6-1-2015

The threat of state sponsored Cyber attacks in Canada: to serve and protect

Andrew MacDougall

The American University in Cairo

School of Global Affairs and Public Policy

"The Threat of state sponsored Cyber Attacks in Canada: To serve and protect"

A Masters Project Submitted
in partial fulfillment of the requirements for Global Affairs

By

Andrew J. MacDougall

Spring 2015

The American University in Cairo

School of Global Affairs and Public Policy

"The Threat of state sponsored Cyber Attacks in Canada: To serve and protect"

A Masters Project by

Andrew James MacDougall

Spring 2015

In partial fulfillment of the requirements for the
Master of Global Affairs and in conjunction with enrollment in PPAD 5293; The Master's Project (Spring/2015)

This project has been evaluated by:

Dr. Allison Hodgkins
Project advisor,
Department of Public Policy and Administration
The American University in Cairo
Date: May 2015

Dr. Sameh Aboul-Enein
Project reader,
Department of Public Policy and Administration
The American University in Cairo
Date: May 2015

Dr. James H. Sunday
Project Reader,
Department of Political Science
The American University in Cairo
Date: May 2015

The American University in Cairo
School of Global Affairs and Public Policy
Department of Public Policy and Administration

"The Threat of state sponsored Cyber Attacks in Canada: To serve and protect"

Andrew James MacDougall

Completed in conjunction with Dr. Allison Hodgkins in conjunction with enrollment in PPAD 5298; The Master's Project (Spring /2015)

ABSTRACT

This Masters of Global Affairs project has been constructed for the use as a piece contributing to policy recommendations for the Canadian Federal government on their response to handling state-sponsored cyber attacks on critical national infrastructure (CNI) in Canada. Throughout this project an exploration is undertaken to understand the means of attacks that Canada has faced since the millennium, as well as to see what defense and security measures were of use, and what security measures were under-utilized. By exploring these attacks to Canada's CNI, clarification on improvements for the federal government on its future state of cyber defense become available. This project will also look to shape policy recommendations that can be considered in further national security agenda creation as well as governmental policies affecting domestic, and global governance on cyber attacks.

TABLE OF CONTENTS

1. Introduction

Cyber space is growing; and as such, government reliance on cyber space has paralleled that growth. With the more reliance placed on cyber systems, there is an increased risk of being the victim of a cyber attack. As the powerful states that possess cyber capabilities grow in strength, so do their capacity to attack those states perceived as either posing a threat or who are perceived as vulnerable. It will be up to the Canadian government to respond to the threat of cyber attacks by other states to ensure the lives of over 35 million people are not jeopardized. Critical National Infrastructure (CNI) and the daily operations could be responsible for "normal" livelihood as Canadians know it. So what could happen if CNI is attacked by another state?

As of October 2010, Canada recognized "information security threats" as one of the top five priorities on Canada's Cyber Security Strategy (CCSS). The cyber security strategy was launched in 2010, addressing cyber security practice by Canadian Department of National Defense (DND) and military allies. The issue of cyber attacks is listed as being in the top five priorities has also led the Canadian military to operate electronics attacks and network operations. Currently, Canadian forces information operations group has allied with its allies to "gain and maintain cyber superiority".[1] Furthermore, my research concerns the question how has Canada positioned itself on the defense and response to cyber attacks by state actors against its CNI.

[1] Lewis, James A., and Katrina Timlin. "Cybersecurity and Cyberattacks Preliminary Assessment of National Doctrine and Organization." UNIDIR. Center for Strategic and International Studies 30 Sept. 2014. <http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberattacks-preliminary-assessment-of-national-doctrine-and-organization-380.pdf>.

The purpose of this project is to assess Canada's cyber security policy and whether the Canadian government is placing sufficient priority to the threat posed by attacks emanating from Cyber-space. Throughout this research I set out to create an understanding and analysis of the readiness Canada has to address and protect itself from the threat of state sponsored cyber attacks, as well as to seek recommendations for the Canadian government on cyber security. This will include an assessment of what Canada has done to create a resilient cyber space and protect its state and CNI from cyber attacks by other states. Inclusively, by exploring what Canada has already done to respond to threats of cyber attacks, a reflection and analysis can be done to see what has been successful, what has failed, and what policy recommendations can be implemented to improve its defensive functionalities.

