 below illustrates these sources of threat, in bold (from both within and outside Canada). Note that private citizens and private corporate sector elements from outside Canada are also potential threats, even if their host nation does not consider them to be criminal or terrorist (either because of inadequate laws, state failure, or state hostility).

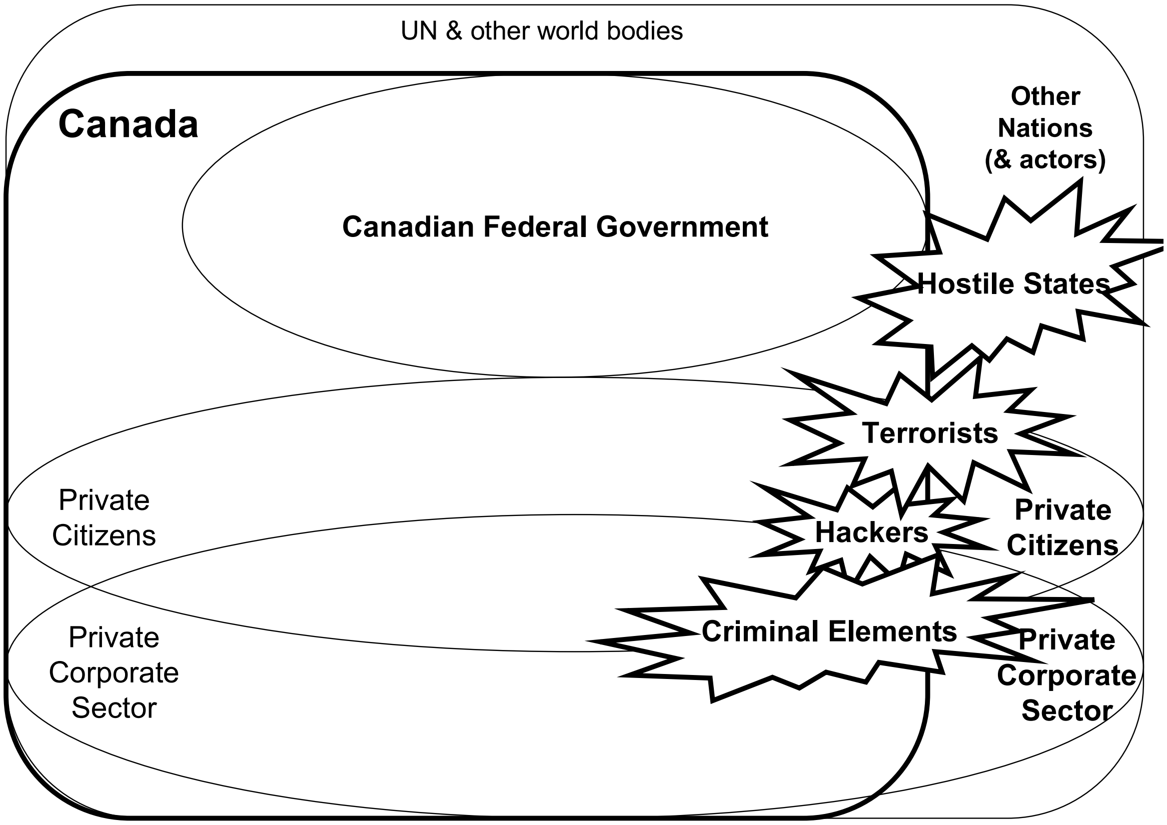


Figure 2. Sources of Threat to Canadians in Cyberspace.

These threats have largely been described in terms of who the victims and aggressors are, and what type of harm is done, in order to provide some understanding of the difficulty in defending against them. Since a detailed description of the actual methods of attack would be highly technical in nature, such description is limited to the set of simplified definitions in Appendix 2. This technical nature of the threats makes it difficult for many stakeholder organizations to fully understand what they are facing in cyberspace.

It should also be emphasized that these threats are evolving, as the technology evolves (according to Moore's Law) and, more significantly, as the ways in which we use cyberspace evolves (in an essentially unpredictable way). Together with the technical complexity, this further exacerbates the problem of developing adequate defences.

2.3 Countering the Threat

There are at least five fundamentally different aspects of defence in cyberspace: first there is the **individual user**, who has a significant role to play in cybersecurity, secondly there is the computer **hardware and software manufacturers**, whose products may or may not provide adequate inherent security measures, thirdly there is the immediate and "physical" work of the **network operation**, which has many layers of defence needed to keep the networks running, fourthly there is the **forensic** activity that is conducted to investigate incidents after the fact to discover and characterize new threats that appear, fifthly there is the **regulatory** work needed to set agreed technical standards for procedures, protocols and formats etc., and finally there is the **legislative and legal** work needed to provide the necessary authorities, constraints, deterrents and recourses needed by the manufacturers, operators, regulators, users and government authorities. At the international level, this last aspect is likely the most difficult.

A cursory description of these roles will help to illuminate the obstacles that stand in the way of current efforts to provide cybersecurity.

The role of the individual user in countering threats in cyberspace, while important, is fairly limited. Other than not directly contributing to cyber crime or cyber terrorism, the individual user can only attempt to secure, to the extent possible, his or her own node and behaviour on the Internet, to ensure that it is not compromised or otherwise contributing to broader security problems. Since all users are on some network, the responsibility largely falls on the network operators to attempt to educate all users and instil in them the proper security etiquette and protocols (such as securing passwords, using firewalls and anti-virus software etc.).

The network operators do what they can to recognize and respond immediately to threats as they appear on the network. Network operators for organizations generally manage the local area network, or intranet, for that organization, which normally has some connectivity with the Internet (classified networks are typically "stand-alone" with dedicated secure communication links to remote parts of the network). Operators generally employ a "defence in depth" approach with layers of defensive measures, such as firewalls (to block threats that have been previously recognized), virus checkers (to detect threats that have penetrated the firewalls), switches (to immediately isolate infected branches of the network), system backups (to enable data restoration in the event of a serious infection) and so on. They will typically have tools that allow them to visualize in real time the health status of the component parts for which they are responsible. A network operations room is in many ways similar to a military operations room. It requires continuous monitoring and defensive action. This is not an environment where there is time to seek legal opinions before initiating a defensive action. Criminals or terrorists who are mounting an attack in cyberspace can hop quickly between servers in different countries, so the authorities, in order to counter a threat, need to be able to access these servers quickly to secure electronic evidence before they move on, and need to be able to subpoena the service providers to hand it over.

There is also a forensic component to network operations that is conducted at a slower pace. This is an important element of the defence in depth approach, as it characterizes threats, in ways that are needed to develop defences against them for real-time operations. Forensics is conducted after the fact for the purpose of precisely reconstructing and understanding the attack. It typically involves an analysis of target and source computers, if available, as well as some networking elements. Cyber forensics can reveal a host of important facts, such as the precise attack time, the "weapon" and methods used, the information that has been destroyed, stolen of corrupted, and perhaps even the identity and location of the attacker. [65] Ultimately this is intended to only to support deterrence, prosecution and post hoc mitigation activity.

In the area of regulation, the ICT Standards Advisory Council of Canada (ISACC) works on the Global Standards Collaboration (GSC) group, together with its international

[65] Stéphane Coulondre, "Cyber Forensics", Chapter XLVI of *Cyber Warfare and Cyber Terrorism*, Information Science Reference, (Hershey, New York, 2008), 397.

counterparts (other participating standards organizations) and the International Telecommunications Union (ITU). Together these organizations, inter alia, maintain an *ICT Security Standards Roadmap,* actively examine the relevant communications protocol standards for their robustness of design and potential for exploitation by malicious parties, and promote global, consistent, and interoperable processes for sharing incident-response related information.[66] At the last meeting of this group (July 2009), it recognized in it~~’~~s resolution “the critical importance of international, regional and national cooperation in developing effective strategies to mitigate cyber threats, including spam” and “new cyber attacks such as phishing, pharming and botnets are emerging and spreading rapidly”.[67]

Unfortunately the legal framework for the prosecution of cyber crime and cyber terrorism, particularly in the transnational context, has not evolved quickly enough to be effective in deterring or responding to these cyber threats. The current legal recourse to extra-jurisdictional attackers is limited to the use of bi-lateral Mutual Legal Assistance (MLA) Treaties. These provide a mechanism for the Canadian Department of Justice to request the cooperation of another county’s legal authorities in the investigation and prosecution of a crime. As of 2004 Canada had such treaties with only 33 other countries.[68] To be truly effective against cyberattack, as explained by Roderic Broadhurst,[69] an international legal regime would really have to be multi-lateral. Such an effort has just begun, as will be described in chapter five.

In summary then, there are four distinct but interdependent “layers” needed for effective cyber defence:

1. Legal
2. Regulatory, policy
3. Forensic, investigative
4. Operational, defensive

[66] Global Standards Collaboration group resolution GSC-14/11 (Geneva, 2009). http://www.itu.int/ITU-T/gsc/index.html; Internet; accessed 14 November 2009.

[67] Ibid.

[68] A list of these 33 countries is available at http://www.oas.org/juridico/mla/en/can/en_can-mla-gen-g8iag.html; Internet, accessed 27 April 2010.

[69] Roderic Broadhurst. “Developments in the global law enforcement of cyber-crime,” *Policing: An International Journal of Police Strategies & Management*, Vol 29 no. 3 (2006): 408-433.

It is important to note that each of these functions operates on a different time scale and in a different environment. Changes to laws and regulations typically take months or years, whereas a forensic operation should ideally be done in the hours or days after an event, and defensive operations are sometimes required within seconds or milliseconds. The expertise needed to do these four functions is different in each case[70], and typically different government organizations have responsibility for each.

2.4 Threat Summary

From the section 2.1 above, it can be seen that the many threats to Canada and Canadians in cyberspace have been widely recognized by the Canadian Government and its many institutional stakeholders, as well as by the private sector and the media. The international community has also recognized these threats.

We have also seen in section 2.2 some examples of how various experts in Cybersecurity have attempted to characterize and categorize the threats in different ways, to suit their needs. We saw that these efforts are of limited use in developing a clear understanding that all stakeholders could share in defending cyberspace, however they will be useful in chapter 4 below when we consider whether or not each type of threat is being defended against.

In section 2.3 we examined the types of activities that are needed to provide Cybersecurity, and we saw that they require different types of expertise and different modus operandi. This identified four different "cyber defence layers" which will be quite useful in chapter 4 below when we consider how well our cyber defence efforts are covering each of these layers.

[70] Legal work of course must be done by legal experts, regulations and policy by experts in technical standards and policy, forensic and investigative work by technical crime experts, and operational defence by network operations experts.

3 Obstacles to Providing Cyber Security

Before discussing specific efforts being made by Canadian and international institutions to provide cyber security, and the inadequacy of those efforts, it is useful to briefly explain why cybersecurity is such a difficult problem, given the manner in which our institutions are organized and empowered.

There are three serious obstacles to our preparedness against this threat. The first obstacle is that the threat is not well understood, and in fact not well defined. While its existence and severity are well recognized by many stakeholders, the appropriate means of defence is not. In one sense it is a complex and technical threat, as described in section 2.2 above, which is evolving rapidly as both the environment itself and the tools that are available to exert effect in this environment are evolving rapidly. This change is expected to continue at an ever-increasing rate, driven by the well-know exponential growth of IT described by Moore's Law[71] (and which, according to Kurzweil[72], applies to much more than just IT). In another sense it is not only about the technology but also about how we are using it and how our social, political and economic structures are evolving.

In 2000 the sociologist Manuel Castells described the many dramatic changes to our social, economic and political landscape that were being driven at that time by "the network society" as he called it. According to Castells this information technology revolution has stimulated the evolution of our social structure by shifting its mode of development from industrialism to informationalism.[73] Castells also suggests that this "did not come out of any pre-established necessity, it was technologically induced rather than socially determined,"[74] which helps to explain why it is so difficult to understand.

[71] Gordon Moore, former Chairman of Intel, observed the doubling of transistors per printed circuit board every 12 months in the mid-1960s. This leads to an exponential growth in computing capability.

[72] Ray Kurzweil, *The Singularity is Near*, (London: Penguin Books Ltd., 2005), 56. He observes exponential growth in many other technologies (with different doubling rates).

[73] Manuel Castells, *The Information Age: Economy, Society & Culture, Volume I: The Rise of the Network Society*, Second Edition, (Malden: Blackwell Publishing, 2000), 164-166.

[74] Ibid. 60.

More recently, even newer phenomenon are being observed, such as the recent rapid rise of social networking. How this will affect our cybersecurity needs and constraints is difficult to predict. These technical and sociological complexities hinder the ability of the responsible institutions, and in particular governments, to formulate and implement clear and effective responses at both the organizational and operational level. Policy development experts are increasingly challenged to remain abreast of relevant technological developments, let alone predict their social impacts. In the case of cyberspace there are also politically sensitive issues involved, such as the trade-offs between freedom of information and copyright/national security and between individual privacy and public safety. For many citizens, the prospect of government oversight of the Internet is threatening, as evidenced by the interestingly provocative title of an article in a popular magazine: “Jackboots on the Infobahn”[75].

These changes in the use of cyberspace are in some sense also driving the change in technology, which responds to that demand. This therefore creates a recursive feedback loop whereby social change and technological change are feeding off each other.

The cyber domain is, therefore, particularly difficult to legislate for, given the slow pace of legislative change compared to the rapid and largely unpredictable evolution of cyberspace and how it is used. This challenge is magnified many-fold in the realm of international law, where the regulative, normative and cultural values of different nations often conflict.

