National Defence | Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

PROTECTING CANADA'S CRITICAL INFRASTRUCTURE ONE BYTE AT A TIME

Major J.A. Roper

JCSP 40

Exercise *Solo Flight*

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 40

Exercice *Solo Flight*

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 40 – PCEMI 40
2013 – 2014

DS/CF 568 DSS

PROTECTING CANADA'S CRITICAL INFRASTRUCTURE ONE BYTE AT A TIME

By Major J.A. Roper

Word Count: 4962

Compte de mots : 4962

Today, the cyber economy is the economy. Corrupt those networks and you disrupt this nation.

- Condoleezza Rice, March 22, 2001

Since the inception of the first computer, technology has developed to the point, whereby it plays a central role in our lives. From alarm clocks to microwave ovens, our society in general is completely reliant on computers. Even modern automobiles are controlled by hundreds of computers.[1] From its humble beginnings in the 1950s, where the Advanced Research Projects Agency (ARPA) was created to help develop information technologies to withstand a nuclear attack to the broadband 30 trillion webpages on the Internet we have today technology has changed the way the world operates. The rapid advancement enabled the expansion of the World Wide Web and allowed for more complex pages and applications. With much more functionality, it did not take long for financial transactions to take place online as demonstrated in 1994 when the first online shopping mall arrived. As with all technologies, there are inherent risks associated with them and it did not take long for the first cyber attack to take place.[2] In fact, in 1988, one of the first recognized "worms" used was to attack the telecommunications infrastructure, which quickly spread across the United States.

---

[1] P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What everyone Needs to Know* (Oxford: Oxford University Press, 2014), 1.

[2] University of Illinois, History of the Internet, accessed 11 May 2014, http://education.illinois.edu/wp/commercialism/history-of-the-internet.htm.

However, password vulnerabilities were found as early as 1965,[3] which leads to the topic of this essay, critical infrastructure and cyber security.

As identified by Canada's National Security Policy, cyber attacks pose an actual threat to critical infrastructure with potentially severe consequences of those attacks.[4] So much so, sophisticated attacks can disrupt power grids, water treatment facilities, and telecommunication networks, which can dramatically affect an area or a population.

The realities are there, our society today is based on information and communications technology which intertwine all aspects of our lives. As outlined in this essay, critical infrastructure, which includes the energy sector, is largely linked to that of the other sectors via telecommunication networks and infrastructure. Additionally, new technologies with imbedded control systems and the expansive interconnectedness of information and communications technologies contribute to the insecurity of the backbone of our nation's critical infrastructure for cyber attacks.[5]

The dependency of modern society on computers demands that government policy regarding the cyber world and critical infrastructure requires protection. The government needs to approach the issue of cyber security with an interdepartmental methodology because, frankly, it is a problem that is larger than any one department.

This paper proves that national critical infrastructure needs to be protected from cyber threats. It focuses on three main areas, defining critical infrastructure, cyber security and threats within that environment. The partnership of these key players

---

[3] NATO. The History of Cyber Attacks – a timeline, http://www nato.int/docu/review/2013/Cyber/timeline/EN/index.htm

[4] Privy Council Office, *Securing an Open Society: Canada's National Security Policy* (Ottawa: Canada Communication Group, 2004), 26, http://publications.gc.ca/collections/Collection/CP22-77-2004E.pdf.

[5] Canadian Security Intelligence Service, "Assessing Cyber Threats To Canadian Infrastructure" (Ottawa: Canada Communication Group, 2012), accessed 6 May 2012, https://www.csis-scrs.gc.ca/pblctns/ccsnlpprs/20121001_ccsnlpprs-en.php.

regarding national critical infrastructure (Government of Canada, private sector, Canadian citizens, and the United States) is essential to adequately protect Canada.

CRITICAL INFRASTRUCTURE

What is National Critical Infrastructure?

To fully understand the relationship between cybersecurity and national critical infrastructure the reader must first know what critical infrastructure entails. As technology and society evolve, the definition of what exactly constitutes critical infrastructure is changing, and this will have implications for any government cyber policy.

In general, national critical infrastructure refers to the complex support system designed to deliver nationwide services, which are essential in the effective operations of a nation.[6] Specifically, it refers to "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." [7] In an Auditor General Report regarding the protection of Canadian critical infrastructure against cyber attacks, critical infrastructure is defined as having two parts, physical and information technology assets. These assets are composed of telecommunications networks, electricity distribution networks, banking systems, manufacturing and transportation systems as well as key information systems for the government enabling key services to the public and effective

[6] Edward G. Amoroso, *Cyber Attacks: Protecting National Infrastructure* (Burlington: Butterworth-Heinemann, 2011), 1.

