National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

STRENGTHENING THE CYBERSECURITY OF CRITICAL INFRASTRUCTURE: THE NEED OF A TARGETED LEGISLATIVE REFORM

Lieutenant-Colonel E. Cyr

JCSP 39

Master of Defence Studies

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI 39

Maîtrise en études de la défense

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 39 – PCEMI 39
2012 – 2013

MASTER OF DEFENCE STUDIES – MAÎTRISE EN ÉTUDES DE LA DÉFENSE

STRENGTHENING THE CYBERSECURITY OF CRITICAL INFRASTRUCTURE: THE NEED OF A TARGETED LEGISLATIVE REFORM

By Lieutenant-Colonel E. Cyr
Par lieutenant-colonel E. Cyr

Word count: 16 920

Compte de mots : 16 920

Abstract

This dissertation examines the roles and responsibilities of key actors involved in the cybersecurity of Canada's critical infrastructure, and provide an overview of current strategies, policies and legislative documents related to the cybersecurity of the nation's critical assets. This paper suggests that the status quo is no longer supportable, and argues that the federal government must strengthen the cyber resiliency of Canada's critical infrastructure by adopting a targeted cybersecurity legislative framework. It emphasizes that the present and future threats to Canadian critical infrastructure via cyber vectors pose clear dangers to national security, but highlights that the current void in legal and regulatory tools is wholly inadequate for the government to meet this mandate. Finally, it validates the need to maintain and enhance a private-public partnership to bolster the cyber resiliency of the critical infrastructure, but maintains that the government cannot completely delegate this responsibility to the private sector to solve.

TABLE OF CONTENTS

STRENGTHENING THE CYBERSECURITY OF CRITICAL INFRASTRUCTURE: THE NEED OF A TARGETED LEGISLATIVE REFORM

"There can be no greater role, no more important obligation for a government, than the protection and safety of its citizens"

– Prime Minister Paul Martin, *Securing an Open Society*, 2004

CHAPTER 1 - INTRODUCTION

The rise of the internet and the expansion of the virtual domain did not happen overnight, but the speed at which it evolved is surely impressive. From the initiation of the Advanced Research Project Agency network (ARPANET) project in 1966 to the first host-to-host transmission between two American universities in October 1969[1], internet protocol developments progressed throughout the 1970s to deliver new communication capabilities in the form of file sharing and information exchange.[2] In the 1980s, the adoption of the Transmission Control Protocol and Internet Protocol (TCP/IP), the introduction of the personal computers and local area networks, and the invention of the Domain Name System (DNS) concept provided a major shift in network connectivity and allowed the internet to flourish.[3] By 1985, the internet already serviced a broad community of researchers and developers, and started to make its way into various communities for daily computer communications.[4] On 24 October 1995, the term "internet" was formally defined by the Federal Networking Council (FNC) as "the global information system that is logically linked together by a globally unique address space based on the Internet Protocol (IP)…[and] provides, uses or makes accessible, either

[1] "Brief History of the Internet", http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet (accessed 2/11/2013).
[2] Alexander Klimburg, ed., *National Cyber Security Framework Manual*, NATO Cooperative Cyber Defence Centre of Excellence, 2012), 2
[3] *Brief History of the Internet*
[4] Ibid.

publicly or privately, high level services layered on the communications and related infrastructure…"[5] Moreover, the expansion of the World Wide Web over the next two decades revolutionized global communications and interconnected mankind to a level never seen before. In a sense, the internet revolution has arguably been the most transformative invention since the printing press.[6]

The complexity and the speed at which the cyber domain has evolved have clearly taken society by surprise. Governments at every level, the private industry, and citizens of nations around the globe have been scrambling in trying to understand cyberspace, and more importantly managing the security challenges it poses. From a technological standpoint, the core protocols upon which the internet is built are now over 30 years old and were never designed to be impenetrable nor founded on a security framework.[7] Similarly, the openness of the internet has also created an opportunity for exploitation of its vulnerabilities. The infection of over 60,000 computers by the Morris worm on ARPANET in 1988 was merely a first glimpse into the problem that laid ahead.[8] In the case of a nation's critical infrastructure, industries that were once running independently are now increasingly relying on the internet to control and operate their control systems remotely. In turn, these control systems are now prime targets of state and cyber terrorists trying to inflict damage[9], and the prey of cybercriminals trying to capitalize on their weaknesses for personal gain. Additionally, the emergence of globalization and the

---

[5] Ibid.
[6] Internet Security Alliance, *The Cyber Security Social Contract Policy Recommendations for the Obama Administration and 111th Congress* (USA: ISAlliance,[2008]), 3
[7] Ibid., 2
[8] Holly Porteous, "Cybersecurity and Intelligence: The U.S. Approach" Library of Parliament, http://www.parl.gc.ca/Content/LOP/ResearchPublications/2010-02-e.pdf (accessed 02/10/2013), 1
[9] For example, Stuxnet is known to have caused significant damage to Iranian nuclear centrifuges, and will be discussed in details in chapter 2.

increasing interconnectedness of our society have created a security vacuum that states and industry must address. Suddenly, the economic, scientific and social benefits and capabilities garnered by the introduction of computers and Information and Communication Technologies (ICT) over the last 25 years now square off with the major vulnerabilities they pose on personal and national security.

The defense of a nation's critical assets is not trivial, nor absolute. From a cyber security perspective, it is a complex endeavor involving advanced technology, managed by multiple stakeholders and actors, and facing an adversary that can't be seen or heard. Certainly, a weak security posture for critical infrastructure can undermine national security. Therefore, it is of the utmost importance that sufficient resources are allocated and proper oversight is maintained to protect it. It is, after all, a matter of national security.

This paper suggests that the status quo is no longer supportable, and argues that the federal government must strengthen the cyber resiliency of Canada's critical infrastructure by adopting a targeted cybersecurity legislative framework. It emphasizes that the present and future threats to Canadian critical infrastructure via cyber vectors pose clear dangers to national security, but highlights that the current void in legal and regulatory tools is wholly inadequate for the government to meet this mandate. Finally, it validates the need to maintain and enhance a private-public partnership to bolster the cyber resiliency of the critical infrastructure, but maintains that the government cannot completely delegate this responsibility to the private sector to solve. Prevention, rather than crisis response, must be the byword.

To do this, a step-by-step approach to the cyber dimension of critical infrastructure will be used. The study will primarily focus on the critical infrastructure of Canada and the United States given their high level of interconnectivity. To that end, chapter 2 describes the current cyber environment and provides an overview of North America's critical infrastructure and the cyber threat facing it. Chapter 3 highlights the role of key actors involved in addressing cyber security of the nations' critical infrastructure, and identifies recent initiatives in the United States that suggest a change in the government approach to tackle the cybersecurity dilemma. In chapter 4, an overview of Canada's national strategies is presented, focusing on the *National Security Policy*, the *Emergency Management Act*, the *National Strategy and Action Plan for Critical Infrastructure*, as well as *Canada's Cyber Security Strategy*. Finally, chapter 5 identifies a void in cybersecurity government oversight and argues for the strengthening of the cyber legislative framework protecting Canadian critical infrastructure.

CHAPTER 2 – CRITICAL INFRASTRUCTURE AND CYBER THREATS

Canada and the United States share the longest undefended border in the world. Both nations have enjoyed peaceful co-location and mutual cooperation on many ventures over the last two centuries. Today, the daily lives of Canadians and Americans are deeply rooted and dependent on services provided by each nation's critical infrastructure. Moreover, Canada and United States critical infrastructure is closely integrated in many areas, interconnected in a way that requires the closest level of cooperation between both nations in order to yield reliable and resilient essential services. However, the emergence of cyberspace has created a new security dilemma affecting critical infrastructure which neither can solve on its own. Hence, mutual cooperation is more important than ever before to properly defend against cyber threats facing critical infrastructure. In order to properly assess the level of cooperation and corrective action required from both nations, it is important to understand what constitutes national critical infrastructure, the cyber threat level, as well as the seriousness of a successful cyber attack on critical services. This assessment will lead to the conclusion that Canada needs to be greatly concerned about the cyber threat facing critical infrastructure and needs to take the appropriate steps to properly defend against cyber attacks.

The National Critical Infrastructure

Critical infrastructure refers to the complex delivery of essential services inherent to the effective operations of a nation as well as the underlying support systems required for their delivery.[10] Domestically, the federal government defines critical infrastructure as

[10] Edward G. Amoroso, *Cyber Attacks: Protecting National Infrastructure*, Butterworth-Heinemann, 1

"the processes, systems, facilities, technologies, networks, assets, and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government."[11] While some government services are included in the national critical infrastructure framework, the private sector provides much of the essential services required by the nation such as the electrical grid, the banking system, transportation, food services and more. In fact, it is estimated that over 85 percent of the critical infrastructure in Canada is owned and operated by industry, provinces and non-governmental agencies.[12] The same ratio applies in the United States.[13]

Formally, Canada has identified ten critical infrastructure sectors as essential capabilities to sustain the nation: energy and utilities, finance, food, transportation, government, information and communication technology (ICT), health, water, safety, and manufacturing.[14] At first glance, there are three main characteristics that are unique to critical infrastructure. First, the list of sectors is quite extensive and encompasses systems and services which impact every aspect in the daily lives of Canadians. Moreover, the critical sectors virtually interconnect each other and provide essential services to one another, thereby creating an atmosphere of mutual dependence.[15] Prime examples are the reliance on ICT by the banking system to perform timely financial transactions, or the dependence of the manufacturing sector on electricity. In a sense, this co-dependence magnifies the impact of the loss of one sector service across others.

---

[11] Government of Canada, "National Strategy for Critical Infrastructure" http://www.publicsafety.gc.ca/prg/ns/ci/_fl/ntnl-eng.pdf (accessed 04/18/2013), 2
[12] Andrew Graham, *Canada's Critical Infrastructure: When is Safe enough Safe enough?*, MacDonald-Laurier Institute,[2011]), 8
[13] The National Association of Regulatory Utility Commissioners, *Information Sharing Practices in Regulated Critical Infrastructure States: Analysis and Recommendations*, [2007]), 4
[14] Government of Canada, *National Strategy for Critical Infrastructure*, 2
[15] Graham, *Canada's Critical Infrastructure: When is Safe enough Safe enough?*, 8

Second, almost every sector crosses the public-private boundary, reaches across several layers of government (federal, provincial, municipal, and territorial), or overlaps corporate-individual precincts, meaning that legal and spatial complexities are major management factors.

Third, many sectors are not unique to Canada and are largely interconnected with the United States infrastructure, meaning that close cooperation and integration with the U.S. infrastructure is vital.[16] Indeed, the interconnectedness of Canada's critical infrastructure with the United States cannot be underscored. The 2003 electrical blackout, which propelled most of Ontario and part of the eastern United States in complete darkness, proved that events originating beyond the border can have a major impact at home.[17] In fact, the outage affected over 50 million people across Canada and the U.S. and impacted the province of Ontario for several weeks with subsequent rolling blackouts. The economic damage to the nation was equally substantial: the gross domestic product was down by 0.7% in August and manufacturing shipments in Ontario were down $2.3 billion (Canadian dollars).[18] Given the significance of critical infrastructure to a nation's survival, protection of these assets becomes a crucial undertaking which cannot be ignored. As critical infrastructure assets support the safety, security, and the economic backbone of the nation, the security of these systems is, by its own definition, a matter of national security.[19]

---

[16] Ibid.
[17] The events leading to the blackout were subsequently attributed to have originated in Ohio. Refer to U.S.-Canada Power System Outage Task Force, "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations," https://reports.energy.gov/BlackoutFinal-Web.pdf (accessed 02/26/2013), 45
[18] Ibid., 1
[19] Standing Senate Committee on National Security and Defence, *Emergency Preparedness in Canada (Volume 1)*,[2008]), 98

Threats to critical infrastructure can be grouped in two separate categories: physical threats and threats from electronic, radio-frequency, and computer-based attacks.[20] Physical threats range from natural disasters such as Hurricane Katrina to terrorist acts such as the attacks on the World Trade Center and the Pentagon on 11 September 2001. Certainly, critical infrastructure is a high-value target for terrorist groups and criminals given their potential for second and third order effects from a successful attack.[21] The second category, summarized as the cyber threat, has been evolving drastically over the last two decades. According to the U.S. Critical Infrastructure Assurance Office, this fundamental shift is the result of greater dependence on information technology and the extent of globalization, resulting in the substitution of the human interface with automated and remote control systems. These new and emerging vulnerabilities are creating a real threat to critical infrastructure operations.[22]

What Is Cybersecurity

One of the prerequisites for building a national cybersecurity framework is to understand what the term *cybersecurity* entails. First, there appears to be no commonly approved definition of cybersecurity, and therefore the casual use of the term can have different meaning across different critical infrastructure sectors. In fact, a comparison of ten National Cyber Security Strategies revealed diverging definitions of the term

[20] The White House, "Executive Order 13010: Critical Infrastructure Protection" http://www.gpo.gov/fdsys/pkg/FR-1996-07-17/pdf/96-18351.pdf (accessed 04/19/2013), 1
[21] Examples of domestic disruption to critical infrastructure include the various occupations of highways and railways from First Nations groups. Refer to Graham, *Canada's Critical Infrastructure: When is Safe enough Safe enough?*, 15
[22] Ibid., 17

cybersecurity.[23] This lack of common understanding can lead to divergent national strategies to cybersecurity and may hamper international cooperation.[24] Also, terms such as *information security* and *information assurance* are commonly used within government as well as *electronic security* in the financial sector, all of which compound the difficulty in properly defining cybersecurity. While agreeing on a specific definition is not currently in the realm of possible, cybersecurity seems to comprise three essential elements:[25]

1. It is a set of activities undertaken to protect computers, software and networks from attacks, disruption, or other threats. Those activities can range from security audits, access control, systems monitoring and recovery procedures to implementing physical security barriers, conducting personnel training and providing general awareness on cyberspace.
2. It is the state or quality of being protected from such threats.
3. It is the wide range of activities related to improving and implementing those activities, including improvement to the quality of protection, research and developments, as well as detailed analysis.

[23] Only five nations provided a clear definition of cybersecurity in their Cyber Security Strategies. Others were descriptive in nature, and one was implicitly stated. Refer to H. Luiijf et al., "Ten National Cyber Security Strategies: A Comparison" CRITIS 2011 – 6th International Conference on Critical information infrastructures Security), 3

[24] Ibid., 15

[25] Eric A. Fischer, "Creating a National Framework for Cybersecurity: An Analysis of Issues and Options" in *Cybersecurity and Homeland Security*, ed. Lin V. Choi (New York: Nova Science Publishers, Inc., 2005), 7

Descriptively, the Canadian National Cyber Security Strategy defines cybersecurity as "an appropriate level of response and/or mitigation to cyber attacks…"[26] Hence, the term cybersecurity used throughout this paper refers to the range of activities encompassing all three properties referred above.

The Cyber Threat to Critical Infrastructure

Before elaborating on the characteristics of cyber threats, it is important to understand what constitutes a cyber attack. According to Canada's National Cyber Security strategy, a cyber attack is defined as "the unintentional or unauthorized access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information."[27] The National Cyber Security Strategy acknowledges that sophisticated attacks can disrupt telecommunication infrastructure, power grid and water production facility, or interference with the production and delivery of goods and services across the country.[28] The impact of these attacks can be severe and have devastating effects on the economy, in political cost, and social apprehension. Surely, the ways and the means in which cyber attacks have evolved over the last decade are reaching levels of complexity and cleverness never seen before.