The other two serious obstacles to cybersecurity both arise from jurisdictional ambiguity. As explained by Gladstone,[76] under traditional legal systems, the sovereign power of the state, which legitimizes the enforcement of its laws, is based on

[75] J.P. Barlow, “Jackboots on the Infobahn”, in *Wired*, April 1994. A discussion by a Libertarian of the US government attempt to introduce the Clipper Chip, which would have provided widespread encryption for privacy, but with the US government having access to all encryption keys.

[76] Julia A. Gladstone, “Global Aspects of Cyberlaw”, in *Global Perspectives in Information Security: Legal, Social and International Issues*, ed. Hossein Bidgoli, 627-665 (Hoboken, New Jersey: John Wiley & Sons Inc., 2009), 630.

territoriality, and there is generally a correspondence between physical borders and legal borders. In this context, according to Gladstone, “The main criticism that transnational cyberspace breaks jurisdictional rules is based on the notion that a state may not act beyond its own territorial borders.”[77]

Hence the second major obstacle is the geographic jurisdictional confusion that results from the connectivity of cyberspace. This arises at both the national and transnational level, leading to a much fractured institutional responsibility for defending this new domain of cyberspace, as will be described below in chapter four. Because of the high level of connectivity (a fundamental design feature of the Internet), actions in cyberspace are not well constrained by geographic boundaries (national jurisdictions). Criminal or terrorist elements in one nation (say A) can easily use the Internet to target victims in another (say B), as described in section 2.2 above, and of course the victim can be an individual, a corporation, a government or even the population in general (via the critical infrastructure, such as disrupting the electrical power grid, water supply or telephone system). In fact element A could even attack victim B by remotely using a hijacked computer in a third country, (say C). Which country then has responsibility for controlling this? Whose laws apply? The victim in country B cannot normally use its own legal system to seek redress from an attacker in another country, when the attack didn’t “take place” in that other country. In this case the victim must either rely on the cooperation of country A (the “host” nation of the attacker) to take effective action (i.e. prosecute its own citizen for a crime committed in another country), and also the host country of C (to collect evidence from the machine from which the attack was directly felt) or else the victim from country B must attempt to take action itself within countries A and C, both foreign nations, which is usually not practical. Even conducting cyber forensics to establish the facts is greatly impeded by this jurisdictional divide. Naturally hostile elements will tend to gravitate to “host” nations that are less willing or able to effectively control them[78]. Particularly in the developing world, there are a number of weak or failing states where the central government is not strong enough, or in some

[77] Ibid. 630.

[78] John Rapley, “The New Middle Ages”, *Foreign Affairs*, May/June 2006, Vol. 85 Issue 3, p95

cases not motivated enough, to exercise control over criminal or terrorist elements. Of course some such states in the recent past have gone so far as to sponsor terrorist activity.

Although efforts are underway, the national and international legal framework for dealing with this has not yet been constructed. According to Roderic Broadhurst of Queensland University of Technology:

> The cross-national nature of most computer-related crimes has rendered many time-honoured methods of policing both domestically and in cross-border situations ineffective even in advanced nations, while the "digital divide" provides "safe havens" for cyber-criminals. In response to the threat of cyber-crime there is an urgent need to reform methods of mutual legal assistance and to develop transnational policing capability. [79]

This cross-jurisdictional problem even arises at the national level. Taylor et al describe the frustrations of law enforcement agencies in the US with incidents that cross state lines.[80]

The third major obstacle is another type of jurisdictional confusion, which arises partly from the anonymity of the Internet, partly from its speed, and partly from its transnational nature. This is the jurisdictional confusion within a nation between the many security organizations such as the military, the police, and the intelligence organizations. In this case the jurisdictional responsibility for dealing with a threat is usually determined by two factors: the type of threat (crime, espionage or military attack) and the source location of the threat (domestic or foreign). The anonymity and speed of the Internet can often make it impossible to identify the type of threat or the source location until after the fact. Cyber attacks can be distributed (coming from many machines that are in different locations) and they can be indirect (such that the actual

[79] Roderic Broadhurst, "Developments in the global law enforcement of cyber-crime," *Policing: An International Journal of Police Strategies & Management*, Vol 29 no. 3 (2006): 408-433.

[80] Robert W. Taylor, *et al*, *Digital Crime and Digital Terrorism*, (Upper Saddle River, New Jersey: Pearson Prentice Hall: 2006), 208 (cites examples where cyber-stalkers from out-of-state could not be prosecuted, where cybercrimes in some jurisdictions, such as gambling and prostitution, may not be illegal in the other jurisdiction, and where a remote computer search authorized by a warrant at one end could be illegal at the other).

triggering computer is not directly participating in the attack), so that the true source is not easily determined, let alone geographically isolated (such as a DDoS attack from a BotNet[81]). The traditional division of responsibility between Canadian police forces, military forces and national intelligence forces, is largely predicated on the assumption that internal threats and vulnerabilities can be separated from external threats and vulnerabilities, by such measures as controlling the borders and coastlines. Cyberspace does not have such well-defined borders.

What is more, there is a blurring of the distinction between warfare and crime in this new domain. The distinction is not easily made between the actions of a warring nation, a criminal organization, a terrorist organization, a spy and a hacker. Clausewitz, who has a great deal to say about war, initially defines it as simply "an act of force to compel our enemy to do our will."[82] He then however goes on to characterize war in many different ways. Today the Cambridge dictionary defines war as "armed fighting between two or more countries or groups" and crime as "illegal activities"[83]. Globalization and technology are making this distinction much more complex, and our laws have not kept up with the changing environment. Nations can now attack each other in cyberspace, without the use of "arms" or physical force in the conventional sense, and can have devastating physical effect by doing so.[84] Estonia attempted unsuccessfully in 2007 to have NATO recognize the cyber-attack from Russia as a clear military attack on their nation, in accordance with Article 5 of the NATO Charter, to trigger a NATO response[85]. At that time, not a single NATO defence minister would define a cyber-attack as a clear military action (which may have required NATO to go to war over Estonia).

[81] See definitions in appendix

[82] Carl von Clausewitz, *On War*, Indexed Edition, ed. and trans. Michael Howard and Peter Paret, (Princeton: Princeton University Press, 1976), 75.

[83] Cambridge Advanced Learner's Dictionary, http://dictionary.cambridge.org/; Internet; accessed 11 May 2010.

[84] For example by sending dangerous control signals to SCADA devices controlling critical infrastructure as described in section 1.2 above.

[85] Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia", *The Guardian*, Thursday 17 May 2007, http://www.guardian.co.uk/world/2007/may/17/topstories3.russia; Internet; accessed 29 April 2010.

The dilemma here is therefore two-fold: at the inter-national level and at the national level. At the international level, each nation has jurisdiction over its own citizens and responsibility to protect its own critical infrastructure and national secrets. In cyberspace neither the threats nor the vulnerabilities are constrained by national boundaries. At the national level, within each nation different institutions have responsibility for defending against and responding to these different types of threat (domestic crime, international crime, state espionage, commercial espionage, military cyber attack, etc.). However, as discussed in section 2.3 above, an effective response has to be launched almost instantaneously. The dilemma is that if any of the responsible agencies wishes to defend against a certain type of attack, it would essentially have to defend against all attacks (most of which will fall outside of its jurisdiction) since defending against a cyber attack generally cannot wait for an inter-organizational discussion to take place to determine responsibility.

The significance of these obstacles will become clearer when the responsibilities and authorities of the various national security agencies are considered in the next chapter.

Now that the threats to Canada's cybersecurity have been exposed, along with Canada's vulnerabilities to them and some of the difficulties in defending against them, hopefully the first part of this paper's hypothesis has been established: namely that cybersecurity is a serious challenge for Canada. The next chapter will argue that Canada is not adequately prepared to deal with this challenge.

4 Canadian Cybersecurity Measures

One could argue that cyberspace is a "common good" in the language of economics, since it is a shared resource that is not owned in the conventional sense by any single private entity or group of entities, given that its value is due more to the individuals, corporations and institutions that provide their "presence" in cyberspace, and less to the wires and routers that connect them. This is therefore somewhat like the high seas or the airspace, or even more like near-earth outer-space, where governance is less mature. Satellite orbits do not "belong" to anyone, but it is in everyone's interest to de-conflict them to avoid collisions. This would point to the vulnerability of cyberspace to the "tragedy of the commons" which refers to the fact that when a resource is shared by many users, no individual will find it economically worthwhile to assume the cost of its maintenance or protection. While the individual computers, routers, switches and communication channels are owned by various entities, and there is a governance body to set standards, the power and value of the Internet is found not in these components, but in the information content that is made freely available to all, and the connectivity that doesn't rely on any particular components (other than some initial connection to the Internet).

Given that cyberspace is a vital common good, without an 'owner' to take responsibility for it's maintenance, and given it's importance to society and to the national economy, one would expect that there would be a strong role for the government in ensuring that this common good is protected. In fact the government of Canada, in the Appendix B of the 2009 *Policy on Government Security*, did promise that Public Safety Canada would "Provide central coordination for assessing emerging complex threats and developing and promoting … approaches to address risks within the federal government and across Canada".[86] While this is far from an explicit recognition of total responsibility for cybersecurity, it could be interpreted as an implicit commitment to ensure that cyberspace is somehow made secure for Canadians.

When it comes to cybersecurity for the government itself, the 2009 Policy is explicit. It states that the Communications Security Establishment Canada (CSEC) is responsible for "Predicting, preventing and defending against sophisticated IT security

[86] Canada: *Policy on Government Security*, http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578&section=text; Internet; accessed 15 January 2010.

incidents, threats and vulnerabilities"[87]. The real question is: who will do this for Canada?

To examine the authorities, responsibilities and capabilities of the various stakeholders in Canada, it will be helpful to have a more complete picture of who they are and how they relate to each other. Figure 3 below attempts to provide this, following the same scheme as figures 1 and 2, by illustrating the primary Canadian stakeholders with responsibility for defending cyberspace, including various federal government organizations and segments of the private corporate sector.

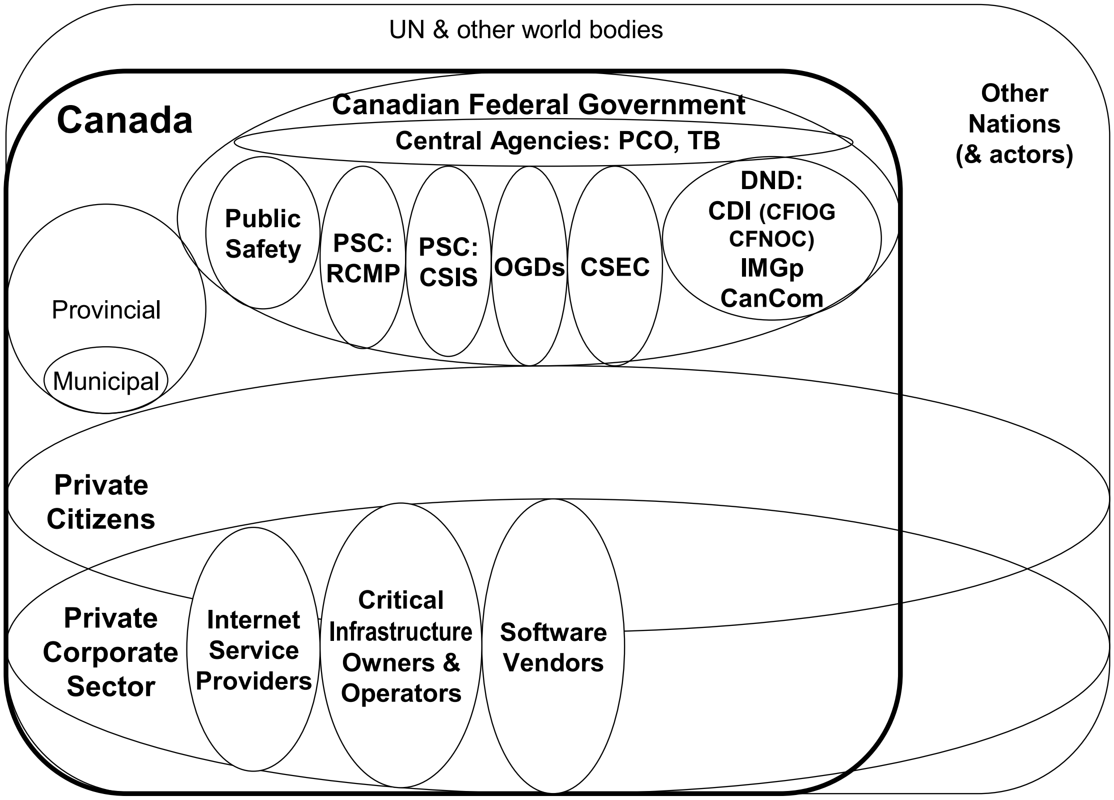


Figure 3. Canadian Stakeholders Who Share Responsibility for Cyber Security.

When it comes to cybersecurity for the government itself, the 2009 Policy is explicit. It states that the Communications Security Establishment Canada (CSEC) is responsible for "Predicting, preventing and defending against sophisticated IT security

[87] Ibid.

incidents, threats and vulnerabilities"[88]. The real question is: who will do this for Canada?