[7] Public Safety Canada, "National Strategy for Critical Infrastructure" http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-eng.aspx, 2.

running of the government.[8] An aspect that adds complexity to the issue of critical infrastructure within Canada is that it is not centrally controlled and a large portion is provided and owned by the private sector.[9] In fact, approximately eighty-five percent of the national critical infrastructure is not owned by the Government of Canada and is the responsibilities of the private sector (Industry), Provinces and Non-governmental Agencies.[10] "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."[11]

Within Canada, the National Strategy for Critical Infrastructure recognizes the uniqueness of how provinces and territories structure their critical infrastructure programs and has broken down critical infrastructure into ten sectors with respect to their essential capabilities. These are energy and utilities, information and communication technology (ICT), finance, health, food, water, transportation, safety, government, and manufacturing.[12]

These ten classifications indicate that critical infrastructure can be described as having three general characteristics. Firstly, it is completely apparent that critical infrastructure involves most aspects of everything that Canadians experience in the conduct of their lives. Secondly, critical infrastructure spans the spectrum between public and private life, all levels of government, corporate and individuals, and back again.

---

[8] 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* (Ottawa: Canada Communication Group, Fall 2012), http://www.oag-bvg.gc.ca/internet/docs/parl_oag_201210_03_e.pdf, 3.

[9] Ibid.

[10] Andrew Graham, *Canada's Critical Infrastructure: When is Safe enough Safe enough?*, MacDonald-Laurier Institute, 2011, http://www.macdonaldlaurier.ca/files/pdf/Canadas-Critical-Infrastructure-When-is-safe-enough-safe-enough-December-2011.pdf, 8.

[11] Public Safety and Emergency Preparedness Canada, *Position Paper on a National Strategy for Critical Infrastructure Protection* (Ottawa: Canada Communication Group, November 2004), 98.

[12] Public Safety Canada, "National…, 5.

Moreover, within this spectrum of interconnectedness there are interfaces between the sectors which in many cases create mutual dependencies.[13] This mutual dependency exacerbates the impact of disruptions of critical infrastructure which in turn could lead to extensive losses economically, situations causing death, and a loss of confidence in the system on behalf of the public.[14] Finally, Canadian critical infrastructure is not uniquely a domestic issue, particularly since the economies of the United States and Canada have become increasingly intertwined over recent decades. In 2003 this was evidenced during a major power outage that started in the United States and spread through Ontario.[15] These results highlighted the shared vulnerabilities and shared responsibilities as opposed to only considering Canadians when developing strategies regarding critical infrastructure.

Threats to critical infrastructure

There are a variety of different categories for critical infrastructure threats. As seen in a White House Executive Order, the threats were broken down into physical and electronic. Physical threats are generally considered to threaten the actual physical or tangible nature of the property.[16] Physical threats can range from terrorist attacks such as the gas pipeline attacks in British Columbia where the Royal Canadian Mounted Police (RCMP) identified them as "domestic terrorism,"[17] to a natural disaster which takes down the power grid as seen during the winter of 2013-14 in Toronto, Ontario during the

[13] Graham, *When is Safe*…, 8.
[14] Public Safety Canada, "National…, 2.
[15] Graham, *When is Safe*…, 8.
[16] The White House, "Executive Order 13010: Critical Infrastructure Protection," accessed 2 May 2014. http://www fas.org/irp/offdocs/eo13010.htm.
[17] Graham, *When is Safe*…, 13.

ice storm. Electronic threats can be electromagnetic or computer based in nature and may be exploited through vulnerabilities within the information technology systems used to control the critical infrastructure. [18]

Specifically within Canada, this refers to an attack via the internet for the purposes of unauthorized use, disruption, or destruction of data used to process, communicate, or store information.[19] Increased levels of connectivity also increase the number of vulnerabilities associated with the critical cyber infrastructure. Of note, information technology security companies say that over sixty percent of all malicious code detected up to now was released in 2008 and that the occurrence and damages which are caused by these cyber attacks is increasing exponentially,[20] thus highlighting the requirements for cyber security.

CYBER

What is cyber security

Compromises caused by hacker, viruses, or malware to the critical infrastructure networks can cause a varying range of issues from life threatening to annoyances. As the proliferation of computerized devices continues to increase (mobile phones, wireless networks, tablets) so does the opportunity for exploitation.[21] Further, in March of 2013 a top intelligence official advised that cyber attacks and cyber espionage were the highest threats to national security.[22]

---

[18] The White House, "Executive Order 13010..., accessed 2 May 2014.
[19] Auditor, *Report of the Auditor*..., 1.
[20] Public Safety Canada, *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada* (Ottawa: Canada Communication Group, 2010), 6.
[21] University of Maryland, "Cyber Security," accessed 6 May 2014, http://www.umuc.edu/cybersecurity/about/cybersecurity-basics.cfm.
[22] Ibid.

As mentioned, cyber attacks are becoming a real threat and they are highlighting the importance of cyber security. National critical infrastructure is not immune and thus requires a robust system in place to ensure its protection and resiliency to attacks. That said defining cyber threats play a major role in proving why it is so important to have expertise in cyber security and cyberspace.