Canada may be facing similar threats to other developed countries, however the pro-active and reactive approaches may be allowing cyber attacks and its threats to enter through the front door. Further, the problem of not prioritizing cyber security as the leading threat to Canada's national security is perceived as a major discrepancy by many experts, policy makers and academics.[2] By not prioritizing cyber security on Canada's national security agenda, Canada could be missing an opportunity to create a more resilient response system and the opportunity to strengthen its own national security beyond that of its current position. However, perhaps Canada does not have the right strategies, techniques, programs and talent to respond to the threat of cyber attacks. The discrepancy is approached from many angles, addressing multiple issues that are

[2] See, literature review

understood as, issues that can be resolved through a variety of changes to Canada's cyber security strategy and national security agenda. These changes and policy recommendations will form the foundation and principal elements that create the purpose behind this research, as well as to understand Canada's response to cyber attacks. The federal government must draw its attention to cyber attacks in Canada as our lives completely revolve around this growing information technology environment. Canadians use the internet for an array of things in our lives; including, but not limited to; research, banking, stock trading, communications, military, political, self-interest, business, air traffic control and national defense. Moreover, the current environment of vulnerability includes personal use, use by businesses, government use, and all public and private use of cyber space. If we are unable to secure the advancement of technology in Canada, it is understood that it will present the same risks as if Canada did not protect its physical boundaries from attacks. We should view our current environment as a vulnerable state for sabotage or espionage and seek to find methods to prevent cyber attacks against the Canadian state.[3] However, this research will reflect Canada's response to cyber attacks against Canada's CNI(Critical National Infrastructure), not its citizens CNI refers to 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. Critical infrastructure can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders.

[3] "INFORMATION ATTACKS: CYBER ATTACKS IS THE FUTURE ATTACKS." Global Information Assurance Certification. 27 Sept. 2014. <http://www.giac.org/paper/gsec/3873/information-attacks-cyber-attacks-future-attacks/106165>.

Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects and significant harm to public confidence."[4]

The threat of cyber attacks must be understood in the context and severity that any state, large or small has the potential to attack unilaterally or be networked as a multi-state attack to create harm against the nation of Canada. By Canada responding alone (e.g. China attacking Canada in 2011) or as part of a networked attack (e.g. USA and Canada compromising Iranian nuclear enrichment program through the use of infectious computer malware), the threats become unlimited in its potentiality. With that being said, global affairs and international influences in the upcoming decades could influence the way resource-rich states network together to have negative effects on other states. With these concerns in mind, Canada has employed many techniques, such as intelligence-gathering and surveillance to address cyber attacks, lending priority to our understanding these threats and the adoption of decision-making policies that prevent these attacks.

Cyber attacks, for this purpose of this investigation is defined as follows. 1). As a politically or non-political motivated attack against an adversary via use of the Internet. Cyber attacks have the potential to disable governmental, personal, financial, and organizational systems through methods of hijacking or altering classified data to undermine networks, websites and services. 2). A massively coordinated digital assault on a government by another, or by large groups of citizens.[5] It is the action by a nation-state to penetrate another nation's computers or networks for the purposes of causing

[4] Critical Infrastructure. (2014, March 20).http://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-eng.aspx

[5] Cyber Attacks Law & Legal Definition Retrieved November 19, 2014, http://definitions.uslegal.com/c/cyber-attacks/

damage or disruption. 3) The term cyber attacks may also be used to describe attacks between corporations, from terrorist organizations, or simply attacks by individuals called hackers, who are perceived as being warlike in their intent.[6]

This investigation will address methods of sabotage and espionage, as well as all other methods and forms of cyber attacks that have presented themselves to the environment as defined above, as well as the existential threats that are present and are understood as potentially forth coming. Throughout this research, sabotage and espionage will be understood and defined by the following. Sabotage is the disruption of a normal operation. For example, the Canadian military having their operation altered or compromised by a third party, being state actor(s). Espionage is used to disable computers, networks, software, steal or acquire data for military, financial or political gain.[7] The relevance of this research will expose the current situation that Canada faces against the threat of cyber attacks in perspective of grounded theory research and case studies. The threat will be assessed and analyzed to explore new policy objectives in alignment with preventative measures made by countries such as the United States and will seek to have new policy strategies created.