This chapter will discuss the responsibilities, authorities and capabilities of various stakeholders to provide cyber-security in general, and specifically for Canada and Canadians. These Canadian stakeholders include the federal government, other public sector institutions, the private corporate sector, and finally individual citizens (the international aspects will be discussed in the following chapter). Each of these stakeholder groups will be considered in turn.

4.1 Government of Canada Effort

While the private sector and individuals share much of the responsibility for their own security, it is the Government of Canada that is ultimately responsible for providing national security, safeguarding the national critical infrastructure and ensuring the delivery of government services. The national government is also responsible for international relations and defending Canadians from external threats. Therefore the focus of the discussion in this section will be on federal institutional capabilities.

As with other government responsibilities, the central agencies provide the overall coordination and top level policy guidance. In this case it is the Treasury Board Secretariat (TBS) that establishes and oversees the whole-of-government (WoG) approach to security, as currently described in their *Policy on Government Security* document[89], which describes the federal governments approach to providing security, including cyber security, for itself. This document identifies the lead security agencies within the federal government and describes their responsibilities. The lead departments and agencies are: TBS, Privy Council Office (PCO), Public Safety Canada (PS), the Department of National Defence (DND) / Canadian Forces (CF), the Communications

[88] Ibid.

[89] Canada: *Policy on Government Security*, http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578&section=text; Internet; accessed 15 January 2010.

Security Establishment Canada (CSEC, which falls under DND), Public Works and Government Services Canada (PWGSC), Canadian Security Intelligence Service (CSIS, which falls under PS), Royal Canadian Mounted Police (RCMP, which also falls under PS), Library and Archives of Canada (LAC), the Department of Foreign Affairs and International Trade (DFAIT) and the Canada School of Public Service (CSPS). This document also describes the relevant responsibilities of these departments and agencies.

The Privy Council Office (PCO) advises and supports the prime minister and Cabinet on national security matters inter alia, and coordinates the related activities of departments and agencies. The associate Secretary to the Cabinet in the PCO is also the "National Security Advisor to the Prime Minister" and as the name implies, advises the Prime Minister on security matters and strengthens the capacity of the PCO to develop and implement an integrated policy on national security and emergencies. This Advisor is supposed to ensure the effective coordination of Canada's security and intelligence community and, together with the Deputy Minister of National Defence, be responsible for the Communication Security Establishment Canada (CSEC). However the National Security Advisor also supports the Security, Public Health, and Emergency Committee to Cabinet, and coordinates integrated threat assessments in all domains, as well as inter-agency cooperation among security organizations. This Advisor clearly doesn't have a great deal of time to dedicate to cyber security!

When it comes to actual operational jurisdiction in this area, the Canadian national security institutions with primary responsibility are, as illustrated in Figure 3 above, our national police force, our military force and a national intelligence agency. That is the Royal Canadian Mounted Police (RCMP), the Department of National Defence (DND), the CSEC, reporting to the Minister of Defence and the Canadian Security Intelligence Service (CSIS). As already mentioned, the Treasury Board Secretariat (TBS) provides oversight, and Public Safety Canada (PS) establishes policy and coordination. Other federal departments are simply responsible for safeguarding their own information holdings.[90]

[90] Ibid.

The question then becomes: are these Canadian government institutions, either individually or collectively, adequately equipped and empowered to provide cybersecurity for Canada? To answer this question we will first briefly examine their roles, responsibilities and capabilities in more detail.

4.1.1 Public Safety Canada (PS)

Public Safety Canada (PS) was created in 2003 to ensure coordination across all federal departments and agencies responsible for national security and the safety of Canadians. Its mandate is to keep Canadians safe from a range of risks such as natural disasters, crime and terrorism. To do this, Public Safety Canada establishes policies, standards and programs for emergency management, and provides advice to government on matters of national security. It provides central coordination for assessing emerging complex threats and developing and promoting comprehensive, coordinated approaches to address risks within the federal government and across Canada[91]. It also coordinates and supports the efforts of federal organizations, works with other levels of government, first responders, community groups, the private sector and other nations.[92] PS also has several constituent agencies, such as the RCMP and CSIS, which have their own roles and capabilities, however these will be considered separately below.

PS made a commitment to develop a Cyber Security Strategy in the 2004 National Security Policy, and is still in the process of developing it. However, according to the *Report of the Auditor General of Canada to the House of Commons*, written in the fall of 2009:

> We found that Public Safety Canada had made slow progress until this past year on its 2004 commitment to develop a cyber security strategy,

[91] Ibid.

[92] Public Safety Canada website. http://www.publicsafety.gc.ca/abt/wwd/index-eng.aspx; Internet; accessed 31 December 2009.

> although threats to computer-based critical infrastructure, including federal information systems, are evolving and growing.[93]

At the time of the audit, Public Safety Canada had only just begun to develop its cyber strategy, by defining the key elements and, along with other federal departments, to initiate a number of cybersecurity initiatives. The Auditor General therefore recommended that PS should define risk-based policies and issue guidance to help departmental sector heads define their own infrastructure protection requirements, and to define the needs of Canadians. One of the challenges that could be holding up the development of policy in this area is the desire to strike a balance between the need to protect and defend our networks and the need to also protect the privacy of individuals.[94]

PS runs the Government Operations Centre (GOC), which is Canada's strategic-level operations centre, designed to continually monitor potential threats to the national interest and provide coordination at the national level, uniting the efforts of all federal departments and agencies in the event of a national emergency. It is the hub of a network of operations centres that are operated by federal departments and agencies including the RCMP, CSIS, National Defence, Health Canada, and Foreign Affairs and International Trade Canada. The federal government also maintains contact with the corresponding provincial and territorial authorities, through regional offices, as well as with international partners such as the United States and NATO.

The GOC however is a strategic level "operations centre" and is designed as an information clearing house to provide awareness and warning. It does not itself have the capability needed to conduct defensive operations. Given the need for extremely rapid (automated) response in the event of a cyber attack, its utility in such a situation would be severely constrained. The conclusion therefore is that PS has neither the authority nor the capability to provide operational cybersecurity for Canada.

[93] Sheila Fraser, "Chapter 7: Emergency Management – Public Safety Canada", *2009 Fall Report of the Auditor General of Canada;* (Ottawa: 2009), 24; Available from http://www.oag-bvg.gc.ca/internet/English/parl_oag_200911_07_e_33208.html#hd3d; Internet; accessed 14 February 2010.

[94] MGen Glynne Hines, "NATO: All for one and one for all in cyberspace", in *Vanguard*, Mar-Apr 2010, 13.

4.1.2 Communications Security Establishment Canada (CSEC)

According to the new *Policy on Government Security*[95]: Communications Security Establishment Canada (CSEC) provides leadership and coordination for departmental activities that help ensure the protection of electronic information and information systems of importance and serves as the government's national authority for SIGINT (signals intelligence) and COMSEC (communications security). CSEC also provides the Government of Canada (GC) with foreign intelligence and guidance on the security of government telecommunications and electronic data processing and is responsible for responding to and participating in the investigation or analysis of sophisticated IT security incidents, threats and vulnerabilities, and for acting on information collected or received from these investigations.

CSEC is also responsible for providing services to federal departments for (inter alia)[96]:

- Predicting, preventing and defending against sophisticated IT security incidents, threats and vulnerabilities,
- Handling and mitigation of sophisticated IT security incidents,
- Security architecture design for GC shared, common or federated initiatives,
- IT security product assessment and/or approval for products in use in classified domain when deemed necessary.

CSEC, therefore, clearly has the mandate to provide some degree of cybersecurity for federal government departments, (particularly for highly sensitive electronically stored information). However this service does not appear to be extended to anyone else, including those responsible for non-government critical infrastructure, the private corporate sector, and Canadian citizens.

The conclusion here is that CSEC, while it does have some very valuable expertise and operational capability in technologies such as data encryption which are

[95] Canada. *Policy on Government Security*. July 1, 2009; available from http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?evttoc=C&id=16578&section=text; Internet; accessed 15 Jan 2010.
[96] Ibid.

used in the protection of information (and to defeat that protection), it does not have the mandate to extend this protection beyond the government of Canada.

4.1.3 Royal Canadian Mounted Police (RCMP)

The new *Policy on Government Security*[97] states that the Royal Canadian Mounted Police (RCMP) provides leadership and coordination for departmental activities that help ensure the physical protection of government information, assets, facilities and people and provides services related to crime prevention, personnel screening, policing, law enforcement and investigations.

Among the list of specific responsibilities, most of which relate to physical protection, are included the following two which relate to cybercrime:

- Providing services for:
    - Reviewing and advising on counter-technical intrusion detection,
    - Criminal investigations, including computer forensics and cyber crime;
- Gathering, analyzing, consolidating and facilitating the sharing of operational threat and vulnerability information related to identity crime, physical security, cyber crime and other relevant criminal activity and communicating it to Public Safety Canada, TBS and, as authorized, departments;

The RCMP therefore has some responsibility for security against cyber crime, but it is in the realm of detection after the fact and response (prosecution) rather than real-time defence of active mitigation, and is particularly targeted against criminal actions such as identity theft, pornography, fraud etc. The RCMP does not have the authority or the capability to actively defend against a cyber attack of any sort.

4.1.4 National Defence (DND)

[97] Treasury Board Policy Suite, "Policy on Government Security"; available from http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?evttoc=C&id=16578&section=text; Internet; accessed 15 January 2010.

The mandate of DND/CF has been articulated by the current government in the *Canada First Defence Strategy* (CFDS)[98]. This document defines, at a high level, the six core missions:

1. Conduct daily domestic and continental operations, including in the Arctic and through NORAD
2. Support civilian authorities during a crisis in Canada such as a natural disaster
3. Support a major international event in Canada, such as the 2010 Olympics
4. Lead and/or conduct a major international operation for an extended period
5. Respond to a major terrorist attack
6. Deploy forces in response to crises elsewhere in the world for shorter periods

While none of these missions is specifically aimed at securing cyberspace, many of these traditional core missions now rely heavily on the use of cyberspace because most DND/CF communication, command and control capabilities are now network based. Some of these missions could even have a primary cyberspace focus. For example, under normal domestic operations the DND/CF networks, which are critical for operations, are under constant attack, and are being actively defended[99]. What is less clear however, is the extent to which these missions (1, 2 and 5 in particular) imply that DND has the responsibility to defend Canada (and not just DND itself) against a concerted cyber attack from another country, or from a terrorist organization.

Without specifically identifying the threat, CFDS does recognize the need for DND to have "the core capabilities and flexibility required to successfully address both conventional and asymmetric threats, including terrorism, insurgencies and cyber attacks." For this purpose DND does have the CF Network Operations Centre (CFNOC), which conducts active cyber defence operations for DND networks, but not for other departments and not for the private sector or the public. CFNOC does collaborate with other key stakeholders such as CSEC, CSIS, RCMP and DFAIT, however they do not operate in an integrated manner. According to the Director General of Information

[98] Canada. "Canada First Defence Strategy"; available from http://www.forces.gc.ca/site/pri/first-premier/index-eng.asp; Internet; accessed 15 February 2010.
[99] Department of National Defence, B-GJ-005-300/FP-000 *Canadian Forces Operations* (Ottawa: DND Canada, 2004), 22-3.

Management within DND, this CFNOC capability (in his organization) is nascent and the necessary horizontal integration is not yet institutionalized[100].

The conclusion from this is that (presumably) DND can adequately defend its own networks from attack, but not anyone else's.

4.1.5 Canadian Security Intelligence Service (CSIS)

According to the new *Policy on Government Security*, Canadian Security Intelligence Service (CSIS) collects, investigates, analyzes and retains information and intelligence that may be suspected of constituting threats to the security of Canada and provides security assessments to departments within its statutory mandate.[101]

CSIS programs are aimed at collecting, investigating, analyzing and retaining information and intelligence that may be suspected of constituting threats to the security of Canada. Its focus is on the threats of: [102]

1. Terrorism:
2. Proliferation of Weapons of Mass Destruction:
3. Espionage and Foreign Interference:
4. Transnational Criminal Activity:
5. Information Security Threats: Investigating threats against critical information systems and infrastructure posed by foreign countries, terrorists, and hackers.
6. Providing security assessments on behalf of federal government departments and agencies (except for the RCMP).

The third and fifth threats clearly give CSIS the responsibility to investigate and report on cybersecurity threats. It does not however appear to have the authority (or the

[100] BGen. Steve Noonan, "The Strategic Requirements of a New Domain", interview in *Vanguard*, March-April 2010, 16.

[101] Canada. Policy on Government Security. July 1, 2009; available from http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?evttoc=C&id=16578&section=text; Internet; accessed 15 Jan 2010.

[102] Canada. CSIS web site. http://www.csis-scrs.gc.ca/prrts/index-eng.asp; Internet. accessed 31 December 2009.

capability) to defend against them, so CSIS can not currently contribute operationally to the provision of security to Canada against even this limited class of cyber attack.

4.1.6 Others

Other federal institutions are responsible for certain limited aspects of cybersecurity in their own sphere:

Public Works and Government Services Canada (PWGSC) provides leadership and coordination of activities to help ensure "security in contracting", through the application of security safeguards through all phases of the contracting process within the scope of the industrial security program (ISP).[103] PWGSC also has responsibility for controlling and managing COMSEC assets in private sector companies, and for conducting security inspections of companies that have access to protected and classified information. PWGSC also gathers, analyzes, consolidates and facilitates the sharing (with OGDs) of operational threat and vulnerability information related to common IT services and government IT critical infrastructure managed by PWGSC. There are obvious cybersecurity aspects of this, but again PWGSC is not actually providing that security.