Cyber security comprises many components and is more than simply defending information technology based equipment against attacks from viruses or malware. The United States Congress defines cyber security as:

> the vulnerability of any computing system, software program, or critical infrastructure, or their ability to resist, intentional interference, compromise, or incapacitation through the misuse, or by unauthorized means of, the Internet, public or private telecommunications systems or other similar conduct that violates… laws… that harms interstate commerce of the United States, or that threatens public health or safety.[23]

Further, cyber security refers to the protection of information technology infrastructure from unauthorized change or destruction of data, unintended access to programs or data, and the prevention of destruction or changing of data on computers and networks. [24]

Cyber Threats to Canadian Critical Infrastructure

Properly defining cyber attacks is critical to the importance of any Canadian policy designed to protect against them. Over the years cyber attacks have increased while the taxonomy of these attacks has evolved to a point whereby they are classified by

[23] T.G. Lewis, *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*, (New Jersey: John Wiley and Sons Inc, 2006), 429.

[24] University of Maryland, "Cyber Security…,

the vulnerabilities to be exploited, the impact of the attack, or the target itself.[25] With the development of new technologies, cyber attacks can be conducted rather easily using viruses, malware, and denial of service (DOS) attacks, espionage and sabotage.[26] Further, a National Research Council put together by the United States government defined a cyber attack as "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks."[27] An example of this occurred in Australia when a former employee hacked into the water treatment plant. Using a known vulnerability on the network they released 264,000 gallons of raw sewage into rivers and parks causing major damage to physical property as well as killing wildlife.[28]

Given the nature of the cyber domain, exploitation has been targeted at key infrastructures, key economic and national assets as they are deemed attractive as low risk, high reward targets. Further, cyberspace provides the perfect low risk, high reward environment for nefarious actions as well as information gathering and theft purposes (cyber espionage, cyber crime). Currently, terrorism both domestic and international, sponsored espionage and sabotage (state and non-state), and malevolent hacktivist are the most prominent threats to Canadian critical infrastructure.[29]

According to Amoroso, there are five reasons why these players mentioned above would carry out cyber attacks on critical national infrastructure. Potentially the most

---

[25] S. Saad, Bazan, S., and Varin, C. "Asymmetric Cyber-warfare between Israel and Hezbollah: The Web as a new strategic battlefield." *Journal of Webscience* (2011), accessed 3 March 2014, http://journal.webscience.org/526/1/96_paper.pdf, 16.

[26] Thomas, Rid, *Cyberwar Will Not Take Place* (Oxford: Oxford University Press, 2013), 36, 39-40, 55, 81.

[27] Singer, *Cybersecurity…*, 68.

[28] Don, Dickinson, *Protecting Water Industry Control and SCADA Systems from Cyber Attacks* (Harrisburg: Phoenix Contact), 1.

[29] Canadian Security Intelligence Service, "Assessing…,

important of the five is country-sponsored attacks. The degree to which the attack can be carried out and the capabilities and resources of an adversary can potentially be unlimited through state funding. Secondly terrorist groups, regardless of the underlying motive, can have the means and capabilities to fund a major attack on critical infrastructure. Commercially motivated attacks, such as espionage or sabotage are used to gain an advantage over the competition when the targeted incident is directed at an owner of a critical infrastructure asset such as Hydro One or Hydro Québec. Criminal organizations make up number four as they are financially motivated to conduct cyber attacks. Using extortion and identity theft as their modus operandi, they are able to exploit the cyber domain for financial gain. Lastly, a hacker's ability to penetrate and attack critical infrastructure where the motivations are "much less sinister" is typically to increase their status as a hacker.[30]

Government networks tend to be targets of cyber attacks by state or non-state sponsored hackers. Hackers probe these networks looking for vulnerabilities to exploit and seeking to gain access to the myriad of classified information vital to military operational and national security.[31] Not only has the Canadian Armed Forces been hit with this type of cyber attack, the United States was the victim of a massive cyber attack called Moonlight Maze, a highly classified probing of computer systems at the Pentagon, National Aeronautics and Space Administration (NASA), Energy Department, private universities, and research labs. This continuous attack allegedly went on for two years before it was discovered. As a result, thousands of files including military equipment

[30] Edward G. Amoroso, *Cyber Attacks…,* 5.
[31] Public Safety Canada, *Canada's Cyber*…, 9.

design and military installation maps were downloaded which was allegedly traced back to Russia who denied involvement.[32]

When thinking about cyber attacks and how they differ from physical attacks, there are two distinct identifiers. Firstly, cyber attacks are not subject to the typical laws of physics compared to traditional attacks. They literally move at the speed of light and have no geographical or political boundaries. Secondly, a cyber attack refers to the target in the digital realm and does not cause direct physical damage to a target. Its primary target is normally a computer or the information on it however; the results of the cyber attack may have an impact on the physical realm. This is where the example of Stuxnet comes into play.[33]

The Stuxnet worm was the first of its kind to bridge the gap between a cyber attack and a physical attack causing damage. The supervisory control and data acquisition (SCADA) is used to run and monitor industrial processes for much of modern technological society in everything from management and operation of gas pipelines, oil refinery controls, wastewater treatment to and transportation controls (subways, trams).[34] SCADA is "…composed of computers, networks, and sensors to control industrial processes by sensing and collecting data from the running process, analyzing that data to determine how best to control it and then sending signals back through a network to adjust or optimize the process."[35]

---

[32] PBS Frontline, "The Warning?" accessed 6 May 2014, http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/

[33] Singer, *Cybersecurity…*, 69.