Damage to critical infrastructure via cyber attacks has the potential to substantially hinder a nation's economic competitiveness, degrade privacy protection, shake public confidence, inflict significant economic losses, and undermine national

[26] Government of Canada, "Canada's Cyber Security Strategy" http://www.publicsafety.gc.ca/prg/ns/cybr-scrty/_fl/ccss-scc-eng.pdf (accessed 04/11/2013), 3
[27] Ibid.
[28] Ibid.

security and sovereignty. As such, the U.S. Cyberspace policy review clearly states that "threats to cyberspace pose one of the most serious economic and national security challenges of the 21st Century for the United States and our allies"[29] Backing this statement is the U.S. Government Accountability Office (GAO) report to Congress released in February 2013 citing several incidents affecting U.S. national security. For example, the Inspector General of the National Aeronautics and Space Administration (NASA) testified in February 2012 that Chinese-based IP addresses had acquired full access to key systems at their Jet Propulsion Laboratory, wreaking havoc by modifying, copying, and deleting highly sensitive files, creating user accounts for mission-critical laboratory systems and uploading hacking tools to steal user credentials and compromise other NASA systems.[30] A year earlier, network authentication tokens belonging to a U.S. military contractor were stolen from the networks of RSA and used against the contractor to breach their security system and steal sensitive weapon system information and other military technology.[31]

Given their high-value in terms of national security, critical infrastructure assets are likely to remain highly desired targets for organizations and individuals seeking to disrupt or neutralize them. In a nutshell, there are five possible motivations to attack national critical infrastructure via cyberspace. The first motivation is country-sponsored cyber warfare, where attacks on a nation are funded and sponsored by a state actor. The second impetus is a terrorist attack conducted by a non-state group who has obtained

---

[29] Executive Office of the President of the United States, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*,[2009]), 1
[30] United States Government Accountability Office, "Cybersecurity: National Strategy, Roles, and Responsibilities Need to be Better Defined and More Effectively Implemented" http://www.gao.gov/assets/660/652170.pdf (accessed 04/19/2013), 10
[31] Ibid.

sufficient capabilities and funding to deliver a blow on critical infrastructure. Third, commercially motivated attacks are used when companies opt to use computers to acquire information about a competitor and gain commercial advantage. Fourth, financially driven criminal attacks are used to finance criminal groups, using identity theft or other extortion techniques for financial gain. Finally, hacking is the simple motivation by hackers to boast their reputation in the cyber community by infiltrating national infrastructure.[32]

Arguably, every sector of critical infrastructure is susceptible to cyber attacks. The issue rests on which group has the motivation to target a particular sector. Government networks are usually a prime target of state-sponsored cyber attacks given the large amount of confidential and classified information normally inaccessible in the public domain. In fact, "the government is entrusted in safeguarding some of [the] most personal and sensitive information in its electronic databases… and transmits highly classified information essential [for] military operations and national security."[33] The cyber attacks on departments of the federal government networks in January 2011 is a prime example, resulting in the exfiltration of sensitive data and subsequently forcing the departments to disconnect the networks from the internet for seven months.[34] In 2011, a water plant in Texas had to disconnect its control systems from the internet after pictures of the facility's internal controls were posted online.[35] Even the medical sector, which by

---

[32] Amoroso, *Cyber Attacks: Protecting National Infrastructure*, 5
[33] Government of Canada, *Canada's Cyber Security Strategy*, 9
[34] Office of the Auditor General of Canada, "Report of the Auditor General of Canada to the House of Commons: Protecting Canadian Critical Infrastructure Against Cyber Threats" http://www.oag-bvg.gc.ca/internet/docs/parl_oag_201210_03_e.pdf (accessed 02/25/2013), 20
[35] Barack Obama, "Taking the Cyberattack Threat Seriously - Wall Street Journal" http://online.wsj.com/article/SB10000872396390444330904577535492693044650.html?KEYWORDS=Obama+cybersecurity (accessed 2/10/2013)

its own nature seems as an unlikely target of cyber exploitation, is becoming increasingly susceptible to targeted cyber attacks. Dr Kevin Fu, an associate professor at the University of Massachusetts, recently demonstrated that implanted medical devices in patients such as pacemakers and defibrillators that communicate via the internet using short range wireless links can be altered or completely shut off remotely. The access can allow a malicious actor to reprogram the defibrillator, deliver a shock to the patient's heart, or disable the battery's power-saving mode causing the battery to run down in hours rather than years.[36] The discovery prompted the release of a security bulletin from the Department of Homeland Security to warn the public of the new vulnerabilities to patients and medical facilities. Similarly, a researcher at the security firm McAfee was able to scan and compromise insulin pumps wirelessly using off-the shelf equipment. Within a 300 foot range, an entire 300 unit reservoir of insulin could be dispensed without requiring the pump's identification number.[37] While not directly tied to a matter of national security, the ability to target an individual with known medical problems can become a more serious issue for nations trying to protect their key leadership.

Perhaps the biggest threat to critical infrastructure comes from cyber attacks capable of inflicting physical damage to equipment and control systems. In a nutshell, critical infrastructure sectors such as oil and gas refineries, power plants, nuclear facilities, the electrical grid, and transportation networks are widely monitored and controlled by Supervisory Control and Data Acquisition (SCADA) systems, which gather

---

[36] American College of Cardiology's CardioSource, "Homeland Security Warns of Medical Device Hacking" http://www.cardiosource.org/News-Media/Publications/CardioSource-World-News/Homeland-Security.aspx (accessed 2/10/2013)

[37] Christine Hsu, "Many Popular Medical Devices may be Vulnerable to Cyber Attacks : Consumer News : Medical Daily" http://www.medicaldaily.com/articles/9486/20120410/medical-implants-pacemaker-hackers-cyber-attack-fda.htm#md5KuC237zm6BE5m.99 (accessed 2/10/2013)

and use real time data to operate generators, pumps, and similar industrial plant machinery.[38] These industrial control systems (ICS) are in turn controlled through programmable logic controllers (PLCs). Not immune to the increasing cyber threat, SCADA systems have become increasingly susceptible for targeted cyber attacks.

Such is the case of Stuxnet, a worm primarily written to target ICS or set of similar systems. In essence, Stuxnet's main goal is to sabotage a facility by reprogramming an ICS though the modification of code on PLCs, making the ICS operate outside their safe and normal performance range while hiding those changes from the operator of the equipment.[39] By doing so, Stuxnet was reportedly capable of disrupting Iran's uranium enrichment production facility by modifying the speed of spinning centrifuges controlled by the PLCs, hereby physically damaging the nuclear facility's centrifuges.[40] Stuxnet was later described as being the first software threat to be used as a cyber weapon.[41] A similar experiment conducted at a U.S. Department of Energy Idaho laboratory proved that physical damage to an electrical generator and motors was possible by intentionally opening a breaker and closing it out of synchronism. Dubbed the "Aurora vulnerability", the 2006 experiment made headlines around the world and proved that physical damage to the electrical grid through a targeted cyber attack was real and feasible.[42]

---

[38] "What is SCADA?" http://www.webopedia.com/TERM/S/SCADA.html (accessed 3/6/2013)
[39] Nicolas Falliere, Liam O Murchu and Eric Chien, "W32.Stuxnet Dossier" Symantec Corporation, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf (accessed 03/04/2013), 1
[40] Kim Zetter, "Stuxnet Missing Link found, Resolves some Mysteries Around the Cyberweapon" Wired.com, http://www.wired.com/threatlevel/2013/02/new-stuxnet-variant-found/all/ (accessed 3/5/2013)
[41] Geoff McDonald et al., "Stuxnet 0.5: The Missing Link" Symantec Corporation, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/stuxnet_0_5_the_missing_link.pdf (accessed 03/05/2013), 1
[42] "Aurora Vulnerability White Paper | Power Grid Security Vulnerable to Cyber Attack" http://unix.nocdesigns.com/aurora_white_paper.htm (accessed 3/5/2013)

While physical destruction of critical infrastructure is conceivably the most dangerous scenario of a successful cyber attack, the most likely arise from the disruption of critical services through denial of service attacks. One of the most publicized cases of a large-scale cyber attack remains the assaults on Estonia's digital infrastructure in April 2007. For weeks, Estonia's national infrastructure was hit with distributed denial of service (DDOS) attacks, the largest ever seen to date, eventually bringing Estonia to its knees. The DDOS were orchestrated though "botnets", a network formed "on demand" by merging infected computers (called zombies) and focused on a target of choice. In the case of Estonia, several botnets, each with tens of thousands of computers scattered around the world, were used to take down internet services by flooding the systems with pings. Public webpages, the credit card verification system, the telephone network as well as Hansapank, the nation's largest bank, were rendered ineffective. Hundreds of key sites were taken down week after week, prompting the country to elevate the matter to the North Atlantic Treaty Organization (NATO).[43] Regardless of who was behind the attack, the scenario presented above reveal a real and present danger of cyber attacks on a nation's critical infrastructure, potentially affecting national security.

Another major threat facing critical infrastructure is tied to the exploitability of the IT supply chain. Investigations by the FBI and other law enforcement agencies concluded that approximately 10% of all electronics coming into the United States is counterfeit, and growing evidence points to the deliberate installation of backdoor access capabilities by foreign governments into products made in their own countries. Certainly, this leaves the Department of Homeland Security and other federal departments wary of

[43] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and what to do about it* (United States of America: HarperCollins, 2010), 15

the potential impact on critical infrastructure in the long term.[44] A major cyber supply chain vulnerability study conducted in 2010 covered 285 U.S.-based organizations in charge of critical infrastructure and concluded that few organizations are thorough with their supply chain and pay due diligence on their IT vendor's security, leaving the potential of installing hardware and software with vulnerabilities "baked in".[45] In the United States, the concept of "cyber supply chain security" originated with the National Security Agency's Trusted Product Evaluation initiative in the 1980s and is aimed at extending internal risk management measures to third party providers of IT equipment and services.[46] In Canada, the vulnerability of the supply chain for Government of Canada telecommunications equipment and services was assessed as an emerging national security issue.[47] The Common Criteria Scheme (CCS) is a Canadian independent third party evaluation and certification service designed to evaluate the trustworthiness of IT security products and systems, and is overseen by a Certification Body (CB) provided by the Communications Security Establishment Canada (CSEC).[48] Additionally, several meetings between various federal government departments in 2008 led to CSEC promulgating the Technology Supply Chain guidelines. The guidelines direct that IT

---

[44] Jennifer Bayuk et al., *Cyber Security Policy Guidebook*, Wiley, 232

[45] Jon Oltsik, John McKnight and Jennifer Gahm, "Research Report: Assessing Cyber Supply Chain Security Vulnerabilities within the U.S. Critical Infrastructure", Enterprise Strategy Group, http://www.nsci-va.org/CyberReferenceLib/2010-11-ESG%20Research%20Report%20Cyber%20Supply%20Chain%20Security.pdf, 6

[46] Ibid., 10

[47] Communications Security Establishment Canada, "Technology Supply Chain Guidelines: Contracting Clauses for Telecommunications Equipment and Services" http://www.cse-cst.gc.ca/documents/services/tscg-ccat/tscg-ccat01g-eng.pdf (accessed 03/08/2013), 1

[48] "CCS Overview" http://www.cse-cst.gc.ca/its-sti/services/cc/ccso-vesccc-eng.html (accessed 3/8/2013)

procurement should be that, whenever possible, only Common Criteria (CC) certified and Crypto Module Validation Program (CMVP) validated products are to be trusted.[49]

While the Common Criteria standards and the CSEC procurement guidelines certainly reduce the risk of introducing vulnerable and shaped technologies into the government IT infrastructure, they are mandated only for federal government acquisitions and not across all critical infrastructure sectors. As Jim Robbins explains in his testimony to the Standing Senate Committee on National Security and Defence regarding the use of the Common Criteria, "…no other [federal] department has been assigned a responsibility for security assurance and product certification related to the financial sector, e-commerce, health care, local governments, [and] the critical infrastructure sectors…"[50] Moreover, he states that "Canada's advocacy for the use of the Common Criteria has diminished [over the years] as the roles and mandates of departments have gradually been narrowed."[51] This issue will be further discussed in chapter 5.

Why Canada Should Be Concerned

In 1996, the federal government acknowledged that critical infrastructure was vulnerable to cyber attacks and had a role to play to protect them from such attacks.[52] In one instance, the financial cost associated with the loss of a critical sector can be quite significant. For example, it is estimated that the 2003 electrical blackout cost the U.S.

---

[49] Communications Security Establishment Canada, *Technology Supply Chain Guidelines: Contracting Clauses for Telecommunications Equipment and Services*, 10

[50] Standing Senate Committee on National Security and Defence, "Proceedings of the Standing Senate Committee on National Security and Defence, Issue 6, Evidence - Meeting of may 7, 2012" http://www.parl.gc.ca/content/sen/committee/411/SECD/06EVB-49519-E.HTM (accessed 3/8/2013)

[51] Ibid.

[52] Office of the Auditor General of Canada, *Report of the Auditor General of Canada to the House of Commons: Protecting Canadian Critical Infrastructure Against Cyber Threats*, 7

economy more than $6 billion dollars.[53] Despite the increased awareness of cybersecurity across the public and private sectors, what is most concerning is that cyber attacks on critical infrastructure are increasing at an alarming rate, are usually more complex in nature, and are showing no signs of slowing down. In July 2012, the Director of the U.S. National Security Agency stated that there had been a 17-fold increase in cyber-related attacks on American infrastructure between 2009 and 2011.[54] Similarly, Mr Jim Robbins highlights that "in the last few years…the number of major compromises of major enterprises has increased significantly, some to such a magnitude that we could not mobilize the large number of people it would take to rebuild their network."[55] Unfortunately, only a fraction of those attacks get reported, and therefore a true appreciation of the real threat facing critical infrastructure is even more difficult to grasp. In fact, Canada is lagging on its ability to centrally record, consolidate and provide cyber attack reports to a central agency or committee responsible for cyber security, and is the only G8 nation who does not have such a system in place.[56]

The 2004 National Security Policy provided a clear description of the problem at hand: "cyber-security is at the forefront of the transborder challenge to Canada's critical infrastructure. The threat of cyber-attacks is real, and the consequences of such attacks

---

[53] Peter Kelly-Detwiler, "Protecting the Electric Grid from Terrorism -- Nobody is in Charge" Forbes, http://www.forbes.com/sites/peterdetwiler/2012/11/16/protecting-the-electric-grid-from-terrorism-nobody-is-in-charge/ (accessed 3/8/2013)

[54] Center for Strategic and International Studies, "Significant Cyber Incidents since 2006" http://csis.org/files/publication/130206_Significant_Cyber_Incidents_Since_2006.pdf (accessed 04/15/2013), incident no. 110

[55] Mr Robbins is President of EWA-Canada, a Systems Engineering Company which addresses the business and security risks inherent in the use of information technology and helps clients solve their most complex problems related to Information Management, Identity Management and Information Technology Security. Refer to Standing Senate Committee on National Security and Defence, *Proceedings of the Standing Senate Committee on National Security and Defence, Issue 6, Evidence - Meeting of may 7, 2012*

[56] Ibid.

can be severe."[57] Certainly, concerns about critical infrastructure cyber security south of the border cannot be undermined. Given the interconnectedness of the Canadian and American critical assets, Canada has a vested interest in synchronizing its efforts with the United States. In fact, Canada's threat level is directly linked to that of the United States.[58] Without a doubt, the United States have led the way in raising cybersecurity as a national security issue, prompting the U.S. government to push for increased regulation in certain areas of the private industries' cybersecurity practices.[59] In a sense, Canada would be far better off in addressing its cybersecurity issues now rather than in the midst or in the aftermath of a major cyber attack on its critical infrastructure. Moreover, it would be in Canada's interest, by mere geographical colocation and interconnectedness of its critical infrastructure with the U.S., to follow suit with the American efforts to strengthen cybersecurity as these efforts are unfolding south of the border. To that end, the U.S. government efforts to further regulate cybersecurity of critical infrastructure will be covered in greater details in Chapter 5.

Despite the numerous strategies and policies released by the Canadian government between 2001 and 2009, limited progress has been made to enhance the cybersecurity of Canada's critical infrastructure.[60] The underlying cause surrounding this lack of progress can be attributed to several factors: lack of funding, lack of government accountability, lack of cyber knowledge, ineffective or insufficient information sharing of cyber threats, and the inability to pressure the owners and operators of critical

---

[57] Privy Council Office, "Securing an Open Society: Canada's National Security Policy" http://publications.gc.ca/collections/Collection/CP22-77-2004E.pdf (accessed 03/27/2013), 26
[58] Graham, *Canada's Critical Infrastructure: When is Safe enough Safe enough?*, 17
[59] Porteous, *Cybersecurity and Intelligence: The U.S. Approach*, 6
[60] Office of the Auditor General of Canada, *Report of the Auditor General of Canada to the House of Commons: Protecting Canadian Critical Infrastructure Against Cyber Threats*, 2

infrastructure in achieving acceptable levels of cybersecurity. In the next chapter, a review of cyber actors involved in the protection of critical infrastructure will be discussed, along with the current strategies and policies driving the security of the nation's critical assets.

CHAPTER 3 – CRITICAL INFRASTRUCTURE AND THE ROLE OF CYBER ACTORS

The scope and complexity of the nation's critical infrastructure, combined with the interdependencies across several sectors and substantial integration with the United States systems, pose a serious management and control challenge. In fact, the span of critical infrastructure is such that no one entity can effectively manage or defend the domain on its own. Therefore, the protection of critical infrastructure, including the cybersecurity component, must derive from the combined effort and involvement of various stakeholders. As articulated in the *National Security Policy*, "national security deals with threats that have the potential to undermine the security of the state or society", and it also states that "these threats generally require a national response, as they are beyond the capacity of individuals, communities or provinces to address alone."[61] In short, there are four principal actors involved in the cybersecurity of Canada's critical infrastructure: the government, the private sector, the citizen, and the United States. As Andrew Graham points out, "Canada's critical infrastructure is massive, geographically dispersed, owned by many different players, and vulnerable. Applying any simple form of governance to protect it will not work."[62] Therefore, the roles and responsibilities of each actor must be properly defined and the interaction between each other clearly articulated in order to maximize the effectiveness of a nation's cybersecurity strategy. Furthermore, a broad review of the current approach to bolster the cybersecurity of critical infrastructure is presented, and finds that the current efforts are unfocused and inadequate in protecting the nation's critical assets.