The Department of Foreign Affairs and International Trade (DFAIT) is responsible for ensuring the confidentiality, integrity and availability of official communications transmitted by electronic means between departments and Canadian diplomatic missions abroad and Library and Archives of Canada (LAC) is responsible for providing secure storage and management for the protection of the essential records of GC institutions during emergencies. These are both very narrow (although important) aspects of cyber security, and neither of these departments is primarily in the security business, so it is doubtful how much capability they actually have to provide the

[103] Canada. Policy on Government Security. July 1, 2009; available from http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?evttoc=C&id=16578&section=text; Internet; accessed 15 Jan 2010.

necessary security. In practice, they undoubtedly rely on the capabilities of other departments.

Others have even more limited and specialized responsibilities. For example Industry Canada has an Electronic Commerce Branch which is responsible for encouraging the development and adoption of e-business in Canada[104].

Generally however, the responsibilities of other federal institutions are limited to the safeguarding of private or sensitive information such as health records. This includes the Canada Border Services Agency (CBSA), Natural Resources Canada, Health Canada, Public Health Agency of Canada, and the Canadian Food Inspection Agency. None of these departments have the specialized capabilities needed to defend against a serious cyber attack.

4.2 Non-Federal Public Institutions

The January 2008 survey commissioned by the Canadian Association of Police Boards (CAPB) suggests in its summary that:[105]

- An unclear definition of cybercrime hinders their efforts to detect, deter and prevent it
- More dedicated resources are needed to increase the collaboration and coordination of stakeholders in the response to increasing the effectiveness of cybercrime prevention, detection, enforcement and prosecution.
- Timely and relevant changes to legislation are needed to address cybercrime issues.

This clearly indicates that the CAPB does not feel that it is adequately equipped to deal with cyber crime.

[104] Canada. “Industry Canada, The Digital Economy in Canada,” http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/home; Internet; accessed 8 April 2010.

[105] Canadian Association of Police Boards. *A Report on CyberCrime in Canada*, April 29, 2008. http://www.capb.ca/presentations.aro; Internet; accessed 11 February 2010.

4.3 Private Corporate Sector

Many of the Cybersecurity stakeholders, as previously illustrated in figure 3, are private corporate sector organizations. Virtually every business today has some "presence" in cyberspace, and relies to some extent on its secure operation. Many conduct their business in whole or in part over the Internet or use the Internet to improve their operation. Much of Canada's critical infrastructure is owned or operated by the private corporate sector[106], such as communications (telephone and wireless), transportation (trucking, shipping and rail), banking (personal and corporate), energy (petroleum, natural gas and electricity) and food (production, processing and retail), and many of these are vulnerable to cyber-attack. While they each have responsibility for ensuring the reliability of their own operations, they must realistically also rely to some extent on others who provide services to them. For example they all rely, to varying degrees on the corporate sector that produces the software and the devices which could have embedded exploitable vulnerabilities. These software producers must therefore also bear~~s~~ responsibility for eliminating these vulnerabilities to the extent practicable.

Most notable however are the Internet Service Providers (ISPs) themselves, who obviously rely for their existence on the Internet. They are not only vulnerable however, but also largely responsible for securing their service for their customers, which includes all other stakeholders. This starts at the top, with the Tier-1[107] and Tier-2 ISPs are major telecommunication companies who own and operate a significant portion of the high capacity, strategically interconnected physical networks and core routers that span individual countries or even the globe, and which carry the Internet (the "Internet

[106] Roughly 85% according to: Marina Rountree, Horizontality and Canada's Office of Critical Infrastructure Protection and Emergency Preparedness: a case study, (master's thesis, University of Manitoba, 2005), 4, available from http://mspace.lib.umanitoba.ca/handle/1993/172; Internet; accessed 10 May 2010. which cites the OCIPEP web site in 2004.

[107] A Tier 1 network is an Internet Protocol network that can reach every other network on the Internet without purchasing IP transit or paying settlements, by "peering" with every other Tier 1 network. A Tier 2 network is peer with some networks but must pay for access to others. A Tier 3 network is one that solely purchases transit from other networks to reach the Internet.

backbone”). Below these are many[108] thousands of Tier-3 ISPs who provide most of the “last-mile” connectivity to individual users. There are on the order of a dozen Tier-1 ISPs, about half of which serve North America (for example AT&T, Sprint, L3, Verizon). These are generally large multi-national corporations. Figure 4 illustrates the major components of one of these Tier-1 backbone segments as of June 2000 (owned by UUNET, which was subsequently acquired by Verizon).

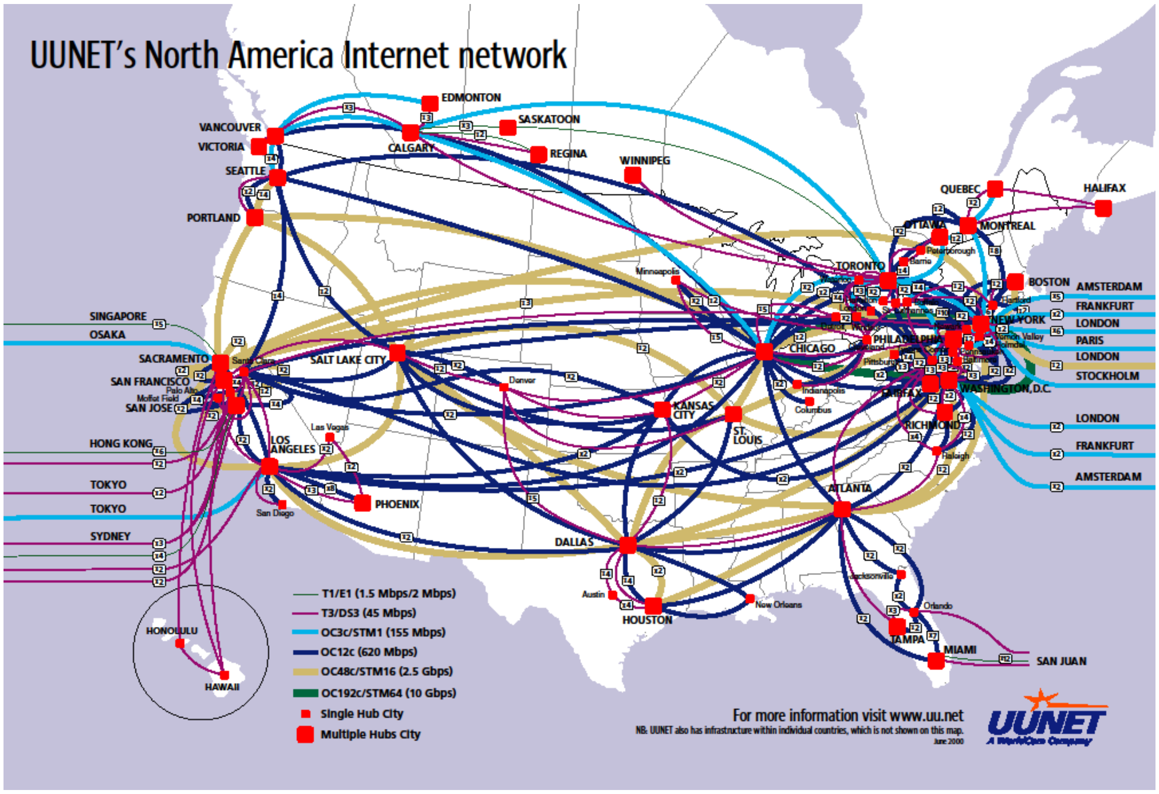


Figure 4. One Segment of Internet Backbone.

Jennifer Chandler argued in 2006 [109] that ISPs should share some legal liability to provide protection to their customers against certain types of cyber attacks. The argument is based on the fact that it is much more efficient to place cyber-security measures at the major nodes of the network (the ISP servers) rather than independently at

[108] About 23,000 as of January 2009, according to the Cooperative Association for Internet Data Analysis, University of California, San Diego, http://www.caida.org/research/topology/as_core_network/; Internet; accessed 10 May 2010.

[109] Jennifer Chandler, “Liability for Botnet Attacks”, *Canadian Journal of Law and Technology*, Vol 5, No 1, Mar-06

each endpoint. Interestingly, since 2006, Rogers Communications and Shaw Communications, the two major ISP providers in Canada, both improved their services by providing all of their customers with free Internet security software downloads. Chandler also argues that the application software vendors, whose products often have vulnerabilities that enable cyber attacks, should also have legal responsibility to ensure a reasonable level of security in their software products so that they cannot be easily exploited in this way.

Of course other elements of the telecommunications sector, who provide services to the ISPs, are also directly involved, being responsible for managing and safeguarding large components of the communications infrastructure that the Internet uses[110]. The financial sector and the health care sector, among others, have stewardship over substantial information storage that is critically important, sensitive and vulnerable to cyber attack. The software development sector has been hard at work developing and selling software tools designed to provide protection from cyber attacks.

In spite of best efforts, the private sector has been suffering significant losses as a result of cyberattack. As discussed in section 1.3, the US National Computer Security Survey in 2005 and the UN Commission on Crime and Criminal Justice survey in 1991 both found high levels of cybercrime incidents in the business and commercial sectors of the US, Europe and Canada. The Canadian Council of Better Business Bureaus estimates that in 2006 identity theft alone may be costing consumers, banks, credit card firms and stores more than $2 billion annually.[111] Of course it is the responsibility of businesses to protect customer information that is entrusted to them, and to take all reasonable precautions to reduce the risk of identity theft[112].

[110] Such as local exchange carriers, interexchange carriers (phone companies), data warehouses, domain name services, satellite communications, fibre-optic cables, telephone lines and switches etc.

[111] Canada. Department of Justice, http://www.justice.gc.ca/eng/news-nouv/nr-cp/2007/doc_32179.html; Internet; accessed 13 February 2010.

[112] Canada. Office of the Privacy Commissioner of Canada. http://www.priv.gc.ca/id/business_e.cfm; Internet; accessed 13 February 2010.

Given the growing occurrence of cyberattack, as described in chapter 2, clearly the private corporate sector is not doing an adequate job of defending itself against this threat. The private corporate sector therefore obviously has a major stake in this problem and shares some responsibility for dealing with it.

4.4 Private Citizens

Ultimately, individual citizens constitute the bulk of the users on the Internet. Since they are the ones in need of secure Internet access, it seems reasonable that individuals also share some of the responsibility for cyber security, particularly since many cyber attacks of national or regional significance (such as DDoS attacks) rely on the use of machines owned by private citizens. Unsecured machines (and private wireless networks) on the Internet are particularly vulnerable to highjacking, and other forms of malevolent exploitation. This makes them a hazard to other responsible users of the Internet. An important element of a layers approach to cybersecurity has to be basic security hygiene by individual users, such as the routine use of virus and spyware checking software, the use of a firewall and strong passwords and the regular practice of saving "back-ups" of their important data[113]. Individuals can therefore be part of the problem or part of the solution.

In January 2008, the Canadian Association of Police Boards (CAPB) commissioned a survey,[114] conducted by Deloitte LLP, to measure the magnitude and impact of cyber crime on Canadian private citizens. This survey had three components; a market research survey by Ipsos Reid of 587 Canadians, an interview process with 63 key contacts throughout law enforcement, prosecutions, industry, government and academia and finally an analysis of open source survey data. Key findings of the CAPB Cyber Crime in Canada report are:

[113] RCMP "Internet 101" website, http://www.internet101.ca/en/index.php; Internet; accessed 29 April 2010.

[114] Canadian Association of Police Boards. *A Report on CyberCrime in Canada*, April 29, 2008, Internet. http://www.capb.ca/presentations.aro, accessed 11 February 2010.

- 49% of respondents have been a victim of cyber crime.
- 86% of respondents indicate that cyber crime has become a concern.
- 95% of respondents believe they are being targeted for cyber crime.
- 89% of respondents believe that preventing cyber crime should be a priority of government and law enforcement agencies.

A recent text on "Digital Crime and Digital Terrorism" forecasts that "the number of offenses reported to police involving computers and electronic storage media will increase substantially" and that "the largest computer crime problem affecting local law enforcement representing the largest number of victims and the largest monetary loss will be Internet fraud, including fraud via identity theft".[115] Evidently private citizens are also not able to effectively defend themselves against cyberattack.