[34] Lewis, *Critical Infrastructure Protection*…, 223.

[35] Ibid., 228.

Why Canada should be concerned

Canada's national critical infrastructure is essential and needs to be protected. Cyber security measures matter for the safety of all Canadians through the protection of critical public services as well as for defending Canada's secrets and its critical infrastructure. Regardless of their origin, cyber attacks from high-tech international terrorists, state and non-state sponsored espionage pose a legitimate threat and must be defended against.[36]

Cyber security is so important due to the proliferation of information technologies in the everyday lives of Canadians. From the Government of Canada to business owners and private citizens, they all collect and process an enormous amount of data on networks and computers at varying levels of sensitivity. The evolution of cyber attacks in their sophistication and numbers requires this information to be protected as a safeguard to national security.[37]

Threats to critical national infrastructure have increased in frequency and brutality within Canada and will continue to be a challenge as the techniques used in cyber attacks evolve quicker than organizations can evolve defenses.[38] This is supported by two reports from the United States. Despite increased cyber awareness within the critical infrastructure sectors, the frequency and types of attacks have increased at an alarming rate. For example, the amount of cyber attacks targeting the United States and its national critical infrastructure increased by over fifty percent in 2012 as reported by the

[36] Canadian Security Intelligence Service, "Assessing…,
[37] University of Maryland, "Cyber Security…,
[38] Auditor, *Report of the Auditor*..., 2.

Department of Homeland Security. The majority of these attacks were focused on the energy sector, water industry, chemical plants, and even six nuclear companies.[39]

Due to the interconnectedness of Canada and the United States, there is potential for collateral damage bi-nationally. Simply put, Canada's threat levels are directly linked to those of the United States.[40] This is evidenced by the blackout of 2003. The disruption which started in Ohio caused the largest blackout ever recorded in North America. According to reports the blackout left fifty million people from New York to Toronto without power. In addition, the outage created cascading effects on other critical infrastructures such as the public health and water treatment plants. The facilities had to operate solely on generators, food and water supplies were at risk as well as the economic impact to grocery stores through loss of revenue by throwing out the spoiled food. Other services that were affected were banking, gas stations could not pump gas, transportation infrastructures such as airports were shut down and telecommunications services failed due to battery failure at the cell towers.[41] This outage was not due to a cyber attack however, it does highlight the havoc that could be caused and strengthens the need to be protected.

---

[39] DailyTech.com. "DHS: Cyber Attacks Against U.S. Infrastructure Increased by 52 Percent in 2012." accessed 8 May 2014. http://www.dailytech.com/DHS+Cyber+Attacks+Against+US+Infrastructure+Increased+by+52+Percent+in+2012/article29632.htm.

[40] Graham, *When is Safe*…, 17.

[41] Public Safety, *Position Paper on a National Strategy*…, 9.

ROLES

Role of each key actor

Keeping in mind Canada's interdependencies with the United States, private sector, civilian population, it is clear that no one entity or organization can adequately ensure the protection of these assets against cyber attacks with regards to critical national infrastructure. This leads into the next section in describing what role each has to play to ensure the protection of national security and public safety. According to the National Strategy for Critical Infrastructure, the responsibility to protect Canada's national critical infrastructure does not belong to one person or entity in fact it belongs to the government (federal, provincial and territorial), critical infrastructure owners and operators, and individual Canadians.[42]

By its very nature critical national infrastructure is multifaceted, complex, and is comprised of numerous moving parts. Therefore, the protection against all physical and electronic threats including cyber is the responsibility of all stakeholders. That said, "Canada's critical infrastructure is massive, geographically dispersed, owned by many different players mostly within the private sector, and vulnerable."[43] In order to ensure they are properly protected from cyber attacks it will take all four principle actors' involvement to ensure these assets' safety. These players which will be discussed in this next section are the government, private sector, citizens, and the United States.

---

[42] Public Safety Canada, "National…, 2.
[43] Graham, *When is Safe*…, 2.