---

[61] Privy Council Office, *Securing an Open Society: Canada's National Security Policy*, 3
[62] Graham, *Canada's Critical Infrastructure: When is Safe enough Safe enough?*, 2

The Government

A core responsibility of the government is to provide for the security of Canadians. As articulated by Canada's Prime Minister in the National Security Policy, "there can be no greater role, no more important obligation for a government, than the protection and safety of its citizens."[63] Similarly, the United States have highlighted the same duty for its government: "[t]he Federal government has the responsibility to protect and defend the country, and all levels of government have the responsibility to ensure the safety and wellbeing of citizens."[64] As discussed in the previous section, critical infrastructure is vital to the survival of a nation, and its disruption or exploitation can easily become a matter of national security. Therefore, not only the federal government has a prime responsibility in protecting the nation's critical infrastructure, but it also plays a key role in providing the level of effort required to safeguard the availability, integrity, and confidentiality of these vital systems. This can be achieved by taking a leadership role at the highest level of government, and by adopting adequate control measures to ensure the protection of the nation's critical assets. In fact, the passage of the *Emergency Management Act* in 2007 affirmed federal authority over critical infrastructure protection, adding a legal obligation for the federal government to play such leadership role.[65]

Consistent with the *National Strategy for Critical Infrastructure* and the *Emergency Management Framework* for Canada, the government currently meets its

---

[63] Privy Council Office, *Securing an Open Society: Canada's National Security Policy*, vii
[64] Executive Office of the President of the United States, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, iv
[65] Standing Senate Committee on National Security and Defence, *Emergency Preparedness in Canada (Volume 1)*, 98

responsibilities by advancing a collaborative approach between federal, provincial, municipal and territorial governments in close partnership with the private sector.[66] In other words, the federal government acts as a national coordinator to promote information sharing between the private sectors and various government levels. To do so, the government committed to establishing sector networks to foster the exchange of information pertinent to their specific sectors.[67] Briefly, these sector networks are expected to address interdependencies between sectors and also lead to the development of plans and programs designed to protect critical infrastructure.[68] While the concept of sector network is sound and logical, there are deficiencies with the current approach, both from a performance and strategy standpoint. From a performance perspective, the latest audit report released by the Office of the Auditor General was critical of the lack of progress in establishing the sector networks, highlighting that sector networks were still at various stages of maturity. In fact, two years after the release of the *National Strategy and Action Plan for Critical Infrastructure* which effectively announced the creation of the sector networks, six sectors still had no representative from all the industry groups identified by Public Safety as key stakeholders in their respective sectors.[69] From a strategy perspective, the Auditor General noted that while most sectors had met by the time the audit was conducted, only five had identified cybersecurity in their discussions. Moreover, membership and attendance to the sector network discussions is voluntary.[70] Given the criticality of these systems to the nation, it is deemed rather disconcerting that

---

[66] Government of Canada, "Action Plan for Critical Infrastructure" http://www.publicsafety.gc.ca/prg/ns/ci/_fl/ct-pln-eng.pdf (accessed 04/18/2013), 3
[67] Office of the Auditor General of Canada, *Report of the Auditor General of Canada to the House of Commons: Protecting Canadian Critical Infrastructure Against Cyber Threats*, 13
[68] Ibid.
[69] Ibid.
[70] Ibid.

attendance to sector network discussions is on a voluntary basis, and that cybersecurity in only a topic of choice in their meetings. As Andre Graham eloquently stated, "[t]he federal government, while trying to provide a form of general leadership and sharing platforms, lacks most of the policy and operational clout to impose solutions, even when they are known."[71] Thus, the power of the government to meet its most fundamental mandate – that of protecting the nation and its citizens – is limited to fostering coordination and information sharing between the public and private sectors, on a voluntary basis. Given the premise of national security implications with the loss of critical infrastructure from cyber attacks, the current situation is deemed inadequate.

Perhaps the most compelling argument to involve the federal government in the cybersecurity of critical infrastructure is embedded in the United States' Cyberspace Policy Review: "[t]he Federal government cannot entirely delegate or abrogate its role in securing the Nation from a cyber incident or accident."[72] In a sense, it is argued that the government is indirectly delegating the responsibility of protecting cyberspace to the owners and operators of critical infrastructure by solely taking a coordinating role in the matter. Discussed in greater details in chapter 5, this deficiency has already been recognized in the United States and is currently being addressed by aggressively advancing a cybersecurity legislative framework that will enhance the role and responsibility of the federal government in protecting critical infrastructure. As Ron Diebert explains, there has been a major shift in the way governments tackle the challenges posed by cyberspace. Over the last two decades, the lack of oversight or

[71] Graham, *Canada's Critical Infrastructure: When is Safe enough Safe enough?*, 3
[72] Executive Office of the President of the United States, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, iv

laissez-faire approach with the private sector has made way for a swift assertion of power in order to shape the domain and suit strategic domestic and foreign policies.[73] Moreover, the United States have led the way in this field, issuing various cyber strategy documents, legislation, policies and reforms to address the seriousness of the cyber threat.[74] Therefore, it would be in Canada's interest to align its efforts with its southern neighbor, more specifically in tailoring its legislative and regulatory frameworks to match the current cyber threat facing critical infrastructure. Certainly, given the interconnectedness of Canada's critical infrastructure with the Unites States, it is imperative that greater planning and close cooperation is exercised between the two nations.[75]

As the government is considered a critical sector network in itself, it is important to understand the roles and responsibilities of key federal departments who actively play a role in enhancing cybersecurity of the Canadian government networks. Table 3.1 highlights the numerous organizations which play a key role in protecting government networks.

Table 3.1: Key federal agencies involved in protecting government systems from cyber threats

Agency	Responsibilities
Privy Council Office (PCO)	Advising and supporting the Prime Minister and Cabinet on national security matters, coordinating the related activities of departments and agencies, and providing government-wide policy direction on national security and intelligence priorities
Treasury Board of Canada Secretariat	Setting government-wide direction, establishing priorities, and defining and formalizing IT security requirements for departments

[73] Jennifer Bayuk et al., *Cyber Security Policy Guidebook* , 236-237
[74] Ron Diebert, "Cyber Security: Canada is Failing the World" http://www.huffingtonpost.ca/2011/05/26/cyber-security-canada-stephen-harper-g8_n_867136.html (accessed 2/23/2013)
[75] Graham, *Canada's Critical Infrastructure: When is Safe enough Safe enough?*, 8

(TBS)	of the Government of Canada
Public Safety Canada (PS)	Coordinating activities related to IT incidents affecting the Government of Canada and monitoring IT threats to services to Canadians or government operations
Communications Security Establishment Canada (CSEC)	Leading and coordinating departmental activities to help ensure the protection of IT systems of importance
Public Works and Government Services Canada (PWGSC)	Delivering IT security services, such as ensuring the confidentiality, integrity, and availability of common IT services provided to departments
Canadian Security Intelligence Service (CSIS)	Providing intelligence reports and assessments relating to IT security to help ensure the protection of the Government of Canada's critical services and systems
Royal Canadian Mounted Police (RCMP)	Providing services related to law enforcement and investigations including computer forensics and cyber crime

Source: Report of the Auditor General of Canada to the House of Commons: Protecting Canadian Critical Infrastructure against Cyber Threats, 21

As Public Safety Canada remains the primary department responsible to protect Canadians, it has been given the responsibility of operating the Canadian Cyber Incident Response Center (CCIRC). Established in 2005, the CCIRC is the "national coordination centre for the prevention and mitigation of, preparedness for, response to, and recovery from cyber incidents on non-federal government systems."[76] It also escalates significant cyber incidents to the Government Operations Center (GOC) to coordinate a national

[76] Public Safety Canada, "Canadian Cyber Incident Response Centre" http://www.publicsafety.gc.ca/prg/ns/cybr-scrty/ccirc-eng.aspx (accessed 04/05/2013)

response to a cyber event.[77] However, the responsibility to protect government information systems was transferred from CCIRC to CSEC in 2011 given CSEC's notable technical expertise and supporting mandate to protect government networks from cyber threats.[78] In short, CSEC "monitors and defends Government of Canada networks by detecting, discovering and responding to sophisticated cyber threats to the Government..."[79] Despite the large emphasis placed by the federal government to foster information sharing with critical infrastructure owners and operators, there remain issues of information sharing within the federal government departments. Indeed, the high sensitivity of information collected by CSEC has prevented sharing of timely and complete information with CCIRC, citing classification levels or sensitivities of client departments as two common pretexts.[80] This has resulted in CCIRC not being completely engaged in ongoing cyber incidents. As a result, CCIRC has been unable to collect and distribute timely and accurate cyber threats information with the sector networks and other key stakeholders involved in critical infrastructure cyber protection.[81] This issue is currently being temporarily addressed by imbedding a liaison officer on a trial basis within CSEC to facilitate secure information sharing. Similarly, CCIRC relies on individual departments to inform it of cyber incidents or attacks in order to coordinate the national response, yet it was only notified one week after the Finance Department and the

---

[77] Public Safety Canada, "Cyber Security in the Canadian Federal Government" http://www.publicsafety.gc.ca/prg/ns/cybr-scrty/fdrl-gvt-eng.aspx (accessed 03/27/2013)
[78] Office of the Auditor General of Canada, *Report of the Auditor General of Canada to the House of Commons: Protecting Canadian Critical Infrastructure Against Cyber Threats*, 17
[79] Public Safety Canada, *Cyber Security in the Canadian Federal Government*, http://www.publicsafety.gc.ca/prg/ns/cybr-scrty/fdrl-gvt-eng.aspx (accessed 03/27/2013)
[80] Office of the Auditor General of Canada, *Report of the Auditor General of Canada to the House of Commons: Protecting Canadian Critical Infrastructure Against Cyber Threats*, 17
[81] Ibid., 18

Treasury Board were subject to a massive cyber attack on their networks.[82] While the need to adopt a different information sharing model will be discussed in chapter 5, it is essential for the government to overcome the issues related to the release of critical cybersecurity information.

The creation of Shared Services Canada (SSC) in August 2011 brings another level of coordination, complexity, and increased ambiguity in determining who is actually responsible for what portion of cybersecurity within the federal government. As SSC provides IT security for email systems, data centres and various networks across 43 federal departments, its role in protecting government systems from cyber threats remains unclear. Establishing itself as a key partner in the delivery of security services for the government, SSC's Report on Plans and Priorities for fiscal year 2013-14 vaguely state that "[SSC] will continue to work collaboratively with other Government of Canada cyber-security agencies to support the implementation of the federal government's cyber-security strategy and help strengthen the security of federal information and information systems."[83] However, the Department does not elaborate on how it will achieve this. Besides, the Government of Canada Information Technology Incident Management Plan (GC IT IMP) currently requires departments to report IT incidents to the Government of Canada Cyber Threat Evaluation Center (GC CTEC) at CSEC until SSC is ready to assume the role of the Government of Canada Computer Incident Response Team (GC

[82] Tom Parry, "Critical Cybersecurity Gaps Remain, Auditor General Says" http://www.cbc.ca/news/politics/story/2012/10/23/pol-auditor-generals-report-cybersecurity-veterans-fiscal.html (accessed 04/08/2013)
[83] Shared Services Canada, "2013-14 Report on Plans and Priorities" http://www.ssc-spc.gc.ca/media/documents/SSC_RPP_2013-14EN%20(NO%20SIGN).pdf (accessed 04/05/2013), 17

CIRT).[84] Lastly, *Canada's Cyber Security Strategy* and the *Policy on Government Security* will need to be updated to include the roles and responsibilities of SSC in protecting the networks of the federal government.

The Auditor General report was also critical of the lack of focus from expenditures made towards improving cybersecurity of critical infrastructure in the last decade. For example, funding of $780 million was allocated to thirteen federal department and agencies between 2001 and 2011 for emergency management and national security initiatives, including enhancing cybersecurity for critical infrastructure. However, approximately $570 million was destined for CSEC to improve the overall program capacity of CSEC, and not solely on cybersecurity. Additionally, Public Safety reported that only $20.9 million of the remaining $210 million was directed towards cyber protection for critical infrastructure between 2001 and 2011.[85] Certainly, such a minute amount of funding is not sufficient to bolster the cybersecurity of critical assets, and certainly not commensurate to the priority assigned to cybersecurity by the federal government. In comparison, major executive branch agencies of the United States government received 12 billion dollars in combined spending on cybersecurity in 2010 alone, and the trend of greater spending on cybersecurity in the coming years is apparent.[86]

---

[84] Treasury Board of Canada Secretariat, "Government of Canada Information Technology Incident Management Plan" http://www.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimti01-eng.asp (accessed 04/07/2013)

[85] Office of the Auditor General of Canada, *Report of the Auditor General of Canada to the House of Commons: Protecting Canadian Critical Infrastructure Against Cyber Threats*, 10-11

[86] Kristin M. Lord and Travis Sharp, *America's Cyber Future: Security and Prosperity in the Information Age (Volume 1)* (Washington: Center for a New American Security,[June 2011]), 34

In reality, it is clear that the myriad of federal departments involved in protecting the nation's critical assets increases the complexity in coordinating cybersecurity efforts within the federal government and with external actors. Most importantly, it leads to the fundamental issue of establishing accountability. Indeed, there is no single department which has the overall responsibility and accountability to take the necessary steps in protecting the assets most critical to the nation. Even with the titular leadership being lodged in Public Safety, the reality is that no one is really responsible and accountable for cybersecurity of critical infrastructure.[87] Instead, ad hoc problem solving supported by a muddled policy process constitutes the cyber defense of the nation's critical infrastructure.[88] Certainly, the lack of accountability, the lack of budget focus and resource allocation, and the difficulty in sharing information within federal departments and with key external partners need to be addressed first and foremost if the government is to gain credibility as a leading institution. These are indeed areas of improvement that will require determination and commitment at the highest level of government, along with the allocation of necessary resources to address this monumental challenge.

Regardless of the hurdles faced by the government in improving cybersecurity of critical infrastructure, the responsibility to protect it from cyber attacks cannot solely be borne by the government. Given that critical infrastructure assets are largely owned and operated by the private sector, the industry delivering the nation' essential services also have a prime responsibility in protecting their networks and control systems.

---

[87] Graham, *Canada's Critical Infrastructure: When is Safe enough Safe enough?*, 10
[88] Ibid.

The Private Sector

Undoubtedly, the private sector plays the largest role in securing critical infrastructure. Given the large proportion of critical infrastructure assets owned and operated by private companies, combined with the technical knowledge and expertise resident within the industry, the private sector is cornerstone to the effective preventative defense of the nation's critical infrastructure. As Scott Charney, Vice President of Microsoft's Trustworthy Computing, explains: "[t]he private sector drives the design, development and implementation of the products and services that power cyberspace…[making] us key partners in developing national and international cyberspace security strategies."[89] Similar to the requirement for leadership at the highest level of government, an effective cybersecurity framework must also involve the highest level of corporate governance. As cybersecurity is often viewed as a technical issue, it is in fact a governance challenge that requires accountability, risk management, responsible reporting, and active engagement from executive management such as Board of Directors (BODs) and Chief Executing Officers (CEOs).[90] Moreover, Jennifer Bayuk *et al* clarify that "…a corporation security policy issued by a Chief Executing Officer will generally apply to an entire corporation, but one issued by the Chief Information Officer will typically only apply to the technology staff."[91] Thus, the imperative of involving the highest echelons of corporate governance is real.

---

[89] United States House of Representatives, "Written Testimony of Scott Charney, Corporate Vice President, Microsoft Corporation's Trustworthy Computing" http://www.whitehouse.gov/files/documents/cyber/Congress%20-%20Charney-microsoft-SFR_10Mar09.pdf (accessed 06/02/2013), 4

[90] National Cyber Security Summit Task Force, "Information Security Governance: A Call to Action" http://www.cyber.st.dhs.gov/docs/Information%20Security%20Governance-%20A%20Call%20to%20Action%20(2004).pdf (accessed 04/05/2013), cover letter

[91] Jennifer Bayuk et al., *Cyber Security Policy Guidebook* , 9

The Congressional Research Service (CRS), which provides legal and policy analysis for the United States House and Senate, suggested that the private sector may move forward in bolstering their cybersecurity in order to avoid liability costs. Certainly, the prospect of being sued for damages incurred from the loss or destruction of confidential information is a major incentive for the industry to take cybersecurity seriously.[92] However, the fear of legal reprisal is equally one of the main reasons why the private sector is reluctant in sharing cyber attack information with other partners or the government.[93] In the current construct, there is no assurance that the private sector will meet a level of cybersecurity commensurate of the criticality of these systems to the nation. In fact, Jack Goldsmith, a former Attorney General with the Bush Administration, proclaims that there is no reason to think that private firms that owns critical infrastructure will invest in cybersecurity to the extent that is actually needed to prevent harm to the industry and those benefitting from these critical services.[94] Moreover, former Secretary of Homeland Security Michael Chertoff equally questions the value of market incentives as being adequate to protect critical infrastructure: "[l]eft to their own devices, few private companies would invest more in securing their cyber assets than the actual value of those assets."[95]

---

[92] U.S. House of Representatives Select Committee on Homeland Security, "Cybersecurity for the Homeland," in *Cybersecurity and Homeland Security*, ed. Lin V. Choi (New York: Nova Science Publishers, Inc., 2005), 92

[93] Ibid.