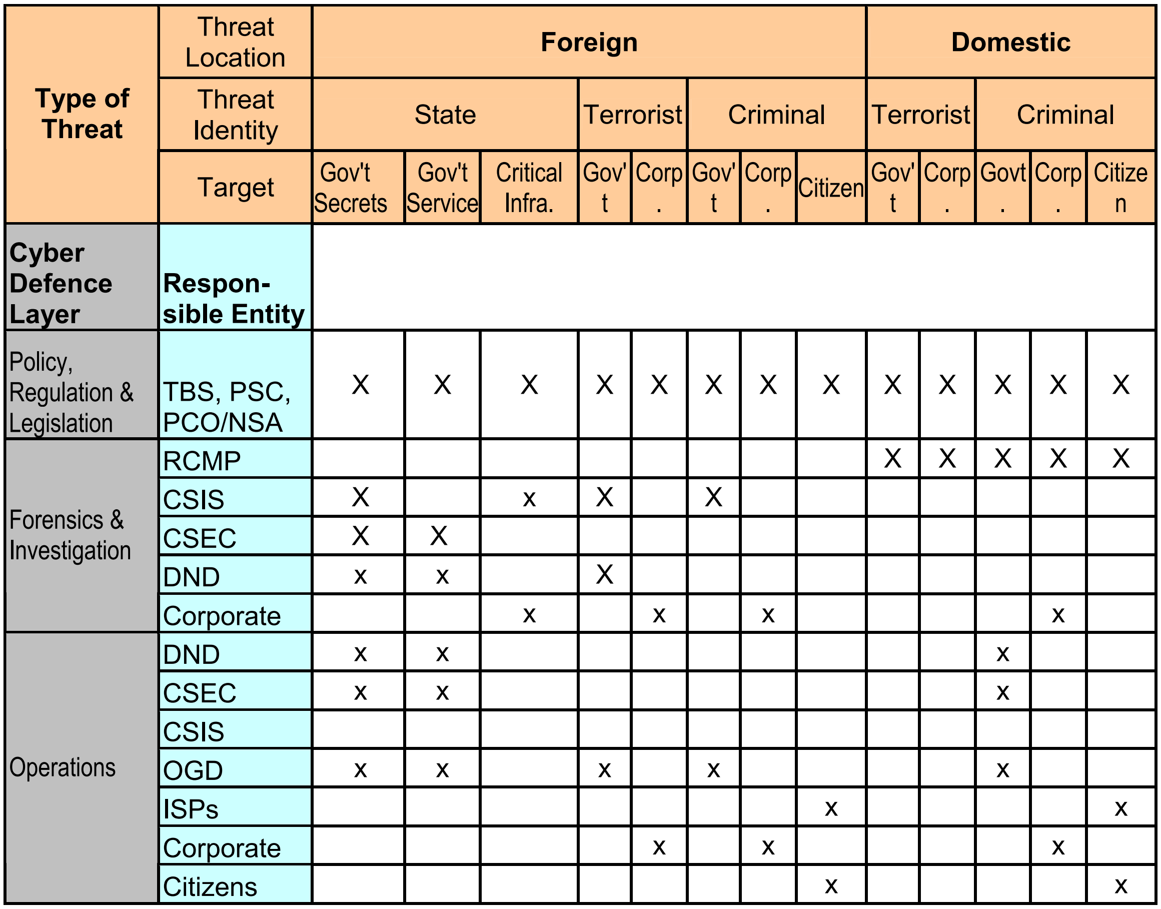
4.5 Summary of Canadian Efforts

Now after having considered in this chapter the responsibilities and abilities of all Canadian stakeholders to provide cyber security, we are in a position to verify the validity of the second part of the hypothesis has been established: that Canada is not adequately prepared to deal with the serious cyber-security challenge that it faces.

The table below attempts to illustrate, in a summary fashion, the different types of threat that Canada faces in cyberspace (as discussed in section 2.2), the types of security measures that would be needed to defend against them (the cyber defence layers as discussed in section 2.3) and the Canadian institutions that have responsibility to provide these needed defensive capabilities. This table is highly simplified, but illustrative of the type of analysis that would be needed to design a comprehensive solution to Canada's cybersecurity challenge. A cross has been placed wherever a threat is being addressed, at least to some extent, by a "responsible entity", as discussed above in this chapter (a small x indicates self-defence, and a large X if defence of others is included). To have a hope of being adequately secured, there should at least be a cross under each threat type for

[115] Robert W. Taylor, *et al*, *Digital Crime and Digital Terrorism*, (Upper Saddle River, New Jersey: Pearson Prentice Hall: 2006), 357.

each of the three cyber defence layers. This would indicate that someone is responsible, but not necessarily capable. As we can see, not even all responsibilities are covered.



Type of Threat	Threat Location	Foreign								Domestic				
	Threat Identity	State			Terrorist		Criminal			Terrorist		Criminal		
	Target	Gov't Secrets	Gov't Service	Critical Infra.	Gov't	Corp.	Gov't	Corp.	Citizen	Gov't	Corp.	Govt.	Corp.	Citizen
Cyber Defence Layer	**Respon-sible Entity**													
Policy, Regulation & Legislation	TBS, PSC, PCO/NSA	X	X	X	X	X	X	X	X	X	X	X	X	X
Forensics & Investigation	RCMP									X	X	X	X	X
	CSIS	X		x	X		X							
	CSEC	X	X											
	DND	x	x		X									
	Corporate			x		x		x					x	
Operations	DND	x	x									x		
	CSEC	x	x									x		
	CSIS													
	OGD	x	x		x		x					x		
	ISPs								x					x
	Corporate					x		x					x	
	Citizens								x					x

Table 1. Canadian Cybersecurity Responsibility Matrix

While this matrix omits considerable detail (particularly in the threat-space), is based entirely on unclassified information, and most importantly doesn't indicate how adequate the capabilities of the responsible entities are in each case, it seems clear even at this simplistic level that there are significant gaps in Canada's ability to provide cybersecurity, particularly in the critically important Operations layer. What is more, it illustrates some of the severe organizational fragmentation that exists in this domain.

To complete the picture, we would have to build a table showing the capability of each of these responsible entities to effectively carry out their responsibilities.

Unfortunately this information is not directly available, for understandable reasons: organizations are naturally reluctant to openly admit their shortcomings. However it is possible to deduce from the empirical evidence presented in chapter two (the serious impact that cyber insecurity is actually having in Canada), that those responsible for cybersecurity in Canada do not in fact have adequate capability (or capacity) to do so.

Of course, on top of these Canadian considerations is the international domain, where much of the threat originates and much of the defensive action would have to take place. This will be considered now in the next chapter, where we consider what other nations are doing, individually and collectively. Then it will remain to recommend a course of action, which is the subject of chapter six.

5 Other Nations and Multi-National Efforts

Before recommending a course of action for Canada, it will be instructive to examine briefly how two of Canada's closest and most advanced allies are approaching this problem. Then, given the dominant international aspect of the problem, it will also be important to explore multi-national efforts to cooperate.

5.1 Other Nations' Efforts

The UK has recently issued a *Cyber Security Strategy of the United Kingdom* with a principal aim being "to bring greater coherence to our cybersecurity work, by setting up two new organizations that will bring together the expertise and advice to meet this objective". [116] This document clearly recognizes the government's role in addressing this threat, and also accurately identifies the threat from other states, which are "seeking to exploit computers and communications networks to gather intelligence on government,

[116] "Cyber Security Strategy of the United Kingdom," Cm 7642, ISBN: 9780101764223, June 2009; available from http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf; Internet; accessed 15 January 2010. 4.

military, industrial and economic targets, and opponents of their regimes"[117] and that "some states also encourage, and benefit from, the expertise of "patriotic hackers" – enthusiastic individuals or groups of skilled hackers, carrying out attacks safe from prosecution in their own countries." This UK strategy document also makes the point that terrorists and violent extremists make extensive use of cyberspace to facilitate their activities. The response promised by the UK government will be to:

- Establish a cross-government programme
- Set up an Office of Cyber Security (OCS)
- Create a Cyber Security Operations Centre (CSOC), and
- Work closely with the Public Sector, Industry … and international partners.

The key aspect of this would seem to be the creation of the CSOC which will inter alia "provide collective situational awareness" and "improve technical response coordination to cyber incidents". This multi-agency body will bring together a number of existing organizations from across government and key stakeholders, to enable a fully integrated defensive posture. This is intended to unify the effort that is currently distributed across various UK stakeholders, including the Home Office, the Police, the Centre for the Protection of National Infrastructure, and the organization responsible for cybersecurity for the public sector.

This clearly demonstrates the recognition of cybersecurity as a government responsibility, and the recognition that a single integrated operations centre is needed to provide that security. It would appear therefore, that at least the UK is in the process of becoming prepared for Cybersecurity. To deal adequately with the transnational aspects however, would require that other nations follow suit, providing strong national entities that could then begin to develop means of cooperating with each other

Similarly, the US DoD appears to have taken decisive measures by establishing a Cyber Command, when on 23 June 2009 U.S. Defense Secretary Robert M. Gates issued a directive "Establishment of a Subordinate Unified U.S. Cyber Command under U.S.

[117] Ibid., 13.

Strategic Command for Military Cyberspace Operations."[118] This Cybercom will be a subunit of the U.S. Strategic Command and will be commanded by the director of the National Security Agency.

For the non-military aspects, in December 2009 the US president appointed Howard Schmidt to be his “Cyber Czar”, to coordinate competing efforts to improve the nation’s cybersecurity in both military and civilian life and to harmonize the nation’s various efforts to “deter, prevent, detect and defend” against cyberattacks. Schmidt will report to the National Security Council.[119]

5.2 Multi-National Efforts

Since cyber threats are often transnational, one could argue that it requires a transnational response. One of the fundamental obstacles to Cybersecurity, as explained in chapter 3 above, is that incidents often span national jurisdictions, so that the victim, threat vector, and perpetrator are often not within the same nation. This suggests three possible approaches to transnational cyber crime. The first approach would be for all nations to vigorously police their own internal cyberspace in an attempt to prevent malicious activity of all types. The second approach would be for all nations to agree on the creation of an international authority to police all of cyberspace for them. The third approach would be for all nations to cooperate closely in policing the “cyber commons” (in conjunction with policing their own nation to their best ability).

The first approach alone is highly unlikely to be effective for two reasons: firstly because of the large “digital divide” that currently separates the cyber maturity of the developed world from the developing world, which leaves many countries unable to police their cyberspace at all; and secondly because of the inherent difficulty of nation detecting a cyber attack that originates from within that nation but is directed at a target

[118] Robert M. Gates, US SECDEF Directive 05914. http://publicintelligence.net/establishment-of-a-subordinate-unified-u-s-cyber-command/; Internet; accessed 15 February 2010.

[119] John Markoff, “Obama to Name Chief of Cybersecurity”, *New York Times*, 21 December 2009.

in another nation. Because of the nature of the connectivity in cyberspace[120], it doesn't appear to be feasible for nations to individually provide for their own security at their borders (or in the "between-states" space), as is done for most crime, since there is no such space in the cyber domain.

The second approach is highly unlikely to be acceptable to most nations, because of the relinquishment of sovereignty that it implies, to say nothing of the contentious questions of locating and financing such an organization.

Thus the only practical approach is the third, which in some sense is simply a combination of the first two. This section will explore the extent to which these approaches are being pursued, and the adequacy of the resulting effort, from a Canadian perspective.

In the international realm, there are three basic lines of attack that must be pursued to mount an effective defence against transnational cyber crime and cyber terrorism: regulatory, legal and institutional.

In the regulatory domain, the International Telecommunications Union (ITU) has examined this issue at its recent meeting (July 2009, Geneva) and issued a Resolution on Cybersecurity that recognized its importance and itemized a long list of vulnerabilities, including new and growing threats, as well as many technical measures that should be taken to address them.[121] This certainly indicates that the international standards community believes that the Cybersecurity threat has not yet been adequately addressed, but they are working hard at it and making progress.

[120] Because of the packet-switching technique used over the internet, and the extensive web of transnational communications connections, it is not generally feasible to intercept a message while it travels between states, since it may have been broken down into packets which are sent over different paths.

[121] International Telecommunications Union. "Resolution GSC-14/11: (GTSC) Cybersecurity (Revised)" http://www.itu.int/ITU-T/gsc/gsc14/documents.html; Internet; accessed 15 February 2010.

On the institutional front, efforts to cooperate internationally on cybersecurity have been rather limited to date, but they are accelerating. In response to the serious cyber attack on Estonia in 2007, NATO conducted an assessment of its approach to cyber defence, which led to the development of a NATO cyber defence policy which was adopted in January 2008. This also resulted in the creation of a Cyber Defence Management Authority (CDMA) and the signing of several MOUs to create a legal framework for cyber defence cooperation between NATO and several member states, including (as of 23 April 2010) Estonia. Perhaps more significantly, it has also led to the creation of a Co-operative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia, and the establishment of a NATO Computer Incident Response Capability (NCIRC), which will have a key role in responding to any cyber aggression against the Alliance. NCIRC is intended to have several capabilities:

- NATO-wide response coordination during an incident
- Central knowledge base to support local System Administrators
- Centralized on-line and on-site services
- Centralized forensic and LE support arrangements
- Optimization of resources
- Contacts with external CERTs/CSIRTs[122]

However, as of May 2010, NCIRC is in the first phase of implementation, with an interim capability only.[123] In any case, these are largely information sharing and coordination functions, rather than cyber defence operations, and are of course restricted to NATO nations.

At the broader international level, such as the UN, no such body, agency or mechanism currently exists to ensure transnational cyber security. While attempts have been made to develop a UN cyber-crime treaty, this effort was defeated as recently as 20 April 2010, because of a preference by the US and UK to use the convention that was

[122] Suleyman Anil, Presentation at 2004 TF-CSIRT meeting, available at www.terena.org/activities/tf-csirt/meeting11/NCIRC-Anil.pdf; Internet; accessed 20 May 2010, 5.

[123] NATO web site. http://www.nato.int/cps/en/natolive/topics_49193.htm; Internet; accessed 29 April 2010.

introduced by the Council of Europe in 2001 (discussed further below).[124] The only relevant global mechanism that is in place is the UN Convention against transnational organized crime (the TOC Convention).[125]

The first effort to achieve such a multi-lateral legal agreement is the Council of Europe (CoE) Convention on Cybercrime[126] of December 2001, which was activated in 2004. This convention aims to harmonize cybercrime legislation among nations (by providing common definitions of cyber-crimes), and to speed up investigation and prosecution by dealing with international cooperation in law enforcement through extradition and through acquisition and preservation of data for cross-border investigations. On the surface, this seems to deal with many of the Cybersecurity challenges described in chapter three.