This exploration will help determine how Canada ranks against other powerful states in comparison. This research will find its importance and relevance by the increasing levels of public awareness through social media and news broadcasting, as well as openly documented and declassified cases of cyber attacks and governmental

[6] Ibid.
[7] "What is Cyberattacks (Cyber War)? - Definition from Techopedia." *Techopedia*. 27 Sept. 2014. <http://www.techopedia.com/definition/1360

properties that experienced cyber threats or attacks, directly or indirectly. Relevance will be drawn primarily from recent global circumstances to enhance the cause of severity for increased priority on the Canadian national security agenda. Concluding this research, transparency will be created as to why certain priorities face higher urgency for the Canadian Government, and expansive support for restructured agenda policies and priorities will be implemented. There are many unknowns about the uses of cyber attacks and to exactly what extent these malicious attacks could be carried out to. To expand, we must also consider the drastic repercussions of something as obscure as a state hacking clocks on international trade markets, and understanding the impact that it could have on Canada. By this form of attack that could be done in a few milliseconds, it could determine where a currency or precious metal could close at the end of the day on the TSX. Understanding that this is real threat, the outcome of this attack could have severe consequences on economic prosperity. This example could potentially allow countries to get a multi-million, even billion dollar advantage on international trade in theoretically a few milliseconds. To further understand, we shall begin by exploring the over arching research question of the prioritization on cyber attacks by the Canadian Government on its agendas and in formulating policy.

2. Research Question

How has Canada positioned itself on the defense and response to cyber attacks by state actors against Canada's CNI?

For the purpose of this research, the question of how Canada has positioned itself on the defense and response is a means to explore Canada's vulnerability to threats in this age of technology and how those threats can be addressed with policy prescriptions. Throughout my research I maintain that the threat needs greater priority on the Canadian national security agenda, and for a greater attention to the realization of the current presence that cyber attacks has on Canada. Assistant Deputy Minister Harlick from the Office of Critical Infrastructure Protection and Emergency Preparedness for DND said during the Y2K campaign that the internet is "immature, unsecured, and unstable." In addition, Harlick proved that "malicious attacks" of cyber attacks increased 430% between 1999-2000 and 525% in 2001.[8] As outlined in my analyses (section 9) clear evidence and statistics are shown on the increasing amounts of attacks. Based on these figures provided by the Parliament of Canada during the Senate Committee on National Security and Defence, it is evident to see the threat emerging since before the turn of the millennium. As Harlick has explained, the internet is "unsecured", which concerns the national security of Canada. Just as if the national waters or ports in Montreal, Vancouver or Halifax were unsecured this would be a major concern receiving utmost attention by

[8] "CANADIAN SECURITY AND MILITARY PREPAREDNESS The Standing Senate Committee on National Security and Defence." Parliament of Canada. 29 Sept. 2014. <http://www.parl.gc.ca/Content/SEN/Committee/371/defe/rep/rep05feb02-e.htm#15.%20Countering%20National%20T

the Parliament, DND, RCMP, and CSIS. In other words, as new threats emerge beyond the bounds of our conventional "physical" understanding of national security, policy-making must reflect the changing nature of what it means to protect a state's national security. To understand where Canadian national security rests, investigating the current threats in 2014 will create an understanding of why cyber attacks remain a critical concern for Canada's state interest.

3. Background

Within the Canadian Cyber Security Strategy (CCSS), the government of Canada outlined a five-year plan between 2010-2015. The strategy is built off three tiers, including: Securing Canadian government systems, enhancing the security of cyber technology beyond the Canadian federal government, and ensuring Canadian safety while engaging in online use.

In 2011, the Canadian government successfully " streamlined" data centers, email, and federal IT communications; a step towards creating a tighter, and more secure cyber space (beginning in 2011). In 2011, the Canadian government also launched national public awareness through the " GetCyberSafe" campaign that keeps Canadians informed on how to ensure their own safety while using the Internet. GetCyberSafe is one step towards the creation of resilient cyberspace for Canada and its citizens. Through the creation of partnerships and streamlining the mentioned above, the Canadian government is able to utilize security measures from all of its partners, increase intelligence abilities, increase the ability to communicate and fight cyber attacks.