[94] Jack Goldsmith, "Conservative Legal Scholar Backs Security Standards for Critical Infrastructure" http://www.hsgac.senate.gov/media/majority-media/conservative-legal-scholar-backs-security-standards-for-critical-infrastructure (accessed 4/6/2013)

[95] United States Senate Committee on Homeland Security and Government Affairs, "Statement for the Record by the Honorable Michael Chertoff - February 16, 2012" http://www.hsgac.senate.gov/download/cybersecurity-support-statement-former-dhs-secretary-michael-chertoff (accessed 04/06/2013)

The private sector faces unique challenges because its customer base and supply chain are global, hereby forcing companies to think about balancing security features with price sensitivities expected by the users.[96] Certainly, the economics of private companies cannot be ignored. As Rob Schneier explains, private companies are in the business of making money, and therefore approach cybersecurity as they do any other business risk: in terms of risk management. Therefore, many organizations prefer not to invest in network security due to the significant costs involved, hereby leading to inadequate cybersecurity posture.[97] While the situation is inconsequential for small businesses in the context of national security, the same cannot be said about critical infrastructure industries. Some argue that the private industry associated with critical infrastructure is likely to see more government oversight of their cybersecurity practices in the coming years.[98] On the other hand, some argue that the government is trying to download their responsibilities to the private sector to police cyberspace.[99] Regardless, the private sector is caught in cross-hairs between hackers continuously trying to penetrate their networks while simultaneously being pressured by governments to do something about it.[100]

In the end, the private sector plays a crucial role in protecting the cybersecurity of the nation's critical infrastructure. Therefore, close coordination and partnership between the government and the industry is an essential element of an effective cyber strategy.

---

[96] United States House of Representatives, *Written Testimony of Scott Charney, Corporate Vice President, Microsoft Corporation's Trustworthy Computing*, 4
[97] Bruce Schneier, *On Security*,(Indianapolis: Wiley Publishing Inc., 2008), 151-152
[98] Brian Zimmet and Jason Wool, "Cybersecurity Regulation: 5 Issues for Companies - MarketWatch" http://articles.marketwatch.com/2013-01-11/commentary/36270525_1_cybersecurity-operators-regulation (accessed 4/8/2013)
[99] Diebert, *Cyber Security: Canada is Failing the World*
[100] Ibid.

However, the question remains whether market incentives are sufficient to drive a cybersecurity posture commensurate of safeguarding national security. For the United States, it appears that it is not the case, and that cybersecurity legislation is lurking on the horizon.

The Citizens

While not necessarily the lead actor in protecting the cybersecurity of critical infrastructure, the citizens of a nation play an important, yet indirect role in a nation's cybersecurity strategy. First, their main responsibilities remain in the ability to prepare and survive the loss of one or many critical services. However, they also indirectly play an important role protecting the nation's critical infrastructure by protecting their personal computers and electronic devices. Recall the discussion in Chapter 2 regarding the establishment of Botnets by malicious cyber actors which use computer vulnerabilities from unsuspecting citizens to disrupt or neutralize critical infrastructure through distributed denial of services attacks. Indeed, that is exactly where citizens play a key role in protecting a nation's critical assets. By using strong password protection techniques or using updated virus detection software, citizens can minimize the risk of having their personal computers used remotely as a cyber weapon on their own critical infrastructure. Certainly, vulnerable computers create a national vulnerability which must be addressed sooner than later.[101] For example, it is estimated that over 50, 000

[101] Richard J. Harknett and James A. Stever, "The Cybersecurity Triad: Government, Private Sector Partners, and the Engaged Cybersecurity Citizen" *Journal of Homeland Security and Emergency Management* 6, no. 1 (2009), 9

compromised computers were used in the DDOS attacks on American and South Korean government sites in July 2009.[102] The current situation is indeed troubling.

Canada's Cyber Security Strategy highlights the requirement of involving the nation's citizens in the overall national cyber strategy: "Canadians will strengthen their own individual cyber security and that of Canada as a whole."[103] Certainly, the threat posed by the subpar computer security is real and cannot be ignored. According to Scott Charney, "…the Internet citizen … is critically relevant to any solution. Unsecured computers can turn everyday users into a launch platform for attacks. Fear about online security and availability can have sweeping economic consequences."[104] Yet the average citizen is still unaware of the risk posed by cybersecurity. In 2005, a Verisign survey found that two-thirds of 272 people stopped on a street in San Francisco were willing to trade their network passwords for a $3 Starbucks card.[105] Such attitude and lack of knowledge about cybersecurity is indeed a major stumbling block towards achieving a successful cybersecurity strategy to protect critical infrastructure.

In summary, cybersecurity citizenship remains an essential component of an effective national cyber strategy. As Harknett and Stever explain, "the ubiquity of computer technology throughout the civilian population will require full social engagement if the national objective is a secure cyberspace."[106] Indeed, cybersecurity

---

[102] Ibid.
[103] Government of Canada, *Canada's Cyber Security Strategy*, 13
[104] United States House of Representatives, *Written Testimony of Scott Charney, Corporate Vice President, Microsoft Corporation's Trustworthy Computing*, 2
[105] Fred H. Cate, "Comments to the White House 60-Day cybersecurity review" http://www.whitehouse.gov/files/documents/cyber/Center%20for%20Applied%20Cybersecurity%20Research%20-%20Cybersecurity%20Comments.Cate.pdf (accessed 01/31/2013), 3
[106] Harknett and Stever, *The Cybersecurity Triad: Government, Private Sector Partners, and the Engaged Cybersecurity Citizen*, 10

should not be an afterthought for the average citizen, but engrained within a nation's populace and deeply rooted in the citizens' day to day activities. To do so, stronger relationships between government and its citizens, as well as an improved education effort aimed at reinforcing cybersecurity are essential components required to strengthen the cybersecurity of critical infrastructure. In the end, the general population must act as active cybersecurity providers, and not solely as simple beneficiaries of a nation's cybersecurity strategy.[107]

The Unites States of America

The origins of the U.S. Cybersecurity efforts to protect critical infrastructure begun in 1996 when President Clinton issued Executive Order 13010 titled *Critical Infrastructure Protection*. It established the President's Commission on Critical Infrastructure Protection, and concluded that cyber attacks posed a threat to the economic and national security of the nation.[108] The recommendations of the commission led to the issuance of Presidential Decision Directive (PDD) 63 in May 1998, establishing several organizations focused on cybersecurity such as the National Coordinator for Security, Infrastructure Protection, and Counterterrorism. It also proposed the formation of the Information Sharing and Analysis Centers (ISACs), which today provide a key role in the public-private partnership necessary to secure cyberspace. Briefly, ISACs are trusted entities established by critical infrastructure owners and operators to provide comprehensive sector analysis, to include risk mitigation, alerts, and actionable

[107] Ibid., 11
[108] Kevin P. Newmeyer, "Who should Lead U.S. Cybersecurity Efforts?" *PRISM* 3, no. 2, 116-117

information, which is shared within and across sectors and with the government.[109] Through the standup of ISACs, the Clinton administration effectively focused on the public-private partnership as the means to secure cyberspace.[110]

The events on 9/11 significantly changed the focus of the threat on critical infrastructure from cyber attacks to physical attacks from terrorist groups. In 2003, the Bush Administration released the *National Strategy to Secure Cyberspace*, which was criticized as not being a comprehensive strategy but merely a compilation of recommendations.[111] In 2008, the *Comprehensive National Cybersecurity Initiative* was published but largely criticized to focus almost exclusively on the government internet domain (.gov). In short, Kevin Newmeyer explains that during the Bush administration, cybersecurity responsibility was vague, with limited leadership and diluted responsibility in the White House, Homeland Security, and DOD.[112]

When President Obama took over the presidency, he ordered a 60-day review of all government activities regarding cybersecurity. In May 2009, the *60-day Cybersecurity Review* was released and presented a detailed summary of the current efforts underway but came short in details on how the recommendations were going to be implemented. The key point from the review was the recommendation to appoint a cybersecurity policy official at the White House to serve as the central coordinator for government and national efforts, a position which would be filled in December 2009.[113] In May 2011, the White House issued the *International Strategy to Secure Cyberspace*, focusing on the

---

[109] National Council of ISAC, "Information Sharing and Analysis Centers" http://www.isaccouncil.org/aboutus.html (accessed 04/06/2013)
[110] Newmeyer, *Who should Lead U.S. Cybersecurity Efforts?*, 117
[111] Ibid.
[112] Ibid.
[113] Ibid.

U.S. efforts at the international stage to address cybersecurity challenges.[114] Despite the various policy documents and cybersecurity directives issued by the White House, the United States are still faced with the issue of not having a consolidated, integrated cybersecurity strategy that clearly highlights roles and responsibilities in securing cybersecurity for critical infrastructure.

In the last two years, the United States have been aggressively trying to mitigate the cyber threat facing critical infrastructure by introducing legislation that would increase oversight from the federal government. For example, the Cybersecurity Act of 2012 (S.3414), also known as the Lieberman-Collins Act, was introduced on 19 July 2012 to the U.S. Senate.[115] Similarly, President Obama signed Executive Order 13636 titled *Improving Critical Infrastructure Cybersecurity* on 12 February 2013, in an attempt to enhance cybersecurity through a collaborative effort between federal agencies and owners and operators of privately owned critical infrastructure.[116] Given the absence of comprehensive cybersecurity legislation, some contend the E.O. is a step in the right direction. Others argue that "the move could lead to government intrusiveness into private-sector activities, for example through increased regulation under existing statutory authority."[117] The impact of these initiatives on the future approach to cybersecurity of critical infrastructure will be discussed in greater details in chapter 5.

---

[114] Ibid.
[115] United States Senate Committee on Homeland Security and Governmental Affairs, "The Revised Cybersecurity Act of 2012 S.3414 (Introduced July 19, 2012)" (accessed 04/08/2013), 1
[116] Congressional Research Service, "The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress" http://www.fas.org/sgp/crs/misc/R42984.pdf (accessed 04/08/2013), summary
[117] Ibid.

Certainly, the interconnectedness of critical infrastructure between Canada and the United States is a major element of a cybersecurity strategy. As Canada's threat level is directly linked to that of the United States, both in real and perceived terms, close cooperation between both nations is must.[118] This close cooperation is seen in the two governments signing the *Canada-United States Action Plan on Critical Infrastructure* in 2011, calling for greater cooperation and coordination between the nations. Moreover, the *Action Plan* recognizes that regional approaches to cross-border collaboration need to be guided by an overarching Canada-U.S. framework.[119] Certainly, regional considerations must be recognized as individual regions face unique challenges across the continent. While the focus on the electrical grid might be more prevalent between Ontario, Quebec and the North East Sector of the United States, the oil and gas sector likely has increased co-dependence in Alberta, British Columbia and the southern States sharing their borders.

Summary

It is evident that the responsibility to enhance the cybersecurity of critical infrastructure is shared between several key actors. Compounding the problem is the transborder nature of these interconnected systems. One thing is clear: cyber threats facing critical infrastructure are real, and countering the threat demands leadership as the highest level of government and the private sector. Yet, it is a complex endeavor. As the GAO indicated, multi-agency coordination issues and a lack of top-level leadership are major impediments to cybersecurity. The situation cannot be allowed to continue; there is too much at stake. [120]

---

[118] Graham, *Canada's Critical Infrastructure: When is Safe enough Safe enough?*, 17
[119] Ibid., 20
[120] Newmeyer, *Who should Lead U.S. Cybersecurity Efforts?*, 118

CHAPTER 4 – CURRENT NATIONAL STRATEGIES AND GOVERNANCE

In order to properly guide and implement a national strategy geared at protecting critical infrastructure against cyber threats, it is important to review and understand the various policies, strategies, and regulatory frameworks driving the activities of the government, the private sector, and other key stakeholders. Moreover, the strategies and plans developed by the government are based on the legal framework available to them.[121] In its report tabled in the House of Commons in the Fall 2012, the Auditor General referenced several source documents to guide the audit and evaluate the effectiveness of the federal government in meeting its leading and coordinating roles and responsibilities to protect the nation's critical infrastructure against cyber threats. Of importance, the *National Security Policy*, the *Emergency Management Act*, the *National Strategy and Action Plan for Critical Infrastructure*, as well as *Canada's Cyber Security Strategy* were used as a baseline to assess the effectiveness of the federal government in meeting its mandate.[122] To determine whether the current policies and legislative frameworks are sufficient for the government to meet its mandate of protecting the nation, an overview of each document is provided and corroborated against the requirement of the government to act when owners and operators of critical infrastructure fail to meet an adequate cybersecurity posture.

---

[121] United States Government Accountability Office, *Cybersecurity: National Strategy, Roles, and Responsibilities Need to be Better Defined and More Effectively Implemented*, 1

[122] Office of the Auditor General of Canada, *Report of the Auditor General of Canada to the House of Commons: Protecting Canadian Critical Infrastructure Against Cyber Threats*, 26

The National Security Policy

In April 2004, the Government of Canada took the historic step of issuing the first-ever National Security Policy (NSP). Titled *Securing an open society*, the document highlights the framework upon which the government intends to address national security concerns while adopting an integrated approach within the government and with key partners. It focuses on three core national security interests: protecting Canada and Canadians at home and abroad, ensuring Canada is not a base of threats to our Allies, and contributing to national security.[123] Of note, the policy clearly highlights the need to balance national security concerns with the protection of core Canadian values such as openness and respect for civil liberties.[124] Certainly, this element is an important factor to consider when discussing options for the government to strengthen the cybersecurity of critical infrastructure, which will be discussed in greater details in chapter 5.

The NSP expands on six key strategic areas related to national security, builds upon existing initiatives, addresses security gaps, and highlights guidelines on how each strategic area will be implemented.[125] Of importance, one of the key strategic area centers on building capacity in preventing and predicting cyber attacks. Specifically, it acknowledges that cyber attacks on critical infrastructure are a growing concern for the nation given the increased vulnerability of these critical assets.[126] Moreover, the NSP clearly states that a seamless national emergency management system requires a comprehensive and contemporary legislative foundation. As such, the NSP broaches the need to review and modernize the government statutory framework, including the

[123] Privy Council Office, *Securing an Open Society: Canada's National Security Policy*, vii
[124] Ibid.
[125] Ibid., viii
[126] Ibid., 7

Emergency Preparedness Act, to reflect emerging requirements such as critical infrastructure protection and cybersecurity.[127] Acknowledging that critical infrastructure protection is one of the main challenges of modern emergency management, it announces the release of a position paper that would highlight Canada's strategy towards critical infrastructure protection. It equally announces the creation of a high-level national task force to develop Canada's cyber security strategy, which would be released six years later in 2010.[128]

In essence, the National Security Policy falls short of providing the government the regulatory tools required to address the cybersecurity challenges facing critical infrastructure. For example, the NSP proposes implementing mandatory regulatory standards to strengthen security at port and other marine facilities that will require operators of marine facilities to have plans in place that address security vulnerabilities.[129] However, it does not propose similar initiatives to address cybersecurity concerns. While the direction to review the government statutory framework is a step in the right direction, it proves to be insufficient to fully address the scope of the problem.

[127] Ibid., 24
[128] Ibid., 26
[129] Ibid., 39

The Emergency Management Act

Nearly three years after the release of the NSP, the Minister of Public Safety announced the coming into force of the new *Emergency Management Act* on 07 August 2007. In a nutshell, the updated *Act* enhanced collaborative emergency management and improved information sharing with other levels of government as well as the private sector.[130] First and foremost, the *Constitution Act of 1867* states that provinces and territories have primary responsibility for emergency management within their respective jurisdictions. However, the modernization of the *Emergency Preparedness Act* announced in the *National Security Policy* gave the Minister of Public Safety the responsibility for "exercising leadership relating to emergency management in Canada by coordinating, among government institutions and in cooperation with the provinces and other entities, emergency management activities."[131] Additionally, the *Act* further defines the term "emergency management" which encompasses four interdependent components: prevention and mitigation, preparedness, response, and recovery.[132] With respect to prevention and mitigation initiatives, these include structural and non-structural mitigation measures such as developing building codes.[133] Therefore, one could argue that the development of minimum cybersecurity standards or similar directives aimed at strengthening cybersecurity of critical infrastructure could fall within the prevention and mitigation initiatives within the *Act*. However, it is not currently the case as much of the

---

[130] The Emergency Management Act came into force on 03 August 2007. Public Safety Canada, "Minister Day Announces the New Emergency Management Act" http://www.publicsafety.gc.ca/media/nr/2007/nr20070807-1-eng.aspx (accessed 04/06/2013)
[131] "Emergency Management Act" http://laws-lois.justice.gc.ca/PDF/E-4.56.pdf (accessed 04/06/2013), paragraph 3
[132] Emergency Management Policy Directorate, "An Emergency Management Framework for Canada" Public Safety Canada, http://www.publicsafety.gc.ca/prg/em/_fl/emfrmwrk-2011-eng.pdf (accessed 03/09/2013), 4
[133] Ibid.

involvement from Public Safety, and the government as a whole, has been solely centered on coordination, discussion, and information sharing.