Unfortunately, according to Kierkegaard of the International Association of IT Lawyers, this effort was conducted without the help of legal experts or human rights advocates[127], and:

> Many think the problems prompted by the borderless Web eventually could be resolved by a treaty, but with the conundrum posed by the CoE cybercrime treaty, it is anyone's guess.[128]

The conundrum referred to here arises because of the substantial surveillance and enforcement powers that the treaty bestows upon governments, which in the hands of a despotic country could represent a risk to privacy and other human rights. The author is therefore advocating more safeguards.

[124] Mark Ballard. "UN rejects international cybercrime treaty", *ComputerWeekly*, 20 April 2010, http://www.computerweekly.com/Articles/2010/04/20/240973/un-rejects-international-cybercrime-treaty.htm; Internet; accessed 29 April 2010.

[125] Roderic Broadhurst, "Developments in the global law enforcement of cyber-crime," *Policing: An International Journal of Police Strategies & Management*, Vol 29 no. 3 (2006): 408-433.

[126] Sylvia Mercado Kierkegaard, "International Cybercrime Convention", in *Cyber Warfare and Cyber Terrorism*, edited by Lech J. Janczewski and Andrew M. Colarik, 469-476. (Hershey, New York: Information Science Reference, 2008), 469.

[127] Ibid. 472.

[128] Ibid. 475.

As of March 2010 there were only 27 states which had ratified it (including the US). Canada, although a signatory, and contributor to its creation, is not yet among them.[129]

The conclusion here is that the current international cyber-security regime is not yet sufficiently mature to provide adequate protection for Canada and Canadians from cyber threats originating outside Canada. To reach an acceptable state will require active Canadian involvement in international negotiations, from informed and empowered representatives who can accurately represent the many complex needs and concerns of all Canadian stakeholders, and gain the support from these Canadian stakeholders to uphold our end of whatever bargain is reached (since other international stakeholders will have their own concerns that will undoubtedly require action and commitment on our part).

Another important thing to note is that these international efforts are simply regulatory and legal, to allow better coordination among national cyber-security efforts: there are no integrated or even coordinated forensic, investigative or operational level efforts to actively provide defensive measure in the international domain (with the possible exception of the limited effort within NATO NCIRC, as discussed above, which is also intended to have forensic capabilities when it reaches full operational capability).

6 Options and Recommendations

From chapter five above, we can see that no single entity or collective has the authority or the ability to provide cybersecurity for Canada today. The question becomes: how to ensure that this function is performed? To address this we will first consider the strategic level question of what principles to apply when deciding how this function should be performed, and then we will consider the operational level question of how these principles apply specifically to the Canadian situation.

[129] Council of Europe web site, http://www.coe.int/t/dc/files/themes/cybercrime/default_EN.asp; Internet; accessed 22 March 2010.

6.1 Strategic Options

At the highest level, or the strategic level, one framework that can be used to examine what is needed to accomplish a mission is the command and control framework. For example the Pigeau and McCann model could be applied to deduce that in order to provide effective cybersecurity a person or organization must have an adequate amount of the following three things (the three dimensions of command[130]):

1. The authority (legal/legislative) to do it,
2. The capability (human and materiel resources) to do it, and
3. The responsibility (desire/will) to do it.

Since the need for cybersecurity is such a new requirement, Canada has not yet fully organized itself to provide it. When a new requirement arises for a function to be performed (the desire/will to perform it exists), and no single existing organization has all three requirements above needed to perform it alone, there are 3 basic options at the strategic level:

1. Leave the function undone (i.e. do nothing and accept the risk).
2. Assign the function to a single organization, either newly created or existing, and providing that organization with all necessary authorities and capabilities to ensure that the function is performed.
3. Assign several existing organizations the task of collectively ensuring that the function is performed, by coordinating amongst themselves.

Option 1 will not be acceptable if the requirement is sufficiently important. The evidence presented in chapters one and two suggests that cybersecurity is too important to ignore. The basic choice therefore, is to either create an *integrated* capability, or a *distributed* (coordinated) capability. As explained in chapter four, Canada has to date chosen the third option, more by default than by design, since several existing organizations already had evolved to assume partial responsibility. Since this approach is

[130] Ross Pigeau and Carol McCann, “Re-Conceptualizing Command and Control.” *Canadian Military Journal* 3, no. 1 (Spring 2002) (57).

showing signs of inadequacy, the argument here is that this "decision" deserves a serious re-evaluation, and the suggestion will be that Canada does need a much more integrated capability.

Before examining this more closely, it will be instructive to briefly consider precedents. What has been the historic response of the government of Canada to emerging requirements? In 1879 Canada created a federal Department of Railways and Canals[131], in 1907 Canada created the Department of Mines, and in 1960 the Department of Forestry.[132] Each of these was created when the need arose, and dissolved or evolved when the need changed (today not one of them exists as such).

More recently, and perhaps more relevant, is the US response to the events of 9/11, which revealed a new requirement for enhanced homeland security. In this case the US government responded by choosing option 2 and creating a new US federal department (DHS). [133]

Ample examples can also be found within DND, where new dedicated organizations have been stood up to deal with new or newly perceived requirements, whether they are designed to be short lived, such as Joint Task Force Games to help secure the 2010 Winter Olympics, or to be permanent, such as Canada Command, to oversee domestic and continental operations.

Turning back to the current case of cyber security, in evaluating options 2 and 3 consideration must first be given to the viability of each option, then to their efficiency (cost) and their effectiveness.

[131] Canada. "National Archives General Guide Series: Government Archives Division." Ottawa: National Archives of Canada, 1991, available online: http://www.trentu.ca/admin/library/archives/72-1003.htm, Internet. Accessed 7 April 2010.

[132] Canada, NRCan website; http://www.nrcan.gc.ca/com/deptmini/histhist/evoevo-eng.php; Internet. Accessed 7 April 2010.

[133] William J. Olson, "Interagency Coordination: The Normal Accident or the Essence of Indecision", in *Affairs of State: The Interagency And National Security,* ed. Gabriel Marcella, 215-254 (Carlisle, PA: Strategic Studies Institute, Army War College, December 2008), 221.

For option 3 to be viable, one would have to decompose the new function into components (sub-functions) and enable each organization to perform one or more component by re-arranging their authorities and capabilities. The degree to which this can be done depends on the degree to which the function can be decomposed into independent sub-functions, and the degree to which different government or private organizations can coordinate their efforts.

6.2 Operational Options

For this new Cybersecurity challenge, the Canadian government, as described in chapter 4 above and illustrated in Figure 1, has been relying upon the third highly distributed approach. This approach is not working particularly well, as can be judged from the empirical evidence of continuing incidents of cyber crime and cyber terrorism, as described in chapter 2. We should hasten to add that this does not imply incompetence or lack of effort on the part of the institutions currently involved. Rather it is the potential for this overall approach to work in the future, as currently organized, which is at the core of the final question to be addressed by this paper. Chapter 3 described some specific obstacles, mostly related to jurisdictional ambiguity. This jurisdictional ambiguity can only be resolved by introducing a fundamental change in the manner in which authorities and responsibilities are assigned to the organizations that currently share responsibility for cyber security.

In order to decide how many and what type(s) of organization(s) Canada needs to ensure an acceptable level of Cybersecurity, the adage “form follows function” suggests that one must first consider the functions to be carried out. Table 1 in chapter 5 above illustrates one attempt to break down the many functions. From this table we see that the only institutions within Canada that have authorities, responsibilities and capabilities to conduct operational level defence (other than self-defence) in cyberspace are DND, CSEC and the ISPs. While there are many other stakeholders, as illustrated below, their responsibilities are in the policy, regulative, legislative or investigative domains.

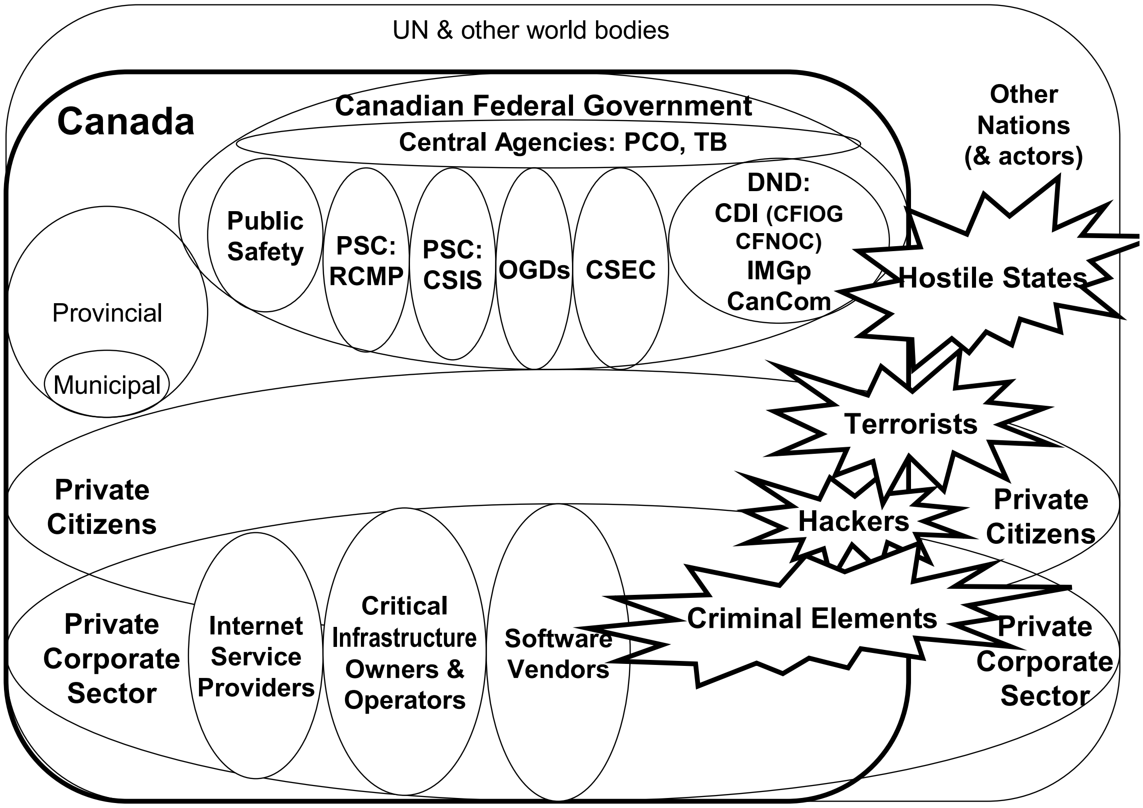


Figure 5. All Stakeholders Who Share Responsibility for Canadian Cyber Security.

This suggests that from an operational perspective, the organizational options to be considered should focus on these three stakeholders.

6.3 Option Analysis

Performing a proper options analysis that evaluates the relative merits of assigning full authority, responsibility and capability to one or more of the current stakeholders, or to a completely new organization, would require the use of considerable classified information. Unfortunately that is beyond the scope of this paper. However some broad comments can be made, which point decidedly in a particular direction. First we can draw upon the published recommendations of several informed commentators, and interpret them within the framework that has been established herein.

In October 2009 Rodney Joffe, senior Vice President and Senior Technologist at NeuStar (a US company that provides various technology services to ISPs), recommended a three-pronged approach[134]:

1. Acknowledge that cyber crime is truly an epidemic by better educating the public.
2. Encourage co-operation between government and private industry, such as providing public funds for ISPs to isolate customers whose machines have been compromised, and establishing a collaborative infrastructure to enable all stakeholders to share information and coordinate defensive measures.
3. Make carefully considered changes to our laws, which are woefully inadequate and don't recognizing the global nature of cyber crime (some recent legislative remedies have actually been counterproductive[135]).

Jeanne Giraldo and Harold Trinkunas (of the Naval Postgraduate School, Monterey, USA), in their analysis of transnational crime[136] suggest that, short of militarization, one option is greater cooperation between law enforcement and national intelligence assets. They also raise the option of greater prevention measures, in terms of capacity building to strengthen the rule of law and law enforcement agencies in the emerging states. While these are laudable goals, and they may be a reasonable approach for dealing with prosecution of common cyber criminals, it does not begin to address the problem of actively defending against a serious cyber attack in progress, and is difficult to imagine how it could deal with a concerted state-on-state attack, unless one of these agencies (law enforcement or national intelligence) was also given the authority and capability to conduct an active defensive operation.

Another lengthy analysis of cyber crime and cyber terrorism gives a similar prescription for dealing with cyber crime:

> …problems related to cybercrime demand attention from a wide variety of groups outside of traditional law enforcement, including

[134] Rodney Joffe, "The cyber crime epidemic; Terrorists and rogue states are moving their battle to the Internet. How do we fight it?" National Post, 23 October 2009.

[135] For example a rule enacted by parliament that criminalizes the placement and execution of computer programs on a computer without the owner's permission also blocks the ability of authorities from releasing countermeasures to disable malicious software.