Government

Canada developed five key elements to ensure the successful protection of national critical infrastructure. The five elements were developed as guiding principles to align with the strategy's objectives which are "awareness, integration, participation, accountability, and all-hazards approach."[44] To be successful, it is essential for the government to provide national leadership "to help reduce vulnerabilities, detect threats and risks more effectively, and improve response and recovery efforts and timing."[45] With respect to the Government of Canada, its role fulfills mainly a management and leadership role when dealing with the protection and management of critical infrastructure during emergencies in conjunction with the private sector. They of course must do this while respecting the jurisdictions and legislation of the provinces and will provide direct assistance upon request from the province during an emergency. [46]

Effectively, the Government of Canada focuses on perfecting methods to provide protection to ensure the sustained provisions of vital services and amenities to Canadians. To achieve the protection and assurance needed, the Government of Canada will strive for better "information collection, assessment and sharing, and through risk management."[47] In building trusted partnerships and better coordination, as part of the National Strategy for Critical Infrastructure, the strategy proposed sector networks to ensure a framework for information sharing to facilitate unique activities pertaining to each of the sectors such as risk assessments and action plans.[48]

---

[44] Public Safety, *Position Paper on a National Strategy*…, 6.
[45] *Ibid.,* 3.
[46] Public Safety Canada, "National…, 2.
[47] Public Safety, *Position Paper on a National Strategy*…, 5.
[48] Public Safety Canada, "National…, 6.

Specifically associated with cyber threats, the Government of Canada has produced a number of strategies and policies as well as leveraged their relationship with the United States to coordinate guidance. For instance, in Canada's Cyber Security Strategy, the federal government is committed to working with all levels of government to facilitate a whole of government approach as well as the private sector for the protection of Canada's national critical infrastructure through the implementation of a cyber security strategy.[49] It directly builds on the partnerships as directed by the National Security and Action Plan for Critical Infrastructure…."[50] To highlight the importance of the United States, the recognition of the relationship between the two economies was solidified with the "Beyond the Border" declaration signed by the President of the United States, Barrack Obama and the Canadian Prime Minister, Stephen Harper. In essence, the declaration states that the two countries will work together with a view to ensuring that there are no disruptions from physical or cybernetic attacks takes place and to prevent or reduce the impacts that a disruption might have on critical infrastructure if it were to occur.[51] As seen with the blackout in August 2003 previously mentioned, it does little use to reinforce power generation infrastructure protection on one side of the border when the outages have cross-border impacts form either a cyber attack or natural disaster.[52]

Private Sector

With over eighty five percent of the nation's critical infrastructure, it makes perfect sense that the owners and operators have a major role to play in the protection of

[49] Public Safety Canada, *Canada's Cyber*…, 1.
[50] *Ibid.,* 1.
[51] Paul Rosenzweig, The International Governance Framework for Cybersecurity, Canada-United States Law Journal Vol 37. Issue 2, 2012, 430.
[52] Rosenzweig, The International Governance…, 430.

their assets. Strengthening the private sector's resiliency to cyber attacks is paramount given the connective nature of their systems and reliance on SCADA controls for optimization of its operations. That said, the government protects their critical infrastructure networks as well and supports the private sector in addressing the challenges of resiliency to their cyber threats in a collaborative way. [53]

It is clear that with the largest portion of the nation's critical infrastructure, the private sector has an enormous role to play in its protection and sustainability.[54] Private sectors' views differ on cyber security from that of the government which are mainly from a money-making perspective where the balance is between risks and profit which drives the cyber security efforts.[55] Further, their efforts to secure themselves with respect to cyber threats help drive research and development, design, and implementation of services within cyberspace. Partnering with the public sector for more than two decades has enabled the development of national and international cyberspace security strategies.[56]

Companies are reluctant to share vulnerabilities however, real life experience is critical to the overall security of the sector networks and protection of national critical infrastructure.[57] Therefore, specifically in a number of Canadian strategies, in order to protect critical infrastructure from cyber attacks, the private sector needs to actively pursue information sharing from government and other partners to adequately prepare for

---

[53] Public Safety Canada, "National…, 5.
[54] Graham, *When is Safe*…, 23.
[55] Brigid, Grauman, "Cyber-security: The vexed question of global rules An independent report on cyber-preparedness around the world," McAfee, February 2012, 35.
[56] House of Representatives, "Written Testimony of Scott Charney, Corpoate Vice President, Microsoft Corporation's Trustworthy Computing:" http://www.whitehouse.gov/files/documents/cyber/Congress%20-%20Charney-microsoft-SFR_10Mar09.pdf, 4.
[57] Grauman, "Cyber-security: The vexed…, 35.

current and emerging threats.[58] This includes sharing their known vulnerabilities and threats to their critical infrastructure to intelligence and security agencies and ensuring timely reporting of compromised networks to fortify network defences across the spectrum of services. Further, sharing their development of rapid action capabilities to prevent or reduce impacts of cyber attacks and adoption of a lesson learned framework for application in future success. [59] Finally, this sharing reinforces the importance of developing cyber security procedures, identifying cyber threats no matter the origin (international terrorist, non-state or state based espionage) aimed at critical infrastructure which are all a threat to national and public security and safety.[60]

The individual Canadian

With respect to national critical infrastructure and its disruption, degradation, or destruction, the primary responsibility of the individual Canadian is to ensure they are prepared and ensure their families have the capacity to cope with the outage for at least seventy two hours.[61] Individuals also play a role in cyber security for critical infrastructure protection. As stated in Canada's Cyber Security Strategy, each individual has a responsibility and role to play in securing cyberspace within Canada. In conjunction with the policies and initiatives that the Government of Canada has put in place, it is up to each individual to protect themselves while online.[62] For example, the average user's computer that is connected to the Internet can become victim to a hacker through a virus