Although the *National Security Policy* clearly highlighted the requirement to modernize the *Emergency Preparedness Act* to include emerging requirements such as cyber security[134], the release of the new *Act* fell short of specifically addressing cybersecurity. In fact, the term "cyber" does not even appear in the wording of the *Act*. Instead, it briefly describes the emergency management responsibilities of ministers accountable to Parliament, more specifically in identifying the risks within or related to the ministers' area of responsibility, including those related to critical infrastructure. More precisely, the *Act* requires ministers: to prepare emergency management plans in respect of those risks; to maintain, test and implement those plans; and to conduct exercises and training in relation to those plans.[135] Additionally, the *Emergency Management Act* and the *Department of Public Safety and Emergency Preparedness Act* do not contain regulations reinforcing the *Acts*, unlike the *Firearms Act* which lists over seventeen regulations supporting it.[136] Moreover, a cursory review of the Public Safety Forward Regulatory Plan (2012-14), which provides information on regulatory proposals that Public Safety Canada expects to bring forward over the next two years, does not list any regulatory proposals regarding cybersecurity.[137]

Thus, the *Emergency Management Act* does not provide the government the required legislative authority to compel the owners and operators of critical infrastructure

---

[134] Privy Council Office, *Securing an Open Society: Canada's National Security Policy*, 24-25
[135] *Emergency Management Act*
[136] Public Safety Canada, "List of Acts and Regulations," http://www.publicsafety.gc.ca/abt/ctsnrg/lstcts-eng.aspx (accessed 04/06/2013)
[137] Public Safety Canada, "Forward Regulatory Plan: 2012-2014" http://www.publicsafety.gc.ca/abt/ctsnrg/frwrdrg-12-14-eng.aspx (accessed 04/06/2013)

to improve the cybersecurity of the nation's critical systems if the situation warrants such action.

The National Strategy for Critical Infrastructure

In 2009, the Canadian federal government released the *National Strategy on Critical Infrastructure*, along with the supporting *Action Plan for Critical Infrastructure*. Briefly, the plan identifies ten critical infrastructure sectors as essential capabilities to sustain the nation: energy and utilities, finance, food, transportation, government, information and communication technology, health, water, safety, and manufacturing. Additionally, it clarifies that the national strategy's primary goal is to strengthen the resiliency of the national critical infrastructure through three strategic objectives: build partnership, implement an all-hazard risk-management approach, and improve the information sharing and protection amongst partners.[138] In essence, the *National Strategy for Critical Infrastructure* complements the *Emergency Management Framework* for Canada, which embraces partnership and a collaborative approach between the private sector responsible for critical assets and federal, provincial, and territorial governments. Also, the strategy reinforces the requirement for enhanced information sharing and information protection, and identifies a risk management approach to strengthen the resiliency of critical infrastructure.[139] Finally, the strategy was released in conjunction with the *Action Plan for Critical Infrastructure* which sets out action items and provides greater granularity on how the strategy is to be implemented.

[138] Government of Canada, *National Strategy for Critical Infrastructure*, 3
[139] Ibid., 5

The *Action Plan for Critical Infrastructure* centers on the main characteristics of the national strategy: establish a sustainable partnership, improve information sharing, and commit to an all-hazards risk management approach.[140] As such, the *Action Plan* announces the building blocks of the information sharing framework, initially focusing on the establishment of sector networks and the standup of a National Cross-Sector Forum. First, the purpose of sector networks is to provide a forum of collaboration in conducting risk assessment, developing plans, and enhancing information sharing within each critical infrastructure sector.[141] Likewise, the main objective of the National Cross-Sector Forum is "to promote collaboration across the sector networks, address interdependencies and promote information sharing across sectors."[142] Second, the plan acknowledges that an information protection framework needs to be developed to accelerate the distribution of information related to cyber threats, improve the quality of information, and prevent the inappropriate disclosure of sensitive information. The plan equally noted that the development of the information sharing and protection protocol must respect the existing legislation and policies related to the sharing and disclosure of protected and classified information.[143] Finally, the plan introduces the implementation of a risk management system through the development of sector risk profiles at the national level, the conduct of risk assessments, and the provision of risk management tools and guidance.[144] Given that the owners and operators of critical infrastructure are responsible to manage the risks related to their specific areas and are cognizant of the risk factors

[140] Government of Canada, *Action Plan for Critical Infrastructure*, 2
[141] Ibid., 4
[142] Ibid., 5
[143] Ibid., 7
[144] Ibid., 8

facing their systems, key limitations driven from a lack of access to relevant and up-to-date cyber threats information hamper their ability to manage risk effectively.

The *National Strategy for Critical Infrastructure* and its associated *Action Plan* simply reinforce the will of the government to maintain a coordinating role in the security of the nation's critical infrastructure. Thus, the *National Strategy on Critical Infrastructure* is essentially founded on the principles of information sharing, collaboration, and partnerships and as such does not provide the force of increased government authority when critical infrastructure owners fail to address critical cybersecurity concerns.

Canada's Cyber Security Strategy

Released in 2010, *Canada's Cyber Security Strategy* is the cornerstone document of the federal government to address the challenges of cyberspace. It embraces the roles of government, the private sector, and Canadian citizens play in securing the cyber environment. In a simplistic form, the strategy mainly leverages on partnerships established under the *National Strategy and Action Plan for Critical Infrastructure*, clarifies the roles and responsibilities of key federal departments, elaborates on the various threats facing the cyber environment, and more importantly confirms that the Canadian economy and the security of the nation is closely tied to the availability of critical assets which could be disrupted from malicious activity carried through cyberspace.[145] Moreover, it designates cyberspace as a strategic asset.[146]

[145] Government of Canada, *Canada's Cyber Security Strategy*, 1
[146] Ibid., 3

The strategy is effectively built on three pillars: securing government systems, partnering to secure vital cyber systems outside the federal Government, and helping Canadians to be secure online.[147] First, the government intends on securing government systems by establishing clear federal roles and responsibilities, by strengthening the security of federal cyber systems, and by enhancing security awareness throughout the government. More specifically, the strategy proposes to reduce the number of internet access points connecting the government networks, and intends on strengthening processes to address security gaps inherent to the global IT supply chain.[148] However, it does not provide a plan detailing how it would achieve this. Secondly, the strategy proposes to secure vital systems outside the federal Government by building on existing programs to better support cybersecurity research and development activities, such as the Defence Research and Development Canada's Public Security Technical Program.[149] Specifically to critical infrastructure, the strategy reinforces the need to strengthen a public-private partnership through increased collaboration with provincial, municipal, and territorial governments as well as private partners.[150] However, the strategy does not properly address the impact and significance of cross-national disruption of critical infrastructure through cyber attacks. Indeed, it simply states: "[f]or this reason, Canada will be active in international fora dealing with critical infrastructure protection and cyber security."[151] Therefore, it does not detail how Canada intends to engage with its most significant partner and stakeholder in critical infrastructure protection: the United

[147] Ibid., 7
[148] Ibid., 10-11
[149] Ibid., 11
[150] Ibid., 12
[151] Ibid.

States.[152] Thus, "the strategy fails to address the international and policy imperatives that cyber security requires."[153] Finally, the strategy plans to help Canadians to be more secure online by establishing a Royal Canadian Mounted Police (RCMP) Integrated Cyber Crime Fusion Centre, and by introducing new legislation to enhance the capacity of law enforcement agencies to investigate and prosecute crimes committed in cyberspace.[154]

The *National Cyber Security Strategy* identifies a need for adequate legislation "to modernize law enforcement's investigative power, and ensure that technological innovations are not used to evade lawful interceptions of communications supporting criminal activity".[155] Indeed, the strategy highlights the requirement to ratify the Council of Europe's *Convention of Cybercrime*.[156] In essence, the legislative elements necessary to ratify the *Convention of Cybercrime* are found in Bill C-30 – the *Protecting Children from Internet Predators Act*.[157] However, the Bill was essentially shelved in February 2013 following strong opposition from civil liberties and privacy advocates[158], despite being strongly backed by police forces who argue that legislation has not kept up with

[152] Victor Platt, "Still the Fire-Proof House? an Analysis of Canada's Cyber Security Strategy" http://www.academia.edu/1534361/Still_the_fire_proof_house_An_analysis_of_Canadas_Cyber_Security_Strategy (accessed 04/11/2013), 165
[153] Ibid., 167
[154] Government of Canada, *Canada's Cyber Security Strategy*, 13
[155] Ibid., 3
[156] Ibid., 8
[157] Jordan Press, "Tories Face International Pressure to Pass Cybercrime Provisions, Documents show - Canada.Com" http://o.canada.com/2012/11/27/tories-face-international-pressure-to-pass-cybercrime-provisions-documents-show/ (accessed 04/09/2013)
[158] Bruce Cheadle, "Bill C-30, Tory Internet Surveillance Legislation, is Officially Dead - the Huffington Post" http://www.huffingtonpost.ca/2013/02/11/bill-c-30-dead-internet-canada_n_2664458.html (accessed 04/11/2013)

technology.[159] Despite being a signatory to the convention in 2001, Canada has yet to ratify the convention amidst increased pressure from the U.S., the United Kingdom, and other Allies to do so.[160] Also, the strategy announces that the Department of National Defence and the Canadian Forces will work with Allies to develop a policy and legal framework for military aspect of cybersecurity.[161] However, the strategy falls short of proposing any additional legal or legislative instruments adequate to bolster the cybersecurity of critical infrastructure.

While the *National Cyber Security Strategy* is a first step in the right direction, it does not properly address the national security implications resulting from cybersecurity vulnerabilities inherent to the nation's critical infrastructure, more specifically in providing the legislative tools available to the government to address the problem. As Ron Diebert states: "[Canada's] cyber security strategy…pales in comparison to the scope of the challenges, or to equivalent strategies released by our allies, like the United States."[162] He further explains that "[i]t devotes far too few resources to the problem, does not fully address the division of appropriate institutional responsibilities, and only barely nods at the importance of a foreign policy for cyberspace."[163]

---

[159] Jordan Press, "Current Laws Not Focused enough to Combat Child Porn Online: RCMP - the National Post" http://news.nationalpost.com/2012/02/21/current-laws-not-focused-enough-to-combat-child-porn-online-rcmp/ (accessed 04/11/2013)
[160] Press, *Tories Face International Pressure to Pass Cybercrime Provisions, Documents show - Canada.Com*
[161] Government of Canada, *Canada's Cyber Security Strategy*, 10
[162] Diebert, *Cyber Security: Canada is Failing the World*
[163] Ibid.

Summary

The evolution of strategies, policies, and frameworks related to the cybersecurity of critical infrastructure over the last decade has largely been based on one common denominator: partnership. Certainly, the need for increased collaboration between government institutions and private actors is a hard requirement given the complexity of these interconnected systems. However, it is not enough given the potential impact to national security. As described in the Auditor General report:

> …Public Safety Canada is responsible for exercising national leadership on public safety and emergency preparedness. But Public Safety Canada does not direct provinces, territories, critical infrastructure owners, or other federal departments on how to carry out their activities. Based on OCIPEP's mandate, the National Security Policy, the National strategy and action plan for critical infrastructure, and Canada's Cyber Security Strategy, Public Safety Canada is to exercise its leadership and coordination role by providing unique support and services to critical infrastructure owners and operators that otherwise may not be available to them. These include: building partnerships and providing a forum for advancing the timely sharing of cyber threat information among stakeholders; monitoring the international and national cyber threat environment to obtain timely and relevant warnings of cyber security vulnerabilities and to analyze cyber threats to critical infrastructure stakeholders; and building critical infrastructure protection capacity through an enhanced policy framework, education and awareness, and research and development.[164]

The question remains why the government is not adopting a more assertive posture to protect the nation's critical infrastructure. As seen above, the government does

[164] Office of the Auditor General of Canada, *Report of the Auditor General of Canada to the House of Commons: Protecting Canadian Critical Infrastructure Against Cyber Threats,* 8

not have a supporting legislative or regulatory framework in place to compel the private industry to bolster the cybersecurity of critical infrastructure, either in the form of mandating minimum cybersecurity standards across the critical infrastructure networks or through other initiatives available at the discretion of the government. Yet, the problem is not unique to Canada. As Michael Chertoff explains, "[d]espite various [U.S.] government efforts, cybersecurity has become an increasingly urgent problem . . . Nevertheless, there is still no comprehensive legislative architecture for cyber defense and security in place today."[165] However, recent initiatives south of the border resemble a pendulum shift in the way the nation is addressing this issue.

Essentially, the current legislative framework guiding the cybersecurity of critical infrastructure needs to be reevaluated to provide the government tools with teeth. Moreover, history shows that legislations have been adopted by governments when forced to address immediate national security concerns. Certainly, the United States have recognized that the current situation is no longer manageable, and that involvement from the federal government is necessary to protect its critical assets. After all, it is the responsibility of the government, and a matter of national security.

[165] United States Senate Committee on Homeland Security and Government Affairs, *Statement for the Record by the Honorable Michael Chertoff - February 16, 2012*

CHAPTER 5 – THE NEED FOR INCREASED GOVERNMENT OVERSIGHT

The Status Quo Is No Longer Supportable

The public debate on the value of increased government involvement in protecting critical infrastructure has been occurring for well over a decade. Whether current efforts provided by the private sector are sufficient in defending against the plethora of cyber threats facing critical infrastructure remains to be solved. Supporters of stronger government efforts argue that oversight is crucial to improve security and that the subsequent increase in security will reduce uncertainty and positively influence the economy.[166] On the other hand, opponents argue that unnecessary costs, difficulties in determining requirements and measuring compliance, and dealing with boundaries that intersect networks and nations are sufficient to quash any desire for further government involvement.[167]

Looking back at progress made over the last decade to increase protection of critical infrastructure from cyber attacks, it is clear that maintaining the current approach is not adequate to address national security concerns. In fact, the status quo is no longer supportable. Recall the discussion in Chapter 3 which details how the current cyber strategy is built solely on information sharing and partnership. Certainly, the Auditor General report on the federal government efforts to protect Canadian critical infrastructure against cyber threats has made some unnerving conclusions. The fact that some sector networks were not fully established more than eleven years after the decision was made to establish partnership with other governments and private sector owners and

[166] Fischer, *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options*, 50
[167] Ibid.

operators in a case in point. As a result, this breakdown hinders on Public Safety's ability to communicate with industry partners and disseminate critical vulnerabilities and threats to specific sectors.[168] In addition, some private sector owners reported that they were unsure whether cyber attacks should be reported to the Government, and to which agency, clearly underlining the inefficiency of the current approach.[169] Indeed, Scott Charney aptly concluded that "[f]or more than a decade, the government and the private sector have partnered to address various aspects of cybersecurity, but this partnership has not achieved the robust results that are needed to protect cyberspace effectively."[170]

At the root of the debate on cybersecurity regulation is the infringement on the economy and its potential adverse effect on innovation. In a sense, private companies argue that the private sector has significant financial incentive to increase cybersecurity, especially in reducing fraud, and that is in itself sufficient in protecting the nation's critical assets. However, market-based solutions alone will not cumulatively lead to a more secure cyber environment.[171] While the financial sector may be best positioned to reduce fraud, security often takes a back seat to consumer convenience. Also, financial incentives are not necessarily predominant in all critical sector networks, such as in the chemical and water sectors. Fred H. Cate, Director of the Center for Applied Cybersecurity Research at Indiana University, provides the following observation:[172]

> While I would argue it is almost always preferable to allow markets to create appropriate incentives for

[168] Office of the Auditor General of Canada, *Report of the Auditor General of Canada to the House of Commons: Protecting Canadian Critical Infrastructure Against Cyber Threats*, 2
[169] Ibid., 16
[170] United States House of Representatives, *Written Testimony of Scott Charney, Corporate Vice President, Microsoft Corporation's Trustworthy Computing*, 4
[171] Harknett and Stever, *The Cybersecurity Triad: Government, Private Sector Partners, and the Engaged Cybersecurity Citizen*, 7
[172] Cate, *Comments to the White House 60-Day cybersecurity review*, 4

> desired behaviors, there are occasions where government intervention is necessary. Information security is one of those instances. The threats are too broad, the actors too numerous, the knowledge levels too unequal, the risks too easy to avoid internalizing, the free-rider problem too prevalent, and the stakes too great to believe that markets alone will be adequate to create the right incentives or outcomes.

In summary, it is apparent that the current situation is no longer supportable, and that market incentives and partnership alone will not lead to an improved cybersecurity posture for critical infrastructure. In fact, recent initiatives to increase government oversight in cybersecurity are a case in point.

Government Legislation South of the Border

Given the criticality of addressing the threats facing critical infrastructure, it is not surprising to notice a shift in the interest shown by governments to address this emergent challenge. While the Canadian government is currently maintaining its leadership through collaboration and partnership, the most significant proposals to legislate cybersecurity of critical infrastructure have been materializing south of the border. In fact, these initiatives have been directly endorsed by the President of the United States. In a rare move, President Obama wrote and published an op-ed article in the Wall Street Journal in July 2012 in order to garner enough support from Congress to pass the Cybersecurity Act of 2012.[173] Commonly known as the Lieberman-Collins bill, the legislation proposed a public-private partnership and the establishment of a National Cybersecurity Council: an agency composed of members from the Defense Department, Justice, Commerce, the intelligence community, as well as sector-specific

[173] Obama, *Taking the Cyberattack Threat Seriously - Wall Street Journal*

representatives, with an overall responsibility of regulating the cybersecurity of covered critical infrastructure.[174] President Obama's article clearly highlights that cybersecurity is a priority for his administration and that adopting comprehensive cybersecurity legislation is essential to strengthen the nation's critical infrastructure. While he makes it clear that developing cybersecurity standards need to be done in partnership between government and the industry, he equally emphasizes that the approach needs to protect privacy and civil liberties, and crafted with ideas originating from the industry. However, he argues that the sharing of information between the two is not sufficient in filling the existing security gaps.[175] More specifically, the President highlights that many companies are lacking the most basic cyber protection measures, putting public safety and national security at risk. As a case in point, he states that nuclear power plants must have fences around their facilities to defend against terrorist attacks, water treatment plants must test their water regularly for impurities, airplanes require secure cockpit doors, and as such "[i]t would be at the height of irresponsibility to leave a digital backdoor wide open to our cyber adversaries."[176]

The bill received strong endorsement from the highest level of federal departments as well as several key industry leaders. The Chairman of the Joint Chiefs of Staff fully endorsed the proposal, stating: "I appreciate your leadership on this urgent issue of national security and share you view that only legislative remedy will enable our

[174] United States Senate, "Letter to Colleagues: Cybersecurity Act of 2012 (S.3414)" http://www.hsgac.senate.gov/download/cybersecurity-dear-colleague (accessed 2/10/2013)
[175] Obama, *Taking the Cyberattack Threat Seriously - Wall Street Journal*
[176] Ibid.