[136] Jeanne Giraldo and Harold Trinkunas, "Transnational Crime", in *Contemporary Security Studies*, ed. Alan Collins, 346-366, (Oxford: Oxford University Press, 2007), 364

> consumers, businesses, privacy advocates, and national security interests. Both the public and private sector have a role to play in fighting cybercrime. … Clearly the need for collaboration and cooperation across different types of public agencies…[137]

However, in their chapter on cyber terrorism there is no such solution proposed, which suggesting that they did not believe the same approach would be adequate.

According to the former director of the United States' National Security Agency Mike McConnell (currently executive vice president of Booz Allen Hamilton, which consults on cybersecurity):

> We need to develop an early-warning system to monitor cyberspace, identify intrusions and locate the source of attacks with a trail of evidence that can support diplomatic, military and legal options -- and we must be able to do this in milliseconds. More specifically, we need to reengineer the Internet to make attribution, geolocation, intelligence analysis and impact assessment -- who did it, from where, why and what was the result -- more manageable.[138]

The identified need to be able to react "in milliseconds" certainly seems to advocate a very tightly integrated defensive mechanism.

One common feature of all of these recommendations is the need for very tight cooperation and collaboration across public and private sector stakeholders. As discussed in chapter five, the US and the UK governments have also expressed the same intention in their cyber strategies, but have gone further by establishing new entities with more comprehensive authorities, responsibilities and capabilities. It will be argued here that the reason why the US and the UK chose to centralize these functions, is that there are very serious limits to how much coordination can be achieved among disparate

[137] Robert W. Taylor, *et al*, *Digital Crime and Digital Terrorism*, (Upper Saddle River, New Jersey: Pearson Prentice Hall: 2006), 274. (a textbook written by a number of professors at the University of North Texas).

[138] Mike McConnell. "Mike McConnell on how to win the cyber-war we're losing", *Washington Post*, 28 February 2010.

organizations. This argument also applies to Canada, which leads to the recommendations of the next section.

Even with the best of intentions, there are fundamental limits to the amount of coordination that can be achieved in attempting to solve complex problems such as cyber security. In fact Professor William J. Olson at the National Defence University goes so far as to argue that relying on this will lead to failure. He identifies many obstacles to inter-agency coordination when attempting to manage a complex operation:

- Complexity defies logical analysis and cognition, which prevents coherent coordination.
- "Everyone wants coordination but no one wants to be coordinated."
- Coordination imposes a cost.
- Agencies tend to consider coordination as a form of or cover for control (especially if one organization has disproportionate power and size).
- Coordination introduces a time lag. More coordination means more time lags.
- Coordination places constraints on the independence of action needed by local responders in demanding, changing circumstances.
- Coordination tends to only be considered at the last minute: at the operational level (not policy, doctrine, training, planning, force development etc.)
- Coordination can take place at different levels within the organization, from tactical to operational to strategic, but coordination at one level does not translate into coordination at the other levels.
- Technical challenges also impede coordination, such as incompatible communication capabilities. [139]

What Olson advocates (in the context of the US DoD requirement to be able to conduct effective joint operations), is wholesale reorganization, (in the form of a "new National Security Reorganization Act, similar to the 1947 effort"[140] which created the DoD among other things, before which the services had been separate institutions). He states that "such solutions as there are do not lie in piecemeal reorganizations or bureaucratic reforms".

[139] William J. Olson, "Interagency Coordination: The Normal Accident or the Essence of Indecision", in *Affairs of State: The Interagency And National Security,* ed. Gabriel Marcella, 215-254 (Carlisle, PA: Strategic Studies Institute, Army War College, December 2008), 224-235.
[140] Ibid., 250.

This leads to a number of recommendations for the Canadian government.

6.4 Recommendations

Based upon the limited analysis above, it seems clear that a national agency is needed to provide, in an integrated manner, an effective operational defence of cyberspace for Canadians. Ultimately this argument can also be extended to the international realm, but this does not relieve us of our domestic responsibility to provide whatever protection is feasible.

While some of this can be distributed, with ISPs providing a layer of defence for their customers, and with corporate and individual users also being required (and enabled) to provide a layer of defence for themselves, we will ultimately need a single centralized agency to coordinate defence against the most serious attacks, such a DDoS attacks. This central agency should have broad responsibility and authority to provide some defence for all vulnerable users in Canada, including not only government but also corporate and private users. It should also be given the necessary capability to perform this function. Whether this agency should be completely independent or attached to a current stakeholder, such as DND, CSEC or Public Safety Canada, is a question that requires a more complete analysis. It is recommended that this more complete analysis be conducted, with full access to classified information on all cyber threats and all Canadian Stakeholder capabilities. This should aim to first establish a more complete taxonomy of threats and stakeholders, similar to that used in Table 1, and it should then create the corresponding table of Canadian Cybersecurity Capabilities. This table would no doubt have far more empty spaces than Table 1 has, within all three cyber defence layers. As was discussed in chapter 3, Canada does not have jurisdiction over many of the threats, so our ability to investigate and do forensic analysis will be severely limited without an international regime. Similarly our ability to effectively regulate and legislate in the international domain is severely limited. Our operational capability would appear to be inadequate, but only an in-depth look at the classified level would reveal the extent and nature of this deficiency.

It is also recommended that, in parallel with the analysis discussed above of our domestic capability, a similar all-of-government analysis of the international options be conducted, with participation from the public and the private corporate sector as well. There are serious public policy questions that will have to be addressed, not the least of which is the right to privacy.

Given the accelerating pace of change in the CIT domain, it is further recommended that these requirements analyses be regularly revisited. The cyber domain is really still an emergent domain, much as manned flight was in the days of bi-planes, and it is therefore anticipated that keeping pace with the security requirements in cyberspace will be a challenging endeavour.

7 Conclusion

In chapter one we saw how real our vulnerability is to cyber crime and cyber terrorism, with personal security, national security and economic prosperity at risk, and in chapter two we saw how serious the threats are (such as identity theft, critical infrastructure disruption, intellectual property theft, financial crimes, etc.).

Since cyber-security encompasses such diverse threats as espionage, identity theft, financial theft, organized crime, terrorism and hostile attacks on national critical infrastructure, the responsibility to defend against and respond to these threats is shared among many institutions, which in Canada span the federal, provincial, municipal levels of government, and may have a significant transnational element. As we have seen in chapter three, there are some fundamental reasons why the creation of geographic and functional jurisdictions, which helps simplify the task of dealing with other threats, does not fit the cyberspace paradigm, and in fact causes serious challenges to effective defensive operations in this domain.

In chapter four we examined the mandates of the various institutions that might be able to provide Canadian cyber security, and found that none of them in fact are equipped with the operational responsibility to provide comprehensive cybersecurity for Canada, and certainly none of them has the technical capability to do so. Attempts to coordinate actions among these organizations are severely constrained by the laws and regulations that have been put in place over the years to keep their jurisdictions separate. As we saw, the Auditor General has suggested that the federal bureaucracy is not prepared, and the Canadian Association of Police Boards is quite clear in stating that they are not.

In chapter five we briefly considered the international dimension of this problem, and saw that some leading nations are taking serious measures to secure their citizens in cyberspace, but that the multi-lateral international effort to put in place the necessary global framework is less advanced.

Options for Canada were then outlined and analysed, to the extent possible, in chapter six, which led to a number of recommendations.

The inescapable conclusion is therefore that the hypothesis stated at the beginning is correct: cyber-crime, together with the closely related cyber-terrorism, is a serious security challenge for Canada, and Canada is not yet well prepared to handle it. The federal government has, and has always had, an important role to play in regulating and protecting vital national interests. These interests evolve, and the organization of the government institutions has evolved to meet the needs of the day. The evidence presented here would suggest that the time has come for the federal government to stand up a major new capability to secure the safe and reliable access to the Internet for Canadian citizens, the Canadian government, and the Canadian private corporate sector. Given the limits to which independent organizations can coordinate their activities, and given the complexity and speed of the threats to cyber security, it would seem that a single organization will have to be given the authority, responsibility and capacity to lead the effort, but will also rely on other stakeholders to add their layers of defence as appropriate.

While prescribing an international solution is beyond the scope of this paper, it seems clear that one aspect will have to be a further erosion of national Westphalian sovereignty, as was alluded to in the first chapter. This is simply because, as discussed in chapter three, most transnational criminals and terrorists will attempt to take advantage of states that are unwilling or unable to prosecute them by using these states as a "safe haven" from which to conduct their hostile activities. The first imperative is therefore to eliminate these safe havens for cyber criminals, by introducing cyber crime into international law, and providing an enforcement mechanism. The second imperative is to provide legal mechanisms for an attacked state to prosecute a cyber criminal from an attacking state. A third measure, to address state-on-state attacks, is to recognize state-sponsored cyber-attack as an act of war, so that sanctions can be applied.

In general then, international laws will have to be developed to allow cross-jurisdictional action in this domain, which of course is yet another erosion of Westphalian sovereignty. This will not be the first such erosion[141] and it probably won't be the last, as technology driven globalization continues inexorably.

What are the prospects for these recommendations to be implemented? Is the policy window of opportunity closing? Is the lack of a transformative metaphor for cybersecurity in the public psyche preventing political action? Will it take a catastrophic disaster to galvanize our leaders into action? Only time will tell, and that time could be soon.

[141] Maogoto, Jackson Nyamuya, Transforming Westphalian Sovereignty: Human Rights & International Justice as a Transitional Crucible. Notre Dame Law Review, Vol. 7, 2005. Available at SSRN: http://ssrn.com/abstract=901224; Internet; accessed 15 February 2010.

Appendix 1: List of Acronyms

AG	Auditor General
CAPB	Canadian Association of Police Boards
CBSA	Canadian Border Services Agency
CCIRC	Canadian Cyber Incident Response Centre
CCDCOE	Co-operative Cyber Defence Centre of Excellence (NATO)
CDMA	Cyber Defence Management Authority (NATO)
CIO	Chief Information Officer
CNCI	Comprehensive National Cybersecurity Initiative (US)
CPNI	Centre for the Protection of National Infrastructure (UK)
CSEC	Communications Security Establishment Canada
CSIS	Canadian Security Intelligence Service
DoS	Denial of Service
DDoS	Distributed Denial of Service
GC	Government of Canada
GOC	Government Operations Centre
ICT	Information and Communication Technology
IM	Information Management
IP	Intellectual Property
IPv6	Internet Protocol version 6
ISACC	ICT Standards Advisory Council of Canada
IT	Information Technology
ITU	International Telecommunications Union
LOAC	Law of Armed Conflict
NCIRC	NATO Computer Incident Response Capability
NSA	National Security Advisor
PCO	Privy Council Office
PS	Public Safety Canada
SCADA	Supervisory Control And Data Acquisition
TBS	Treasury Board Secretariat
TF-CSIRT	Task Force - Computer Security Incident Response Teams
TOC	Transnational Organized Crime
WAN	Wide Area Network
WoG	Whole of Government

Appendix 2: Definitions[142]

BotNet: of vast networks of compromised or 'zombie' machines that can be used for malicious purposes, such as stealing information (eg. gathering credit card numbers by 'sniffing' or logging the strokes of a victim's keyboard) or for the delivery of malware or DDdoS attacks.

Denial of Service (DoS) Attack: a malicious attempt to disrupt the operation of a computer system or network that is connected to the Internet. The most common form of attack is one which disrupts the operation of the computer system or network by consuming the bandwidth of the victim network or overloading the computational resources of the victim system.

Distributed Denial of Service (DDoS) Attack: a more dangerous, evolved version of a DoS attack, which uses a network of compromised 'zombie computers' (a BotNet) to mount the attack, so that there is no identifiable single source (which could otherwise be defended against with a simple filter).

Hacking: an individual attempting to 'get into' your computer systems for personal use. Hackers have a range of motives; from showing off their technical prowess, to theft of money, credentials or information, or simply to cause damage. There are many hacking tools available on the Internet as well as online communities actively discussing hacking techniques enabling even unskilled hackers to break into unprotected systems.

Malware: (malicious software) any program or file that is harmful to a computer (such as viruses, worms, Trojan horses, spyware etc.)

Phishing: the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Typically using email or instant messaging to direct users to a fake web site.

[142] Adapted from the websites of Wikipedia, http://en.wikipedia.org/wiki/Main_Page and the Centre for the Protection of National Infrastructure, http://www.cpni.gov.uk/default.aspx.

Pinging: a simple form of denial-of-service attack, in which the attacker overwhelms the victim by bombarding it with ICMP (Internet Control Message Protocol) echo request packets. In legitimate use, such a request (a 'ping') is a computer network administration utility used to test whether a particular host is reachable across an Internet Protocol (IP) network and to measure the round-trip time for packets sent from the local host to a destination computer, including the local host's own interfaces.

Port Scanning: is a software application designed to probe a network host for open ports. This is often used by administrators to verify security policies of their networks and by attackers to identify running services on a host with the view to compromise it.

Spoofing: a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.

Spyware: malware that is installed on computers and collects little bits of information at a time about users without their knowledge. Typically, spyware is secretly installed on the user's personal computer. Sometimes, however, spywares such as keyloggers are installed by the owner of a shared, corporate, or public computer on purpose in order to secretly monitor other users. Spyware is also known to change computer settings, resulting in slow connection speeds, different home pages, and/or loss of Internet or functionality of other programs.

Trojan Horse: any apparently innocent document or program that has hidden malicious (but non-self-replicating) code imbedded in it. Once installed, they can be used to remotely collect information (such as usernames and passwords), to upload documents and data, to download other malware, or to relay further attacks against other computers (creating a BotNet).