[58] Canadian Security Intelligence Service, "Assessing…,
[59] Canadian Security Intelligence Service, "Significant Cyber Incidents Since 2006," accessed 6 May 2014, http://csis.org/files/publication/140310_Significant_Cyber_Incidents_Since_2006.pdf, 47-48.
[60] Ibid.
[61] Public Safety Canada, "National…, 5.
[62] Public Safety Canada, *Canada's Cyber*…, 8.

or malware attack. Unaware of the attack, the hacker has full access to their computer as part of a "zombie" attack against other networks through spam, phishing, or even as part of a denial of service attack against the critical infrastructure networks. [63]

For Canadians, there are a number of ways to protect themselves from becoming an asset or cyber weapon for a hacker. This can be accomplished through awareness of threats and properly protecting themselves through antivirus software, internet protection tools, and strong passwords.[64] In looking at the impact this can have, the attack in South Korea[65] or Estonia in 2007 are good examples. Using a number of techniques including "zombie" computers, the attacks targeted government, banks, universities' websites, and Estonian media outlets. Following several weeks of attacks, the affected networks had to be disconnected, successfully cutting off one of the "most wired countries in Europe" from the outside world.[66]

Cybersecurity is and will remain an integral part in the lives of all Canadians. With emerging cyber threats, it is essential that the public plays their role in protecting critical infrastructure networks. For citizens of Canada, cyber security cannot be an afterthought and must be made as part of daily life to change behaviours to be better protected. Through coordination with the government, campaigns such as the Cyber Security Awareness Month are designed to keep everyone educated and safe. From Canada's Minister of Public Safety, the Honourable Vic Toews, "…The *Get Cyber*

---

[63] Trendmirco. Zombie PC definition. accessed 6 May 2014. http://www.antivirus.com/security-software/definition/zombie-computers/index.html.

[64] Department of Homeland Security, "Protect Myself from Cyber Attacks," accessed 6 May 2014, https://www.dhs.gov/how-do-i/protect-myself-cyber-attacks.

[65] Wired, "Logic Bomb Set Off South Korea Cyberattack," accessed 30 April 2014. http://www.wired.com/2013/03/logic-bomb-south-korea-attack/.

[66] Jason, Richards, "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security." *International Affairs Review* Volume XVIII, no. 1 (2009), http://www.iar-gwu.org/node/65.

Safe campaign provides Canadians with the information they need to protect themselves and their families against online threats. This is a shared responsibility, and we all have a role to play in cyber security."[67]

United States

As with the Canadian critical infrastructure, the United States is increasingly at risk of attacks through the Internet from the same types of groups that wish to do harm on Canadian infrastructure. The interconnectedness of their network centric infrastructure opens them up to a myriad of threats which has the potential to compromise national security and their economic system. Moreover, critical infrastructure for the United States represents the same types of critical services as Canada and includes the telecommunications networks both wired and wireless, water purification and treatment facilities, as well as the energy generation sectors for the nation.[68] Protection of these services is critical to "the resilience and reliability of the nation's critical infrastructure and key resources; therefore, to our economic and national security."[69]

The United States seems to be clearly in the lead when it comes to policies and legislation for protecting national critical infrastructure. Similar to that of the Government of Canada, it focuses on public safety and the maintenance and security of its critical infrastructure. As our closest ally, the United States has a role to play in the

---

[67] Public Safety Canada, Government of Canada Launches Cyber Security Awareness Month with New Public Awareness Campaign Partnership, accessed 8 May 2014, http://www.publicsafety.gc.ca/cnt/nws/nws-rlss/2012/20120927-1-eng.aspx.

[68] Department of Homeland Security, Protecting Our Nation's Critical Infrastructure from Cyber Threats, accessed 8 May 2014, http://www.dhs.gov/protecting-our-nations-critical-infrastructure-cyber-threats.

[69] Department of Homeland Security. "About the National Cybersecurity and Communications Integration Center." accessed 3 May 2014. http://www.dhs.gov/about-national-cybersecurity-communications-integration-center.

protection of Canadian critical infrastructure mainly due to the interconnectedness and interdependencies of the two countries. So much so that to promote information sharing and a collaborative approach to critical infrastructure protection, Canada has engaged not only with the United States but with Canada's other international partners to enable the strengthening of the backbone for critical infrastructure. [70] As previously mentioned, the blackout of 2003 is a perfect example of why this is necessary. From the mid-nineties, starting with the Executive Order 13010 on Critical Infrastructure Protection to the latest Executive Order 13636 regarding Improving Critical Infrastructure Cybersecurity, security of these assets is recognized as potential threats to national and economic security of the nation,[71]. This is to be accomplished through the interagency ((National Institute of Standards and Technology) (NIST), Department of Homeland Security (DHS), Department of Defense (DoD)) partnerships with the owners and operators of critical infrastructure to address cyber threats. To achieve this, the focus is on developing a cybersecurity framework, improved information sharing as seen in the Canadian framework, and a review of established cyber regulation to name a few of the initiatives.[72]