Nation to adequately address the cyber threat."[177] In his letter of support, he further emphasized that a comprehensive cybersecurity legislation needs to be based on three tenets: the real-time sharing of threat information between the public and private industry, the adherence of minimum security standards to harden the resiliency of the critical infrastructure, and the imperative of the Department of Defense to work closely with the industry partners to prevent the exfiltration of sensitive information. The Director of the National Security Agency equally expressed his strong support for the proposal, citing that information sharing alone is insufficient in addressing the core vulnerabilities of Nation's critical infrastructure.[178] Likewise, the Silicon Valley Leadership Group which represents more than 375 of Silicon Valley's most respected employers was also very supportive of the bill. The group recognizes that "the legislative progress on cybersecurity is an important step towards protection of personal information", and also supports the adoption of a single, federal standard for data breach notification and security.[179]

According to Michael Chertoff, the approach taken in the Lieberman-Collins bill to securing private critical infrastructure is important. Specifically, the proposal recognizes that, for identified highly critical infrastructure, outcome-based performance standards are necessary rather than imposing detailed security regimes.[180] While these

---

[177] Chairman of the Joint Chiefs of Staff, "Letter of Support to the Chairman of the Committee on Commerce, Science, and Transportation" http://www.hsgac.senate.gov/download/cybersecurity-support-letter-joint-cheifs-of-staff-chairman (accessed 2/10/2013)
[178] Director of the National Security Agency, "Letter to the Honorable Harry Reid" http://www.hsgac.senate.gov/download/cybersecurity-support-letter-general-keith-alexander (accessed 04/06/2013)
[179] Silicon Valley Leadership Group, "Letter of Support to S.3414 the Cybersecurity Act of 2012" http://www.hsgac.senate.gov/download/cybersecurity-support-letter-silicon-valley-leadership-group (accessed 04/06/2013)
[180] United States Senate Committee on Homeland Security and Government Affairs, *Statement for the Record by the Honorable Michael Chertoff - February 16, 2012*

performance standards would provide private owners the flexibility to innovate in achieving security, the proposal would also require them to demonstrate that they have attained that appropriate level of security. Interestingly, Chertoff elaborates that "similar performance-based approaches work well in promoting physical security in our ports, transportation networks, and other key infrastructure."[181]

Despite the support from several high-ranking military officers, national security officials and private industry leaders, the bill was voted down in the Senate by a margin of 52 to 46 in favor of the bill, coming up short of the two-third majority required to move the bill to its final vote.[182] In the end, it is widely believed that the U.S. Chamber of Commerce had significant influence against the bill[183], supporting the argument that cybersecurity legislation has historically been opposed on the grounds that it would negatively affect the economy. Notwithstanding the disappointing result, President Obama countered by issuing Executive Order (E.O.) 13636 on 12 February 2013.[184] Titled *Improving Critical Infrastructure Cybersecurity*, the E.O. was issued primarily to address the lack of cybersecurity legislation in the absence of congressional action.[185] While the purpose of this paper is not to determine the authority and legal power attached to the Executive Order, it remains an important step towards bolstering a legislative framework to counter the threats posed by cyberspace on critical infrastructure, and

---

[181] Ibid.
[182] Ed O'Keefe and Ellen Nakashima, "Cybersecurity Bill Fails in Senate - the Washington Post" http://www.washingtonpost.com/world/national-security/cybersecurity-bill-fails-in-senate/2012/08/02/gJQADNOOSX_story.html (accessed 4/6/2013)
[183] Ibid.
[184] Congressional Research Service, *The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress*, 1
[185] Ibid., 7

certainly provides an indication of what is on the horizon for the foreseeable future. Certainly, the press release of E.O. 13636 offered the following unmistakable insight:

> The Administration continues to believe that legislation is needed to fully address this threat. Existing laws do not permit the government to do all that is necessary to better protect our country. The Executive Order ensures that federal agencies and departments take steps to secure our critical infrastructure from cyber attack, as a down-payment on expected further legislative action.[186]

Although the E.O. clearly stipulates that it provides no additional authority to an agency for regulating critical infrastructure beyond what currently exists under law, it reassigns new roles to some federal agencies and is widely based on other legislative proposals such as the Cybersecurity Act of 2012 (S.3414) .

Under the new construct, Executive Order 13636 expands a Department of Homeland Security program for information sharing to a greater audience, establishes a consultative process for high priority critical infrastructure, and requires existing regulators to assess the adequacy of the existing posture as well as determine their authority to address those risks. One component that is unique to E.O. 13636 is the new mandate assigned to the National Institute of Standards and Technology (NIST) to lead in developing a Cybersecurity framework of standards and best practices for protecting critical infrastructure.[187] However, unlike the provisions contained in the Lieberman-

---

[186] Office of the Press Secretary to The White House, "Executive Order on Improving Critical Infrastructure Cybersecurity" http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0 (accessed 04/12/2013)

[187] Congressional Research Service, *The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress*, 11

Collins bill, the E.O. does not provide for exemption of liability resulting from information sharing since it would require changes to current laws.[188]

Regardless of the details, provisions, and exclusions embedded in the *Cybersecurity Act of 2012* and the Executing Order 13636, one common denominator can be extracted from these initiatives: the current approach does not work and needs to change. Moreover, the strengthening of the legislative framework in the United States is of significant importance to Canada. Given the interconnectedness of the critical infrastructure between the two nations, the reality of a new approach in the United States cannot simply be overlooked by the Canadian government.

Why Governments Regulate

Government regulation is not a new concept in today's society. Certainly, the government is highly involved in legislating and imposing rules, mandatory standards and procedures in areas that affect public health and safety, or impact national security. However, history has shown that government legislation in certain domains have often been prompted by a major disrupting event, or a situation that had gotten out of control. For example, the *National Security Policy* highlights that the tragic bombing of Air India Flight 182 in 1985 prompted the government to implement measures to search passengers and baggage, as well as conducting background checks for airport workers.[189] Similarly, commercial airlines were individually responsible and accountable for passenger screening and security personnel prior to the attacks on the United States on 11 September 2001. Realizing that a major security gap existed within the airline industry,

[188] Ibid.
[189] Privy Council Office, *Securing an Open Society: Canada's National Security Policy*, 36

the federal government created the Canadian Air Transport Security Authority (CATSA) on 01 April 2002 to standardize and strengthen aviation security screening in Canada.[190] In the United States, the Center for Strategic and International Studies indicated that it took nearly 40 years for Congress to mandate safety regulation on steamboats which regularly blew up. Moreover, over half a century had passed before the U.S. government enacted automobile safety rules due to stiff opposition from the carmakers, and nearly 23 years elapsed before the first set of air safety regulation appeared after the first fatal air crash.[191] Nonetheless, historical opposition from the industry has steadily relied on the argument that legislation would stifle innovation and negatively impact the economy. Given the substantial advancements and developments in each domain, this argument lacks punch at best.

Regulations are rules used to carry out the intent of Acts enacted by the Parliament of Canada. Therefore, they are instruments of legislative power and have the force of law. More specifically, regulations are meant to complement and expand on specific guidelines not usually found in parliamentary Acts. Such examples include definitions, licensing requirements, performance specifications, exemptions, forms, and other supporting requirements.[192] One critical determinant of a sound regulatory system is that it must achieve its intended goal by adopting the least disrupting approach possible. Also, regulations must meet some general principles in order to be effective. First, it must protect public health, welfare, and safety while promoting economic growth, innovation,

---

[190] Canadian Air Transport Security Authority, "Stepping Forward: Annual Report 2010" http://www.catsa-acsta.gc.ca/file/library/87/english/AnnualReport2010.pdf (accessed 02/10/2013), 5

[191] Center for Strategic and International Studies, "Cybersecurity Two Years Later" http://csis.org/files/publication/110128_Lewis_CybersecurityTwoYearsLater_Web.pdf (accessed 04/06/2013), 1

[192] Transport Canada, "List of Regulations," http://www.tc.gc.ca/eng/acts-regulations/regulations.htm (accessed 04/06/2013)

and competitiveness.[193] Certainly, a regulatory system must not impede on job creation and maximizes on net benefits. Regulatory systems must also allow, to the extent feasible by law, for public participation and foster open exchange of ideas. Moreover, it must be based on the best science available and use the best tools to achieve regulatory aims.[194] To do so, the objectivity of scientific and technological information used to support the regulatory actions must be maintained. Finally, an effective regulatory system must take into account qualitative and quantitative benefits and costs, be measurable, and seek to improve the actual results of regulatory requirements.[195]

Many arguments have been put forth to oppose the involvement of government in matters that would be better left to the private sector to manage. For example, many suggest that governments cannot adapt to rapid change and thus quickly fall behind with respect to public policies while cyber attacks and strategies keep evolving.[196] Equally, others believe that the linear and hierarchical structure of many government organizations often impede on the ability of the government to quickly react to fast-changing situation as required in cybersecurity.[197] As described previously, others contend that market incentives are sufficient to drive the cybersecurity resilience of critical infrastructure. Despite the limited validity of these statements, one of the main issues with critical infrastructure is that inadequate cybersecurity in one sector can have a significant impact on others[198], and therefore market incentives are not mutually exclusive. Also, some argue that cybersecurity is fundamentally a public good and therefore require government

---

[193] The White House, "Executive Order 13563: Improving Regulation and Regulatory Review" http://www.gpo.gov/fdsys/pkg/FR-2011-01-21/pdf/2011-1385.pdf (accessed 04/06/2013)
[194] Ibid.
[195] Ibid.
[196] Jennifer Bayuk et al., *Cyber Security Policy Guidebook* , 237
[197] Ibid.
[198] Fischer, *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options*, 50

oversight. To illustrate this point, criminal organization are increasingly trying to benefit from the growing amount of personal and financial information communicated via cyberspace, and as such require a law enforcement function from the government.[199]

Interestingly, a study conducted by the Enterprise Strategy Group (ESG) of 285 security professionals working in critical infrastructure showed that seventy-one percent of critical infrastructure organizations believe that there needs to be more involvement from the federal government in developing cybersecurity strategies and defenses, and nearly one-third stating that the government should be "significantly more active". Similarly, less than four percent believe the government should be less active in this area.[200] Of note, U.S. organizations that must comply with three or more government or industry regulations, such as the Federal Information Security Management Act (FISMA) or the North American Electric Reliability Commission (NERC), believe the federal government should take the following actions (in order of priority): enact more stringent cybersecurity legislation, create better ways to share security information with the private sector, and enact legislation with high fines for data breaches. Certainly, there seems to be an underlying agreement amongst industry leaders who are subject to some sort of compliance regulation that the federal government has a key role to play in securing cyberspace.

---

[199] Ibid., 51

[200] Oltsik, McKnight and Gahm, *Research Report: Assessing Cyber Supply Chain Security Vulnerabilities within the U.S. Critical Infrastructure*, 45

Examples of Government Regulations

There are several regulatory frameworks where government intervention has been able to address national security and public safety concerns, and keep up with evolving threats. For example, the Air Transport Security regulations, the Foods and Drugs Safety regulations, and the Motor Vehicle Safety regulations are prime examples of such achievements. Moreover, it has been demonstrated that there is a direct correlation between cybersecurity protection and regulatory compliance. Indeed, the ESG survey of security professionals working in critical infrastructure offers the following: "ESG concludes there is a cumulative security effect from multiple regulations that changes an organization's cyber security requirements while simultaneously improving skills and preparation."[201]

Air Transport Security Regulations

The tragic bombing of Air India Flight 182 in 1985 gave rise for the government to strengthen the aviation security framework. However, the attacks on 11 September 2001 became the culminating point in increasing regulation of the air transport security domain. As reported by CATSA, "[w]ith a Canadian-wide strategy in place, CATSA is now able to deploy a national approach to security that ensures consistency in both operations and mandate."[202] To achieve this, several acts and regulations have been developed in partnership with the aviation industry and adopted by the federal government to regulate the industry with a view of protecting Canadian citizens. The

[201] Ibid., 7
[202] "Why we do it - Canadian Air Transport Security Authority" http://www.catsa.gc.ca/Page.aspx?ID=36&pname=WhyWeDoIt_NotreRaisonDEtre&lang=en (accessed 2/10/2013)

creation of CATSA has resulted in positive outcomes for the protection of the Canadian population. Prior to mandating the oversight of aviation security screening, accountability rested with individual airlines for their respective passengers. Today accountability is clearly held by the minister of Transport, Infrastructure and Communities.[203] Similarly, a national system to standardize the use of explosive detection technology was inexistent prior to CATSA's inauguration, while today such equipment has been deployed equally to all designated airport under CATSA's mandate.[204] Thus, a focused regulatory framework and clear accountability positively influence the outcome of protecting a nation and its citizens against a specific threat.

Foods and Drugs Safety Regulations

In order to enhance the health and well-being of Canada's citizens, the environment and the economy, the federal government created the Canadian Food Inspection Agency (CFIA), which draws its authority from 13 federal statutes and 38 sets of regulations such as the Canadian Food Inspection Agency Act and the Food and Drugs Acts.[205] Acting as Canada's largest science-based regulatory agency, the CFIA is responsible for administering, enforcing, and regulating the safety and quality of food sold in Canada, and for ensuring that a sustainable resource base for plants and animals is established.[206] Similar to the role of the federal government in protecting critical infrastructure, the CFIA shares many of its core responsibilities with other federal departments and agencies, with provincial, territorial and municipal authorities, and with

---

[203] Canadian Air Transport Security Authority, *Stepping Forward: Annual Report 2010*, 16
[204] Ibid.
[205] Canadian Food Inspection Agency, "2011-12 Performance Report" http://www.inspection.gc.ca/DAM/DAM-aboutcfia-sujetacia/STAGING/text-texte/acco_reparl_2011-12dpr_pdf_1352435614609_eng.pdf (accessed 04/14/2013), 6
[206] Ibid.

private stakeholders. As a prime example of effective partnership between regulator and industry, the CFIA initiated discussions with the Canadian Fertilizer Products Forum (CFPF), a stakeholder-led initiative, with a goal to review, improve, and implement the regulatory system regarding fertilizers and supplements.[207] To achieve its goal, the CFPF established a series of working groups in order to develop recommendations and provide advice to the CFIA of possible regulatory changes. Interestingly, the CFIA reported that one strategic risk area is that "[the current] legislative, regulatory and program framework may be insufficient to protect Canadian consumers and facilitate trade", which in a sense links a strong regulatory framework with an increased protection of Canadians along with a positive outcome on the economy.[208] Thus, there is a correlation between a strong and tailored regulatory framework with an increase in efficiency.

Motor Vehicle Safety Regulations

Guided by the *Motor Vehicle Safety Act* and the *Motor Vehicle Transport Act*, Transport Canada is responsible for the development and implementation of the Motor Vehicle Safety Program. The aim of the program is to develop legislation, policies, and regulations; and provides oversight of the regulated industry in order to reduce the deaths, injuries and social costs caused by motor vehicle use.[209] As such, the 1993 *Motor Vehicle Safety Act* was enacted to regulate the manufacture and importation of motor vehicles and motor vehicle equipment and reduce the risk of death, injury and damage to property and

---

[207] Ibid., 53
[208] Ibid., 12
[209] Transport Canada, "Report on Plans and Priorities 2013-14" http://www.tc.gc.ca/media/documents/corporate-services/Transport_Canada_RPP_2013-14_English.pdf (accessed 04/14/2013), 42

the environment.[210] As a measure of program effectiveness, the 2011-12 Departmental Performance Report concludes that the number of fatalities and injuries in the 2008-10 period were 22.4 percent and 26.3 percent lower, respectively, than comparable figures from the baseline period of 1996-2001.[211] Furthermore, in light of a recent release of new regulations aimed at improving vehicle safety, David Adams, President of the Association of International Automobile Manufacturers of Canada, eloquently stated that:

> [t]he government is to be commended for its commitment to ensuring that Canada's regulatory framework keeps pace with industry safety practices and technologies for the benefit of Canadians, and for their commitment to aligning Canadian safety regulations with major global standards.[212]

Hence, a well-established regulatory framework led by the government is able to keep pace with technology and global influence.