Virus: Sometimes used to refer to any malware, or computer program that can copy itself and infect a computer. A true virus can only spread from one computer to another (in some form of executable code) when its host is taken to the target computer; for instance because a user sent it over a network or the Internet, or carried it on a removable medium. Viruses can increase their chances of spreading to other computers by infecting files on a network file system or a file system that is accessed by other computers.

Worm: a self-replicating malware computer program which uses a computer network to send copies of itself to other computers on the network. Unlike a virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

Bibliography

1. Anil, Suleyman. Presentation at 2004 TF-CSIRT meeting, available at www.terena.org/activities/tf-csirt/meeting11/NCIRC-Anil.pdf; Internet; accessed 20 May 2010.

2. Ballard, Mark. "UN rejects international cybercrime treaty", *ComputerWeekly*, 20 April 2010, http://www.computerweekly.com/Articles/2010/04/20/240973/un-rejects-international-cybercrime-treaty.htm; Internet; accessed 29 April 2010.

3. Broadhurst, Roderic. "Developments in the global law enforcement of cyber-crime," *Policing: An International Journal of Police Strategies & Management*, Vol 29 no. 3 (2006): 408-433.

4. Bull, Hedley, *The Anarchical Society, A Study of Order in World Politics*, London: The Macmillan Press Ltd., 1977.

5. Canada. *Canada First Defence Strategy*. available from http://www.forces.gc.ca/site/pri/first-premier/index-eng.asp; Internet; accessed 15 February 2010.

6. Canada. CSIS web site. http://www.csis-scrs.gc.ca/prrts/index-eng.asp; Internet; accessed 31 December 2009.

7. Canada. "CSIS Public Report 2007-2008". Available from http://www.csis-scrs.gc.ca/pblctns/nnlrprt/index-eng.asp; Internet; accessed 16 February 2010.

8. Canada. Department of National Defence. B-GJ-005-300/FP-000 *Canadian Forces Operations*. Ottawa: DND Canada, 2004.

9. Canada. *Policy on Government Security*. July 1, 2009; available from http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?evttoc=C&id=16578&section=text; Internet; accessed 15 Jan 2010.

10. Canada. *Securing an Open Society: Canada's National Security Policy;* available from http://www.pco-bcp.gc.ca/docs/information/Publications/natsec-secnat/natsec-secnat-eng.pdf; Internet. accessed 13 February 2010.

11. Canada. Treasury Board Policy Suite. "Policy on Government Security"; available from http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?evttoc=C&id=16578&section=text; Internet; accessed 15 January 2010.

12. Canadian Association of Police Boards. *A Report on CyberCrime in Canada*. (April 29, 2008); available from http://www.capb.ca/presentations.aro; Internet; accessed 11 February 2010.

13. Canadian Association of Police Boards. *A Report on CyberCrime in Canada*, April 29, 2008. http://www.capb.ca/presentations.aro; Internet; accessed 11 February 2010.

14. Carter, D.L. and Katz, A.J.. "Computer Crime Victimization: An Assessment of Criminality in Cyberspace". *Police Research Quarterly* vol. 1, no.1,1998.

15. Carvalho, Ferdinand Duarte and Eduardo Mateus da Silva editors, *Cyberwar-Netwar, Security in the Information Age*, NATO Security through Science Series, IOS Press, Amsterdam, Netherlands, 2006.

16. Castells, Manuel. *The Information Age: Economy, Society & Culture, Volume I: The Rise of the Network Society*, Malden, MA: Blackwell Publishing, 2000.

17. Centre for the Protection of National Infrastructure website: http://www.cpni.gov.uk/default.aspx.

18. Chandler, Jennifer. "Liability for Botnet Attacks", *Canadian Journal of Law and Technology*, Vol 5, No 1, March 2006.

19. Coulondre, Stéphane. "Cyber Forensics", Chapter XLVI of *Cyber Warfare and Cyber Terrorism*, Information Science Reference, Hershey, New York, 2008.

20. Department of Justice website: *Backgrounder:* Investigative Powers for the 21st Century (IP21C) Act.   http://www.justice.gc.ca/eng/news-nouv/nr-cp/2009/doc_32388.html; Internet; accessed 30 December 2009.

21. Department of Justice, http://www.justice.gc.ca/eng/news-nouv/nr-cp/2007/doc_32179.html; Internet; accessed 13 February 2010.

22. Dubowitz, Mark and Larry Footer. "'The code is mightier than the sword'; Terrorists and rogue states are moving their battle to the Internet," *National Post*, 20 October 2009.

23. Dunnigan, James F. *The Next War Zone: Confronting the Global Threat of Cyberterrorism*. Kensington Publishing Corp., New York, NY, 2003.

24. European Commission. *7th Synthesis Report of the Sectoral e-Business Watch (2010)*, http://www.ebusiness-watch.org/key_reports/synthesis_reports.htm; Internet; accessed 25 April 2010.

25. Fagnot, Isabelle J., "Behavioral Information Security", in *Cyber Warfare and Cyber Terrorism*, edited by Lech J. Janczewski and Andrew M. Colarik, 199-205. Hershey, New York: Information Science Reference, 2008.

26. Fraser, Sheila. "Chapter 7: Emergency Management – Public Safety Canada", *2009 Fall Report of the Auditor General of Canada;* (Ottawa: 2009), 23; Available from http://www.oag-bvg.gc.ca/internet/English/parl_oag_200911_07_e_33208. html#hd3d; Internet; accessed 14 February 2010.

27. Giraldo, Jeanne and Harold Trinkunas. "Transnational Crime." in *Contemporary Security Studies*, edited by Alan Collins, 346-366. Oxford: Oxford University Press, 2007.

28. Gladstone, Julia A. "Global Aspects of Cyberlaw." in *Global Perspectives in Information Security: Legal, Social and International Issues*, edited by Hossein Bidgoli, 627-665. Hoboken, New Jersey: John Wiley & Sons Inc., 2009.

29. Held, David and Anthony McGrew, eds. *Governing Globalization, Power, Authority and Global Governance*, Oxford, UK: Polity Press, 2002.

30. International Telecommunications Union. “Resolution GSC-14/11: (GTSC) Cybersecurity (Revised),” http://www.itu.int/ITU-T/gsc/gsc14/documents.html; Internet; accessed 15 February 2010.

31. Janczewski, Lech J. and Andrew M. Colarik. *Cyber Warfare and Cyber Terrorism*, Hershey, PA: Information Sciences Reference, 2008.

32. Jennex, Murray E.. “Cyber War Defense: Systems Development with Integrated Security”, in *Cyber Warfare and Cyber Terrorism*, edited by Lech J. Janczewski and Andrew M. Colarik, 241-253. Hershey, New York: Information Science Reference, 2008.

33. Joffe, Josef. “Rethinking the Nation-State: The Many Meanings of Sovereignty”; *Foreign Affairs*, November/December 1999, http://www.foreignaffairs.com/articles/55618/josef-joffe/rethinking-the-nation-state-the-many-meanings-of-sovereignty; Internet; accessed 15 February 2010.

34. Joffe, Rodney. “The cyber crime epidemic; Terrorists and rogue states are moving their battle to the Internet. How do we fight it?” *National Post*, 23 October 2009.

35. Joint Publication 1-02. “Department of Defence Dictionary of Military and Associated Terms”, http://www.dtic.mil/doctrine/dod_dictionary/, Internet, accessed 29 March 2010.

36. Kierkegaard, Sylvia Mercado, “International Cybercrime Convention”, in *Cyber Warfare and Cyber Terrorism*, edited by Lech J. Janczewski and Andrew M. Colarik, 469-476. Hershey, New York: Information Science Reference, 2008.

37. Kurzweil, Ray, *The Singularity is Near*, Penguin Books Ltd., London, England, 2005.

38. Lewis, James A., *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, Centre for Strategic & International Studies, Washington, 2002, available at http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf; Internet; accessed 9 October 2009.

39. Maltz, Milton. “Turning Power Lines Into Battle Lines; Terrorist groups and rogue states are moving their battle to the Internet,” *National Post*, 21 October 2009.

40. Maogoto, Jackson Nyamuya. “Transforming Westphalian Sovereignty: Human Rights & International Justice as a Transitional Crucible”. *Notre Dame Law Review*, Vol. 7, 2005. Available at SSRN: http://ssrn.com/abstract=901224; Internet; accessed 15 February 2010.

41. Markoff, John. “Obama to Name Chief of Cybersecurity”, *New York Times*, 22 December 2009, http://www.nytimes.com/2009/12/22/technology/internet/22cyber.html; Internet, accessed 15 April 2010.

42. McMahon, Dave, Bell Canada. *Global Network Operations and the Emerging Threat*, unpublished paper, private communication.

43. McMahon, Dave, http://ca.linkedin.com/pub/dave-mcmahon/4/1b7/510; Internet; accessed 11 February 2010.

44. Mosco, Vincent. *The Digital Sublime: Myth, Power and Cyberspace*, MIT Press, Cambridge, Massachusetts, 2004.

45. Office of the Privacy Commissioner of Canada. http://www.priv.gc.ca/id/business_e.cfm; Internet; accessed 13 February 2010.

46. Ohmae, Kenichi. "The End of the Nation State: The Rise of Regional Economies", New York: Free Press, 1995.

47. Olson, William J. "Interagency Coordination: The Normal Accident or the Essence of Indecision", in *Affairs of State: The Interagency And National Security,* ed. Gabriel Marcella, 215-254. Carlisle, PA: Strategic Studies Institute, Army War College, December 2008.

48. Organization of American States. A Comprehensive Inter-American Cybersecurity Strategy: A Multidimensional And Multidisciplinary Approach To Creating A Culture Of Cybersecurity, http://www.oas.org/juridico/english/cyber_security.htm; Internet; accessed 27 April 2010.

49. Owens, William A., Kenneth W. Dam, and Herbert S. Lin, editors. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities,* Washington D.C.: The National Academies Press, 2009.

50. Parker, Donn, *Crime by Computer*. New York: Charles Scribner and Sons, 1976.

51. Pigeau, Ross and Carol McCann, "Re-Conceptualizing Command and Control." *Canadian Military Journal* 3, no. 1 (Spring 2002) 53-63.

52. Rapley, John, "The New Middle Ages", *Foreign Affairs*, Vol. 85 Issue 3, (May/June 2006) 95-103.

53. Reinart, Vaino. "Lessons from Estonia: Protecting the West from a computer attack," *National Post*, 22 October 2009.

54. Robert M. Gates, US SECDEF Directive 05914. http://publicintelligence.net/establishment-of-a-subordinate-unified-u-s-cyber-command/; Internet; accessed 15 February 2010.

55. Rountree, Marina, "Horizontality and Canada's Office of Critical Infrastructure Protection and Emergency Preparedness: a case study," Master's thesis, University of Manitoba, 2005.

56. Schneidewind, Norman F., "Cyber Security Models", in *Cyber Warfare and Cyber Terrorism*, edited by Lech J. Janczewski and Andrew M. Colarik, 228-240. Hershey, New York: Information Science Reference, 2008.

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

58. Shapiro, Carl and Hal R. Varian. *Information rules: a strategic guide to the network economy*, Harvard Business School Press, Boston, 1999.

59. Taylor, R.W., T.J. Caeti, D.K. Loper, E.J. Fritsch and J. Liederbach. *Digital Crime and Digital Terrorism*. Upper Saddle River, New Jersey: Pearson Prentice Hall, 2006.

60. Traynor, Ian. “Russia accused of unleashing cyberwar to disable Estonia”, *The Guardian*, Thursday 17 May 2007, http://www.guardian.co.uk/world/2007/may/17/topstories3.russia; Internet; accessed 29 April 2010.

61. U.N. Commission on Crime and Criminal Justice. *United Nations Manual on the Prevention and Control of Computer-Related Crime*. New York: United Nations, 1995.

62. United Kingdom. “Cyber Security Strategy of the United Kingdom,” Cm 7642, ISBN: 9780101764223, June 2009; available from http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf; Internet; accessed 15 January 2010.

63. United Kingdom. “Information Security Briefing provided by the UK Government Centre for the Protection of National Infrastructure (CPNI)”; http://www.cpni.gov.uk/Docs/cloud-computing-briefing.pdf; Internet; accessed 18 March 2010.

64. US Bureau of Justice Statistics website: http://bjs.ojp.usdoj.gov/index.cfm?ty=tp&tid=41; Internet; accessed 29 December 2009.

65. Veenhof, Ben and Larry McKeown, “New economy indicators” in *Innovation Analysis Bulletin — Vol. 11, no. 1 (June 2009)*, available from http://www.statcan.gc.ca/bsolc/olc-cel/olc-cel?lang=eng&catno=88-003-X200900110816; Internet; accessed 11 May 2010.

66. von Clausewitz, Carl. On War. Edited and translated by Michael Howard and Peter Paret. Princeton: Princeton University Press, 1976.

67. Wellman, Barry. “The Glocal Village: Internet and Community”, *the arts* & science re*view* University of Toronto, Autumn 2004 Volume I, Number I.

68. Williams, Phil. “Strategy for a New World: Combating Terrorism and Transnational Organized Crime”, in *Strategy in the Contemporary World*, edited by John Baylis et al. New York: Oxford University Press, 2007.

69. Wolfers, Arnold. “National Security as an Ambiguous Symbol”, *Political Science Quarterly*, Vol. 67, No. 4. (Dec., 1952), pp. 481-502.