From the outset, the United States pushed a number of executive orders and created a number of organizations to protect critical infrastructure from cyber threats. For instance, as part of the Department of Homeland Security, the National Cybersecurity & Communications Integration Center was created in response to the increased level of cyber threats to national critical infrastructure. The National Cybersecurity &

---

[70] Public Safety Canada, "National…, 5.
[71] The White House, "Executive Order 13010..., accessed 2 May 2014.
[72] Office of the Press Secretary, "Executive Order --- Improving Critical Infrastructure Cybersecurity," accessed 9 May 2014, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

Communications Integration Center is the central point for all interagency local and federal, private sector and international to provide a better understanding of cybersecurity and the threats within cyberspace. [73] "It is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats."[74]

It is clear that Canada and the United States have their dependencies on one another due to the interconnectedness of the critical infrastructure. This translated into a glaring requirement to have mutual assurance on the way ahead for cybersecurity. The signing of the Canada-United States Action Plan on Critical Infrastructure is a clear indicator of the shared understanding of its importance. It is designed to promote an "…integrated approach to critical infrastructure protection and resilience by enhancing coordination of activities and facilitating continuous dialogue among cross-border stakeholders." [75] Through this framework, the bi-national plan aims to fortify the safety, security and resiliency of the two countries through an all-inclusive bi-national approach to critical infrastructure security.[76] In addition to this, the "Beyond the Borders" declaration, Canada shares emergency management measures with the United States to further identify risks and protect interconnected infrastructure against threats, either through physical or cybernetic means.[77] "The highest value of United States-Canada

---

[73] DHS, "About the National Cybersecurity…, accessed 3 May 2014.
[74] Press Secretary, Improving Critical Infrastructure…, accessed 9 May 2014.
[75] Public Safety Canada, "Canada-United States Action Plan on Critical Infrastructure," accessed 8 May 2014, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cnd-ntdstts-ctnpln/index-eng.aspx.
[76] Ibid.
[77] Public Safety Canada, "National…, 5.

cybersecurity cooperation is, at this juncture, probably American willingness to share best practices and other operational capacities."[78]

Thus, as highlighted in the last section, Canada needs all levels of government, the private sector, individual Canadians and the United States to properly protect the Canadian critical infrastructure.

CONCLUSION

This essay looked at Canada's national critical infrastructure and the importance of partnerships in its protection. It focused on the cyber threats, roles of key players in its protection, as well as the importance of protecting these assets.

Evidenced throughout this essay, it is clear that critical infrastructure is complex and susceptible to many forms of cyber attacks. The consequences demonstrated by the examples placed throughout the essay illustrate the requirements to protect critical infrastructure. The potential life-threatening impacts that cyber attacks cause could also have major economic and national security implications. Supported by the information presented throughout, the Government of Canada cannot adequately protect the entire critical infrastructure alone. To reiterate, cyber security and protection for national critical infrastructure is a shared responsibility where the members of the society also play a most important role.[79]

The fact that cyber attacks are still happening and increasing at an alarming rate fifty percent in 2012 against critical infrastructure targets compared to 2011, illustrates that improvements are required with respect to cyber security and critical infrastructure.

---

[78] Rosenzweig, The International Governance…, 432.
[79] DHS, Protecting Our Nation's Critical…, accessed 8 May 2014.

Through strong partnerships and a collaborative approach between the United States and Canada as well as the Government of Canada and the private sector, cyber security can be achieved to minimize the risks to national critical infrastructure.

Therefore, based on the information, the Government of Canada is meeting its leadership and coordination responsibilities as it is putting the strategies in place as well as the sector networks to facilitate the protection of the critical infrastructure assets. This does not say that the strategies are all working as effectively as they should, however with further development, investment and coordination from the other main players (private sector, citizens, and the United States) they will continue to evolve with the cyber threats as the government cannot do it alone.

BIBLIOGRAPHY

Amoroso, Edward G. *Cyber Attacks: Protecting National Infrastructure*. Burlington:Butterworth-Heinemann, 2011.

Canada. Canadian Security Intelligence Service. "Assessing Cyber Threats To Canadian Infrastructure." (Ottawa: Canada Communication Group, 2012). accessed 6 May 2012, https://www.csis-scrs.gc.ca/pblctns/ccsnlpprs/20121001_ccsnlpprs-en.php.

Canada. Canadian Security Intelligence Service. "Significant Cyber Incidents Since 2006." accessed 6 May 2014. http://csis.org/files/publication/140310_Significant_Cyber_Incidents_Since_2006.pdf.

Canada. 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*. Ottawa: Canada Communication Group, Fall 2012, http://www.oag-bvg.gc.ca/internet/docs/parl_oag_201210_03_e.pdf.

Canada. Public Safety and Emergency Preparedness Canada. *Position Paper on a National Strategy for Critical Infrastructure Protection*. Ottawa: Canada Communication Group, November 2004.