Regulatory Framework and Partnership

Experts have been trying to identify a model which would provide an adequate approach to develop an efficient cybersecurity framework. In short, two models have been advanced as potential solutions – the Y2K program, as well as environmental and safety regulations.[213] While the Air Transport Security, Foods and Drugs, and Motor Vehicle Standards regulations discussed above have the potential of serving as an initial framework to address the cybersecurity challenge, the Y2K model is not necessarily deemed as strong an option.

---

[210] Transport Canada, "Motor Vehicle Safety Act" http://www.tc.gc.ca/eng/acts-regulations/acts-1993c16.htm (accessed 04/01/2013)
[211] Transport Canada, "Departmental Performance Report 2011-12" http://www.tc.gc.ca/media/documents/corporate-services/2011-12_TC_DPR_-_PDF_(ENGLISH_-_no_signature_for_web).pdf (accessed 04/14/2013), 50
[212] Transport Canada, "Canada Strengthens Vehicle Safety Standards" http://www.tc.gc.ca/eng/mediaroom/releases-2013-h012e-7056.htm (accessed 04/01/2013)
[213] Fischer, *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options*, 51

The key element in the Y2K model was the use of evolving requirements as time progressed towards the 01 January 2000 deadline. In the United States, the Securities and Exchange Commission (SEC) issued rules that required companies to respond to the Y2K problem, which was in turn backed by laws passed by Congress to facilitate information sharing and reduce liability if the companies had complied with the required actions.[214] This approach to the computer problem seems to demonstrate that: the SEC can be effective in promoting changes in cybersecurity posture; Congress can become an enabler by enacting laws to improve information sharing; and an incremental methodology is effective.[215] However, many argue that the model is inappropriate on the grounds that the Y2K problem was not a serious as originally imagined, and therefore is fundamentally much simpler than the current concerns posed by cybersecurity. Moreover, Y2K was merely a one-time issue and therefore not within the scope of the current cyber threat faced by critical infrastructure.[216] While some key lessons can be extracted from the Y2K experience, the safety regulations approach seems to offer a more promising option to address the cybersecurity challenges of critical infrastructure.

As discussed in the three regulatory models above, effective regulatory frameworks are based on a strong partnership between the government and the private sector. However, the complexity of cyberspace is such that a solution will likely resemble of mix a various approaches. Indeed, Kevin Newmeyer explains that "[c]ybersecurity is a daunting policy problem, and a simple solution is not apparent. The choice will be a compromise among various options that must occur within a political environment with a

[214] Ibid., 52
[215] Ibid.
[216] Ibid.

limited attention span and several competing priorities."[217] Additionally, Harknett and Stever stress that "there must be emphasis placed on creating a new regulatory model not based on 19th and 20th century dynamics, but rather one that undergirds the synergy between national security and private sector activity."[218] Regardless, the government must strike a balance and create a framework which avoids two potentially precarious scenarios: an overly regulated industry with unsustainable overhead cost, or a complete inability to implement necessary changes through the lack of adequate regulatory tools (the current situation). Richard Clarke, a former National Coordinator for Security, Infrastructure Protection, and Counterterrorism, argues that overregulation sometimes creates high consumer prices and requirements that do little to fixing the root cause of the problem. Conversely, refusal to regulate often result in situations akin to the 2008 market crash or lead paint in children's toys.[219]

According to the NATO Cybersecurity framework, three issues are central to the national security debate: how a government assures the availability of essential services, protects intellectual property of the nation, and maintains citizen confidence to use the internet to fuel the economy. Certainly, nations are struggling to find the right mix of policy interventions and market incentives to secure the cybersecurity of its critical infrastructure. Of importance is that policy intervention, whether regulatory or incentive-based, must consider the capabilities of the private sector and promote economic growth without impeding productivity. [220] While some sectors are already regulated, such as the electrical sector through the North American Electric Reliability Commission (NERC),

---

[217] Newmeyer, *Who should Lead U.S. Cybersecurity Efforts?*, 124
[218] Harknett and Stever, *The Cybersecurity Triad: Government, Private Sector Partners, and the Engaged Cybersecurity Citizen*, 7
[219] Clarke and Knake, *Cyber War: The Next Threat to National Security and what to do about it* , 134
[220] Klimburg, *National Cyber Security Framework Manual*, 35-36

other sectors are not. Therefore, the government must capitalize on cybersecurity efforts already established in the private sector and avoid creating a new regulatory framework when one already exists. As Christine Adams, Director of the U.S. Chemical Sector Cyber Security Program, explained in her response to the White House 60-Day Cyber Security Review: "[t]he government should leverage security guidance implemented in the Chemical sector rather than creating different requirements and regulations. [221]

Scott Charney proposes that "the government should encourage a balanced approach, one that combines industry self-regulation with government influence (through, for example, procurement regulations) and then includes carefully tailored regulation when necessary."[222] Richard Clarke is equally supportive of what he calls "smart regulation". In short, "smart regulation" is an idea of government regulators that specify goals and objectives rather than micromanaging by specifying the means, allowing the regulated actor sufficient room to figure out how best to achieve the goals established.[223] In a sense, regulations where compliance is not enforced are worthless and are almost as perturbing as regulations requiring a large oversight from federal officials.[224]

As discussed earlier, information sharing between the government and the private sector is crucial to preventing, detecting, and responding to cyber attacks. In order to create an effective partnership between the public and private sectors, an information

---

[221] Christine Adams, "Comments to the 60-Day Cyber Security Review" http://www.whitehouse.gov/files/documents/cyber/Chemical%20Industry%20Responses%20to%20Hathaway%27s%204%20questions%20-%20FINAL.pdf (accessed 03/27/2013), question 4
[222] United States House of Representatives, *Written Testimony of Scott Charney, Corporate Vice President, Microsoft Corporation's Trustworthy Computing*, 9
[223] Clarke and Knake, *Cyber War: The Next Threat to National Security and what to do about it* , 132
[224] Ibid., 134

sharing framework built on trust needs to be established. However, the current situation is far from ideal. Scott Charney elaborates that the current partnership model requires a radical evolution from the current system and replaced with one that is synergistic and efficient.[225] Many suggest that the main restriction on information sharing arise from the government's reluctance to disclose information derived from collection methods and sources which are classified.[226] In certain cases, the existence of a threat is itself classified information since disclosure could adversely affect security.[227] However, Paul Rosenzweig, a former deputy assistant secretary for policy in the Department of Homeland Security, highlights that the current instinct against disclosure is self-imposed and conflicts with a newer post-9/11 standard of enhanced information sharing.[228] In fact, the issue is one of policy rather than law. Indeed, there is no legal barrier preventing the issuance of security clearances to key personnel involved in cybersecurity of critical infrastructure. Rather, the problem is simply a matter of inadequate resources to take on the task.[229] In their 2008 and 2010 reports, the GAO also reported that the lack of security clearances is a major barrier to information sharing.[230] Similarly, there also exists a cultural reluctance by the private sector to share information with the government, mainly derived out of concerns with Access to Information and Privacy (ATIP) legislation.[231] The GAO equally reported that private sector companies were unwilling to share incident

---

[225] United States House of Representatives, *Written Testimony of Scott Charney, Corporate Vice President, Microsoft Corporation's Trustworthy Computing*, 5
[226] Paul Rosenzweig, "Cybersecurity and Public Goods: The Public/Private "Partnership"" http://media.hoover.org/sites/default/files/documents/EmergingThreats_Rosenzweig.pdf (accessed 04/06/2013), 12
[227] Ibid.
[228] Ibid.
[229] Ibid., 13
[230] United States Government Accountability Office, *Cybersecurity: National Strategy, Roles, and Responsibilities Need to be Better Defined and More Effectively Implemented*, 54
[231] Graham, *Canada's Critical Infrastructure: When is Safe enough Safe enough?*, 22

data out of concerns of releasing proprietary data to their competitors.[232] Regardless of the reasons currently hindering information sharing, a balance will be required to ensure the right information is provided to the right industry at the right time to enable the private sector to prepare or defend against an upcoming cyber threat. The key challenge remains knowing how much information sharing is just enough to protect the nation's critical infrastructure.

Nevertheless, the federal government would need to put its house in order before contemplating the development of legislation tailored at improving the cybersecurity of the private sector. As discussed earlier, the lack of accountability, the lack of budget focus and resource allocation, and the difficulty in sharing information within federal departments and outside entities would need to be addressed first and foremost if the government is to gain credibility as a leading institution in this particular area.

Other Options

In addition to the adoption of a regulatory framework, there are several options available at the disposal of the government to strengthen the cybersecurity of the nation's critical infrastructure, each having their own strengths and weaknesses. While a detailed analysis of the effectiveness each option would provide on improving cybersecurity is beyond the scope of this paper, it is worth highlighting alternatives which could be adopted and implemented by the government. For example, the adoption of minimum cybersecurity standards tailored to each critical infrastructure sector would be worth investigating, and would complement the U.S. initiative of involving NIST in developing

[232] United States Government Accountability Office, *Cybersecurity: National Strategy, Roles, and Responsibilities Need to be Better Defined and More Effectively Implemented*, 55

standards and best practices for the critical infrastructure industry. Certainly, standards can add robustness to a network and avoid unnecessary outages. As elaborated by the Canada/U.S. Task Force investigating the 2003 electrical blackout, "[c]lear standards with mandatory compliance, as contemplated under legislation pending in the U.S. Congress, might have averted the start of this blackout."[233]

Other options for the government include the use of certification, conducting audits, establishing benchmarks and checklists, developing metrics, building cybersecurity into enterprise architecture, and improving training and education across the sector networks.[234] Surely, these are valid approaches worth exploring in greater details to address the cybersecurity dilemma, however are out of scope for this paper. Similarly, the United States' Cyber Policy Review proposed possible incentives including adjustments to liability considerations (reduced liability in exchange for improved security or increased liability for the consequences of poor security), indemnification, tax incentives, and new regulatory requirements and compliance mechanisms.[235] Regardless, none of these initiatives would likely be adopted if there were no economic advantages to do so.

As discussed in Chapter 2, the use of the Common Criteria Scheme and contracting clauses for the procurement of IT equipment applies only to the federal government. Potentially, more stringent cybersecurity regulations could promote the use of these standards and guidelines for critical infrastructure sectors. Ideally, a set of

---

[233] U.S.-Canada Power System Outage Task Force, *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, 17
[234] Fischer, *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options*, 26
[235] Executive Office of the President of the United States, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, 28

mandatory minimum standards for critical infrastructure sectors, such as limiting the acquisition to the mandatory certification of IT equipment under the CCS, could reduce the risk of introducing questionable IT equipment in the critical infrastructure networks. Christine Adams equally supports the concept of establishing minimum cybersecurity standards for technology providers when delivering solutions to critical infrastructure companies.[236] She also proposes that the federal government use its procurement power to enhance the security of IT equipment and services by mandating higher requirements, and sharing the technology and services with the critical infrastructure industry.[237] Similarly, the Intelligence and National Security Alliance also recognizes the crucial role of the government in developing and sharing defensive practices and procurement guidance to address advanced cyber threats.[238]

Summary

In summary, it has been demonstrated that the status quo is no longer supportable, and that the current partnership model is being reinforced by cybersecurity legislations, primarily led by the United States. As such, the Canadian government must ensure it keeps pace with the initiatives of its southern neighbor given the high degree of interconnectivity found in the critical infrastructure. Also, history has proven that government intervention has often resulted from dire situations, akin to the cyber threat facing the nation's critical infrastructure today. As a result, legislative and regulatory frameworks have emerged to address critical issues related to public safety and national

---

[236] Adams, *Comments to the 60-Day Cyber Security Review*, question 3
[237] Ibid., question 4
[238] Intelligence and National Security Alliance, "Critical Issues for Cyber Assurance Policy Reform: An Industry Assessment" http://www.whitehouse.gov/files/documents/cyber/INSA%20-%20Critial%20Issues%20for%20Cyber%20Assurance%20Policy%20Reform%20-%2026Mar2009.pdf (accessed 04/06/2013), 5

security. While the concept of regulations might look appealing to address immediate concerns, other options are available at the discretion of the government to tackle the cybersecurity issue. However, adequate monetary and personnel resources would need to be provided, along with clear accountability, to effectively enhance the cybersecurity resiliency of the nation's critical infrastructure.

CHAPTER 6 – CONCLUSION

This paper has discussed the cyber threats facing the nation's critical infrastructure, and highlighted the roles and responsibilities of key cyber actors involved in the cybersecurity of the nation's critical assets. It also provided an overview of existing policies, strategies and legislative frameworks guiding the activities necessary to counter the cyber threat. Finally, the dissertation discussed possible options to address the cybersecurity threats to the nation's critical infrastructure.

The evolution of the internet has certainly revolutionized the world. More importantly, the speed and complexity of the evolution of cyberspace has caught today's society by surprise. Indeed, governments, private industries and citizens of nations around the globe are now desperately trying to address the intricate security concerns that emerged from the growth of cyberspace. Moreover, the emergence of globalization has broadened the issue on a global scale. Given this complex scenario, solutions to address cybersecurity deficiencies are not trivial, and demand a combined effort to overcome.

The increased reliance on cyberspace to deliver private and government services essential to the health, safety, security and economic well-being of Canadians has created a security gap that must be addressed. Certainly, damage to critical infrastructure via cyber attacks has the potential to substantially degrade a nation's economic competitiveness, reduce privacy protection, shake public confidence, result in significant economic losses, and undermine sovereignty. Given that the vast majority of the critical assets are owned and operated by agencies outside the federal government, clear roles and responsibilities of key cyber actors is essential to maximize the effectiveness of a

nation's cybersecurity strategy. In reality, those responsibilities are murky at best, and the current strategy is hampered by stakeholders' diverging interests.

This paper has demonstrated that threats to critical infrastructure from cyber vectors pose clear dangers to national security. It highlighted the complexity and ever-growing cyber threats to the nation's critical assets, and discussed the implications of disruption to the Canadian economy and to the health, safety, and security of Canadian citizens. Moreover, the study highlighted the roles and responsibilities of key cyber actors in protecting critical infrastructure, and concluded that the imperative of the federal government to address national security concerns is real.

An overview of current strategies, policies, and legislative frameworks in place to address the cybersecurity threats to critical infrastructure proved that the current framework is wholly inadequate for the federal government to meet its mandate. Moreover, the paper argued that the Canadian government must strengthen the cyber resiliency of critical infrastructure by adopting a targeted cybersecurity legislative framework. In other words, simply maintaining a coordinating role at the national level is insufficient, and the magnitude of the problem demands a framework that allows the government to shape and influence the cybersecurity of critical infrastructure. As such, the study highlighted that the United States have led the way in strengthening the cybersecurity posture of its critical infrastructure by advancing cybersecurity Acts and an Executive Order to address the seriousness of the problem. Given the interconnectedness of critical infrastructure across the Canadian-American border, the initiatives south of the border are of significance to Canada and cannot simply be overlooked by the Canadian government.

This paper suggested that the complexity of cyberspace combined with the interests of public and private actors demand a strong partnership between government and the private sector. However, the paper argued that the federal government cannot completely delegate its role in protecting the nation's critical infrastructure from cyber threats. It equally demonstrated that the status quo is no longer supportable, and a new approach is warranted. Therefore, bolstering the public-private partnership is crucial, and overcoming the hurdles of information sharing between government and private institutions is essential to build an effective cybersecurity strategy.

The paper hinted that historical events tend to support the notion of increased government oversight following significant events tied to national security. It also discussed current government legislative frameworks in place to address concerns in the realm of air transport security, foods and drugs safety, and motor vehicle standards commensurate of public safety requirements. Similarly, these frameworks have been proposed as potential models for the government to address current and future cybersecurity concerns related to critical infrastructure. However, it is recognized that a solution to the cybersecurity problem is not simple, and requires a balanced approach. As such, the government must capitalize on the progress made to date by the private industry to secure cyberspace.

Further research on the strengths and weaknesses of other options presented, such as the use of certification, conducting audits, tax incentives, reduced liability, indemnification, establishing benchmarks and checklists, developing metrics, and improving training and education across the sector networks, would provide additional value to develop a robust cybersecurity strategy for critical infrastructure.

Critical infrastructure is vital to the economy and the well-being of the nation, and affects the daily lives of every Canadian citizen. Consequently, it demands a high-degree of resources allocated to secure it from cyber threats. While partnership is critical to bolstering cybersecurity, involvement from the federal government is necessary to protect its critical assets. After all, it is the responsibility of the government, and a matter of national security.

BIBLIOGRAPHY

"Aurora Vulnerability White Paper | Power Grid Security Vulnerable to Cyber Attack", accessed 3/5/2013, http://unix.nocdesigns.com/aurora_white_paper.htm.

"Brief History of the Internet" accessed 2/11/2013, http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet.

"CCS Overview", accessed 3/8/2013, http://www.cse-cst.gc.ca/its-sti/services/cc/ccso-vesccc-eng.html.

"Emergency Management Act", accessed 04/06/2013, http://laws-lois.justice.gc.ca/PDF/E-4.56.pdf.

"What is SCADA?", accessed 3/6/2013, http://www.webopedia.com/TERM/S/SCADA.html.

"Why we do it - Canadian Air Transport Security Authority", accessed 2/10/2013, http://www.catsa.gc.ca/Page.aspx?ID=36&pname=WhyWeDoIt_NotreRaisonDEtre&lang=en.

Adams, Christine. "Comments to the 60-Day Cyber Security Review", accessed 03/27/2013, http://www.whitehouse.gov/files/documents/cyber/Chemical%20Industry%20Responses%20to%20Hathaway%27s%204%20questions%20-%20FINAL.pdf.

American College of Cardiology's CardioSource. "Homeland Security Warns of Medical Device Hacking", accessed 2/10/2013, http://www.cardiosource.org/News-Media/Publications/CardioSource-World-News/Homeland-Security.aspx.

Amoroso, Edward G. *Cyber Attacks: Protecting National Infrastructure* Butterworth-Heinemann.

Canadian Air Transport Security Authority. "Stepping Forward: Annual Report 2010", accessed 02/10/2013, http://www.catsa-acsta.gc.ca/file/library/87/english/AnnualReport2010.pdf.

Canadian Food Inspection Agency. "2011-12 Performance Report", accessed 04/14/2013, http://www.inspection.gc.ca/DAM/DAM-aboutcfia-sujetacia/STAGING/text-texte/acco_reparl_2011-12dpr_pdf_1352435614609_eng.pdf.

Cate, Fred H. "Comments to the White House 60-Day cybersecurity review", accessed 01/31/2013,

http://www.whitehouse.gov/files/documents/cyber/Center%20for%20Applied%20Cybersecurity%20Research%20-%20Cybersecurity%20Comments.Cate.pdf.

Center for Strategic and International Studies. "Cybersecurity Two Years Later", accessed 04/06/2013, http://csis.org/files/publication/110128_Lewis_CybersecurityTwoYearsLater_Web.pdf.

———. "Significant Cyber Incidents since 2006", accessed 04/15/2013, http://csis.org/files/publication/130206_Significant_Cyber_Incidents_Since_2006.pdf.

Chairman of the Joint Chiefs of Staff. "Letter of Support to the Chairman of the Committee on Commerce, Science, and Transportation", accessed 2/10/2013, http://www.hsgac.senate.gov/download/cybersecurity-support-letter-joint-cheifs-of-staff-chairman.

Cheadle, Bruce. "Bill C-30, Tory Internet Surveillance Legislation, is Officially Dead - the Huffington Post", accessed 04/11/2013, http://www.huffingtonpost.ca/2013/02/11/bill-c-30-dead-internet-canada_n_2664458.html.

Clarke, Richard A. and Robert K. Knake. *Cyber War: The Next Threat to National Security and what to do about it*. United States of America: HarperCollins, 2010.

Communications Security Establishment Canada. "Technology Supply Chain Guidelines: Contracting Clauses for Telecommunications Equipment and Services", accessed 03/08/2013, http://www.cse-cst.gc.ca/documents/services/tscg-ccat/tscg-ccat01g-eng.pdf.

Congressional Research Service. "The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress", accessed 04/08/2013, http://www.fas.org/sgp/crs/misc/R42984.pdf.

Diebert, Ron. "Cyber Security: Canada is Failing the World ", accessed 2/23/2013, http://www.huffingtonpost.ca/2011/05/26/cyber-security-canada-stephen-harper-g8_n_867136.html.

Director of the National Security Agency. "Letter to the Honorable Harry Reid", accessed 04/06/2013, http://www.hsgac.senate.gov/download/cybersecurity-support-letter-general-keith-alexander.

Emergency Management Policy Directorate. "An Emergency Management Framework for Canada", Public Safety Canada, accessed 03/09/2013, http://www.publicsafety.gc.ca/prg/em/_fl/emfrmwrk-2011-eng.pdf.

Executive Office of the President of the United States. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, 2009, accessed 04/18/2013, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

Falliere, Nicolas, Liam O Murchu and Eric Chien. "W32.Stuxnet Dossier." Symantec Corporation, accessed 03/04/2013, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

Fischer, Eric A. "Creating a National Framework for Cybersecurity: An Analysis of Issues and Options." In *Cybersecurity and Homeland Security*", edited by Choi, Lin V. New York: Nova Science Publishers, Inc., 2005.

Goldsmith, Jack. "Conservative Legal Scholar Backs Security Standards for Critical Infrastructure", accessed 4/6/2013, http://www.hsgac.senate.gov/media/majority-media/conservative-legal-scholar-backs-security-standards-for-critical-infrastructure.

Government of Canada. "Action Plan for Critical Infrastructure", accessed 04/18/2013, http://www.publicsafety.gc.ca/prg/ns/ci/_fl/ct-pln-eng.pdf.

———. "Canada's Cyber Security Strategy", accessed 04/11/2013, http://www.publicsafety.gc.ca/prg/ns/cybr-scrty/_fl/ccss-scc-eng.pdf.

———. "National Strategy for Critical Infrastructure", accessed 04/18/2013, http://www.publicsafety.gc.ca/prg/ns/ci/_fl/ntnl-eng.pdf.

Graham, Andrew. *Canada's Critical Infrastructure: When is Safe enough Safe enough?*: MacDonald-Laurier Institute, 2011, accessed on 04/18/2013, http://www.macdonaldlaurier.ca/files/pdf/Canadas-Critical-Infrastructure-When-is-safe-enough-safe-enough-December-2011.pdf

Harknett, Richard J. and James A. Stever. "The Cybersecurity Triad: Government, Private Sector Partners, and the Engaged Cybersecurity Citizen." *Journal of Homeland Security and Emergency Management*, 6, no. 1 (2009).

Hsu, Christine. "Many Popular Medical Devices may be Vulnerable to Cyber Attacks : Consumer News : Medical Daily", accessed 2/10/2013, http://www.medicaldaily.com/articles/9486/20120410/medical-implants-pacemaker-hackers-cyber-attack-fda.htm#md5KuC237zm6BE5m.99.

Intelligence and National Security Alliance. "Critical Issues for Cyber Assurance Policy Reform: An Industry Assessment", accessed 04/06/2013, http://www.whitehouse.gov/files/documents/cyber/INSA%20-%20Critial%20Issues%20for%20Cyber%20Assurance%20Policy%20Reform%20-%2026Mar2009.pdf.

Internet Security Alliance. *The Cyber Security Social Contract Policy Recommendations for the Obama Administration and 111th Congress*. USA: ISAlliance, 2008, accessed 04/18/2013, http://www.whitehouse.gov/files/documents/cyber/ISA%20-%20The%20Cyber%20Security%20Social%20Contract.pdf.

Jennifer Bayuk, Jason Healey, Paul Rohmeyer, Marcus Sachs, Jeffrey Schmidt, and Joseph W. Weiss. *Cyber Security Policy Guidebook.* Wiley, 2012.

Kelly-Detwiler, Peter. "Protecting the Electric Grid from Terrorism -- Nobody is in Charge" Forbes, accessed 3/8/2013, http://www.forbes.com/sites/peterdetwiler/2012/11/16/protecting-the-electric-grid-from-terrorism-nobody-is-in-charge/.

Klimburg, Alexander, ed. *National Cyber Security Framework Manual*. NATO Cooperative Cyber Defence Centre of Excellence, 2012, accessed 04/18/2013, http://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf.

Lord, Kristin M. and Travis Sharp. *America's Cyber Future: Security and Prosperity in the Information Age (Volume 1).* Washington: Center for a New American Security, June 2011, accessed 04/18/2013, http://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume%20I_0.pdf.

Luiijf, H., K. Besseling, M. Spoelstra, and P. de Graaf. "Ten National Cyber Security Strategies: A Comparison" CRITIS 2011 – 6th International Conference on Critical information infrastructures Security, September 2011.

McDonald, Geoff, Liam O Murchu, Steven Doherty and Eric Chien. "Stuxnet 0.5: The Missing Link" Symantec Corporation, accessed 03/05/2013, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/stuxnet_0_5_the_missing_link.pdf.

National Council of ISAC. "Information Sharing and Analysis Centers", accessed 04/06/2013, http://www.isaccouncil.org/aboutus.html.

National Cyber Security Summit Task Force. "Information Security Governance: A Call to Action", accessed 04/05/2013, http://www.cyber.st.dhs.gov/docs/Information%20Security%20Governance-%20A%20Call%20to%20Action%20(2004).pdf.

Newmeyer, Kevin P. "Who should Lead U.S. Cybersecurity Efforts?" *PRISM* 3, no. 2, accessed 04/18/2013, http://ndupress.ndu.edu/lib/pdf/prism3-2/prism115-126_newmeyer.pdf

Obama, Barack. "Taking the Cyberattack Threat Seriously - Wall Street Journal" accessed 2/10/2013, http://online.wsj.com/article/SB10000872396390444330904577535492693044650.html?KEYWORDS=Obama+cybersecurity.

Office of the Auditor General of Canada. "Report of the Auditor General of Canada to the House of Commons: Protecting Canadian Critical Infrastructure Against Cyber Threats", accessed 02/25/2013, http://www.oag-bvg.gc.ca/internet/docs/parl_oag_201210_03_e.pdf.

Office of the Press Secretary to The White House. "Executive Order on Improving Critical Infrastructure Cybersecurity", accessed 04/12/2013, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0.

O'Keefe, Ed and Ellen Nakashima. "Cybersecurity Bill Fails in Senate - the Washington Post", accessed 4/6/2013, http://www.washingtonpost.com/world/national-security/cybersecurity-bill-fails-in-senate/2012/08/02/gJQADNOOSX_story.html.

Oltsik, Jon, John McKnight and Jennifer Gahm. "Research Report: Assessing Cyber Supply Chain Security Vulnerabilities within the U.S. Critical Infrastructure" Enterprise Strategy Group, http://www.nsci-va.org/CyberReferenceLib/2010-11-ESG%20Research%20Report%20Cyber%20Supply%20Chain%20Security.pdf.

Parry, Tom. "Critical Cybersecurity Gaps Remain, Auditor General Says", accessed 04/08/2013, http://www.cbc.ca/news/politics/story/2012/10/23/pol-auditor-generals-report-cybersecurity-veterans-fiscal.html.

Platt, Victor. "Still the Fire-Proof House? an Analysis of Canada's Cyber Security Strategy" accessed 04/11/2013, http://www.academia.edu/1534361/Still_the_fire_proof_house_An_analysis_of_Canadas_Cyber_Security_Strategy.

Porteous, Holly. "Cybersecurity and Intelligence: The U.S. Approach" Library of Parliament, accessed 02/10/2013, http://www.parl.gc.ca/Content/LOP/ResearchPublications/2010-02-e.pdf.

Press, Jordan. "Current Laws Not Focused enough to Combat Child Porn Online: RCMP - the National Post" accessed 04/11/2013, http://news.nationalpost.com/2012/02/21/current-laws-not-focused-enough-to-combat-child-porn-online-rcmp/.

———. "Tories Face International Pressure to Pass Cybercrime Provisions, Documents show - Canada.Com", accessed 04/09/2013, http://o.canada.com/2012/11/27/tories-face-international-pressure-to-pass-cybercrime-provisions-documents-show/.

Privy Council Office. "Securing an Open Society: Canada's National Security Policy", accessed 03/27/2013, http://publications.gc.ca/collections/Collection/CP22-77-2004E.pdf.

Public Safety Canada. "Canadian Cyber Incident Response Centre", accessed 04/05/2013, http://www.publicsafety.gc.ca/prg/ns/cybr-scrty/ccirc-eng.aspx.

———. "Cyber Security in the Canadian Federal Government", accessed 03/27/2013, http://www.publicsafety.gc.ca/prg/ns/cybr-scrty/fdrl-gvt-eng.aspx.

———. "Forward Regulatory Plan: 2012-2014", accessed 04/06/2013, http://www.publicsafety.gc.ca/abt/ctsnrg/frwrdrg-12-14-eng.aspx.

———. "List of Acts and Regulations", accessed 04/06/2013, http://www.publicsafety.gc.ca/abt/ctsnrg/lstcts-eng.aspx.

———. "Minister Day Announces the New Emergency Management Act", accessed 04/06/2013, http://www.publicsafety.gc.ca/media/nr/2007/nr20070807-1-eng.aspx.

Rosenzweig, Paul. "Cybersecurity and Public Goods: The Public/Private "Partnership"", accessed 04/06/2013, http://media.hoover.org/sites/default/files/documents/EmergingThreats_Rosenzweig.pdf.

Schneier, Bruce. *On Security*. Indianapolis: Wiley Publishing Inc., 2008.

Shared Services Canada. "2013-14 Report on Plans and Priorities", accessed 04/05/2013, http://www.ssc-spc.gc.ca/media/documents/SSC_RPP_2013-14EN%20(NO%20SIGN).pdf.

Silicon Valley Leadership Group. "Letter of Support to S.3414 the Cybersecurity Act of 2012", accessed 04/06/2013, http://www.hsgac.senate.gov/download/cybersecurity-support-letter-silicon-valley-leadership-group.

Standing Senate Committee on National Security and Defence. *Emergency Preparedness in Canada (Volume 1)*, 2008, accessed 04/18/2013, http://www.parl.gc.ca/Content/SEN/Committee/392/defe/rep/rep13aug08vol1-e.pdf

———. "Proceedings of the Standing Senate Committee on National Security and Defence, Issue 6, Evidence - Meeting of may 7, 2012", accessed 3/8/2013, http://www.parl.gc.ca/content/sen/committee/411/SECD/06EVB-49519-E.HTM.

The National Association of Regulatory Utility Commissioners. *Information Sharing Practices in Regulated Critical Infrastructure States: Analysis and Recommendations*, 2007, accessed 04/18/2013, http://www.naruc.org/Publications/NARUC%20CIP%20Information%20FIN.pdf

The White House. "Executive Order 13010: Critical Infrastructure Protection", accessed 04/19/2013, http://www.gpo.gov/fdsys/pkg/FR-1996-07-17/pdf/96-18351.pdf.

———. "Executive Order 13563: Improving Regulation and Regulatory Review", accessed 04/06/2013, http://www.gpo.gov/fdsys/pkg/FR-2011-01-21/pdf/2011-1385.pdf.

Transport Canada. "Canada Strengthens Vehicle Safety Standards", accessed 04/01/2013, http://www.tc.gc.ca/eng/mediaroom/releases-2013-h012e-7056.htm.

———. "Departmental Performance Report 2011-12", accessed 04/14/2013, http://www.tc.gc.ca/media/documents/corporate-services/2011-12_TC_DPR_-_PDF_(ENGLISH_-_no_signature_for_web).pdf.

———. "List of Regulations", accessed 04/06/2013, http://www.tc.gc.ca/eng/acts-regulations/regulations.htm.

———. "Motor Vehicle Safety Act", accessed 04/01/2013, http://www.tc.gc.ca/eng/acts-regulations/acts-1993c16.htm.

———. "Report on Plans and Priorities 2013-14", accessed 04/14/2013, http://www.tc.gc.ca/media/documents/corporate-services/Transport_Canada_RPP_2013-14_English.pdf.

Treasury Board of Canada Secretariat. "Government of Canada Information Technology Incident Management Plan", accessed 04/07/2013, http://www.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimti01-eng.asp.

U.S. House of Representatives Select Committee on Homeland Security. "Cybersecurity for the Homeland." In *Cybersecurity and Homeland Security*, edited by Choi, Lin V. New York: Nova Science Publishers, Inc., 2005.

U.S.-Canada Power System Outage Task Force. "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations", accessed 02/26/2013, https://reports.energy.gov/BlackoutFinal-Web.pdf.

United States Government Accountability Office. "Cybersecurity: National Strategy, Roles, and Responsibilities Need to be Better Defined and More Effectively Implemented", accessed 04/19/2013, http://www.gao.gov/assets/660/652170.pdf.

United States House of Representatives. "Written Testimony of Scott Charney, Corporate Vice President, Microsoft Corporation's Trustworthy Computing", accessed 06/02/2013, http://www.whitehouse.gov/files/documents/cyber/Congress%20-%20Charney-microsoft-SFR_10Mar09.pdf.

United States Senate. "Letter to Colleagues: Cybersecurity Act of 2012 (S.3414)", accessed 2/10/2013, http://www.hsgac.senate.gov/download/cybersecurity-dear-colleague.

United States Senate Committee on Homeland Security and Government Affairs. "Statement for the Record by the Honorable Michael Chertoff - February 16, 2012", accessed 04/06/2013, http://www.hsgac.senate.gov/download/cybersecurity-support-statement-former-dhs-secretary-michael-chertoff.

United States Senate Committee on Homeland Security and Governmental Affairs. "The Revised Cybersecurity Act of 2012 S.3414 (Introduced July 19, 2012)", accessed 04/08/2013, http://www.hsgac.senate.gov/download/cybersecurity-act-of-2012_-revision-two-page-summary

Zetter, Kim. "Stuxnet Missing Link found, Resolves some Mysteries Around the Cyberweapon." Wired.com, accessed 3/5/2013, http://www.wired.com/threatlevel/2013/02/new-stuxnet-variant-found/all/.

Zimmet, Brian and Jason Wool. "Cybersecurity Regulation: 5 Issues for Companies - MarketWatch", accessed 4/8/2013, http://articles.marketwatch.com/2013-01-11/commentary/36270525_1_cybersecurity-operators-regulation.