Canada. Public Safety Canada. *National Strategy for Critical Infrastructure*. Ottawa: Canada Communication Group, 2009. http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-eng.aspx

Canada. Public Safety Canada. "Government of Canada Launches Cyber Security Awareness Month with New Public Awareness Campaign Partnership." accessed 8 May 2014. http://www.publicsafety.gc.ca/cnt/nws/nws-rlss/2012/20120927-1-eng.aspx

Canada. Public Safety Canada. "Canada-United States Action Plan on Critical Infrastructure." accessed 8 May 2014. http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cnd-ntdstts-ctnpln/index-eng.aspx.

Canada. Privy Council Office. *Securing an Open Society: Canada's National Security Policy*. Ottawa: Canada Communication Group, 2004, http://publications.gc.ca/collections/Collection/CP22-77-2004E.pdf.

Canada. Public Safety Canada. *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada*. Ottawa: Canada Communication Group, 2010.

Cavelty, Myriam Dunn. *Cyber-Security and Threat Politics: US efforts to secure the information age*. New York: Routledge Taylor and Francis Group, 2008.

DailyTech.com. "DHS: Cyber Attacks Against U.S. Infrastructure Increased by 52 Percent in 2012." accessed 8 May 2014. http://www.dailytech.com/DHS+Cyber+Attacks+Against+US+Infrastructure+Increased+by+52+Percent+in+2012/article29632.htm.

Dickinson, Don. *Protecting Water Industry Control and SCADA Systems from Cyber Attacks*. Harrisburg: Phoenix Contact.

Graham, Andrew. *Canada's Critical Infrastructure: When is safe enough safe enough?* MacDonald-Laurier Instituted, 2011, http://www.macdonaldlaurier.ca/files/pdf/Canadas-Critical-Infrastructure-When-is-safe-enough-safe-enough-December-2011.pdf

Grauman, Brigid. Cyber-security: The vexed question of global rules An independent report on cyber-preparedness around the world. McAfee,February 2012.

Lewis, T.G. *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*. New Jersey: John Wiley and Sons Inc, 2006.

Libicki, Martin. *Cyberdeterrence and Cyberwar*, Washington DC: RAND, 2009. http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

NATO. The History of Cyber Attacks – a timeline, http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm

PBS Frontline. "The Warning?" accessed 6 May 2014. http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/

Rid, Thomas. *Cyberwar Will Not Take Place*. Oxford: Oxford University Press, 2013.

Richards, Jason. *"Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security." International Affairs Review* Volume XVIII, no. 1 (2009), http://www.iar-gwu.org/node/65.

Rosenzweig, Paul. *"The International Governance Framework for Cybersecurity"*, Canada-United States Law Journal Vol 37. Issue 2, 2012.

Saad, S., Bazan, S., and Varin, C. "Asymmetric Cyber-warfare between Israel and Hezbollah: The Web as a new strategic battlefield." *Journal of Webscience* (2011): 14-17, http://journal.webscience.org/526/1/96_paper.pdf, accessed 03/03/2014.

Singer, P.W., and Allan Friedman. *Cybersecurity and Cyberwar: What everyone needs to know.* Oxford: Oxford University Press, 2014.

Trendmirco. Zombie PC definition. accessed 6 May 2014. http://www.antivirus.com/security-software/definition/zombie-computers/index.html

Rosslin, John Robles, Min-kyu, Choi, Eun-suk Cho, Seok-soo, Kim, Jang-Hee Lee. Common Threats and Vulnerabilities of Critical Infrastructures. International Journal of Control and Automation. 17-22.

United States. Department of Homeland Security. "Protect Myself from Cyber Attacks." accessed 6 May 2014. https://www.dhs.gov/how-do-i/protect-myself-cyber-attacks

United States. Department of Homeland Security. "Protecting Our Nation's Critical Infrastructure from Cyber Threats." accessed 8 May 2014. http://www.dhs.gov/protecting-our-nations-critical-infrastructure-cyber-threats

United States. Department of Homeland Security. "About the National Cybersecurity and Communications Integration Center." accessed 3 May 2014. http://www.dhs.gov/about-national-cybersecurity-communications-integration-center.

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

United States. The White House. "Executive Order 13010: Critical Infrastructure Protection." accessed 2 May 2014. http://www.fas.org/irp/offdocs/eo13010 htm.

United States. Office of the Press Secretary. "Executive Order --- Improving Critical Infrastructure Cybersecurity." accessed 9 May 2014. http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

University of Illinois, History of the Internet, accessed 11 May 2014, http://education.illinois.edu/wp/commercialism/history-of-the-internet.htm

University of Maryland. "Cyber Security." Accessed 6 May 2014. http://www.umuc.edu/cybersecurity/about/cybersecurity-basics.cfm.

Wired, "Logic Bomb Set Off South Korea Cyberattack," accessed 30 April 2014. http://www.wired.com/2013/03/logic-bomb-south-korea-attack/.