Moreover, in 2012; the Canadian government added additional funding to enhance protection of IT for Canadians... claiming it was to only strengthen the “already secure, stable and resilient digital infrastructure". Understanding that the federal government has made a claim as " already secure" is more than ambitious, and in fact incoherently incorrect. As mentioned in section II, Harlick (DND) stated that the Internet is " immature, unsecured, and unstable". The strategy has been implemented through the 2010-2015 time frame by engaging a cross-network governance strategy with all departments and agencies in Canada working towards the common goal of securing Canada's cyber security. The strategy includes governance from (but not limited to); Department of National Defence, Royal Canadian Mounted Police, Justice Canada, Canadian Forces, Department of Foreign Affairs and International trade, and Communications Security Establishment Canada.

Beyond the Canadian governments actions, 2012 saw Canada sign the Cyber Security Action Plan in cooperation with the United States. The goal of this agreement is to help protect critical digital data between the neighboring states. However, also allowing Canada to recognize that the fight against cyber attacks is too large to handle alone, potentially even with assistance from the USA[9].

This threat to Canada’s National Security is being recognized as severe and vital (as mentioned above in the increasing amounts of attacks), needing close partnership with provincial, territorial, federal, international partners, private and public sectors to ensure secure cyber systems and that the threat is secured appropriately. The efforts have started

[9] "Action Plan 2010-2015 for Canada's Cyber Security Strategy." 4 Mar. 2014. 10 Oct. 2014. <http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/index-eng.aspx>.

being made, however; a plan is not an action, a plan is merely an opportunity for an outcome without a transfer of effort towards the attacker. In this case, if a cyber attack could be predicted, it would be then, that the government would lose sleep. Recognized as severe, grass roots approaches may need to be looked at as a part of securing cyber space for Canada and potentially its allied nations.

According to Public Safety Canada, the priorities clearly indicate that Canada has highly prioritized the threat of cyber attacks in Canada, and the various programs, agendas, councils, and strategies provide assurance measures are being taken to handle matters. The usage of the Internet in Canada is more than twice as high as the world average. Heavily dependent on the use of the Internet, Canada has the highest increase in e-commerce in 2011 involving more than forty nine billion dollars (CAD).[10] According to a recent study in 2011, Canada was found to be the only “major country" that was currently not operating a computer emergency response team.

Further, mentioned above should be looked at as a great liability, regardless of the security strategies Canada is undertaking.

3.1 Current State of Threat and Response

Listed as the sixth most likely nation in the world to undergo a malicious cyber attack by comscore, more than 36% of Canadian businesses have undergone malicious

[10] "2012 Canada Digital Future in Focus." comScore, Inc 12 Oct. 2014. <http://www.comscore.com/Insights/Presentations-and-Whitepapers/2012/2012-Canada-Digital-Future-in-Focus>.

attacks. An increase from being between the 10th and 20th position for frequency of attacks previously.[11] This form of response team seems inevitable to implement.

So why should we see Canada as unprepared?

Simply, the creation of malware and malicious viruses, spam and code that hackers and " cyber terrorists" have been using far outdates any form of developed strategy Canada holds, not to mention the severity if states are backing them. [12] Perhaps when the internet was created in the private sector by a group of people with similar mindsets and needs for creation, the risk of conflicting interests on the internet were much smaller than today. In fact, one could argue that with an ever-growing rate of users, it is foreseeable that cause for a cyber attack is merely guaranteed. As I look more into the Canadian Cyber Security Strategy (2010), it becomes more clear that the basis of its cyber security program is built similarly of the United States and Australia's Security programs, focusing on domestic threats and not international.

What becomes seemingly obvious is that the Canadian government is lagging behind the global framework and governance on cyber security is overly lacking on the end of the Canadian government. As I mentioned a grass roots approach to solving or becoming closer to halting the threat, a particular focus must be placed on municipal -> provincial -> federal government, and finally partnering with the P-5, United Nations and the international community.

---

[11] Cyber attacks have hit 36 per cent of Canadian businesses, study says. (2014, August 18 http://www.theglobeandmail.com/report-on-business/cyber-attacks-have-hit-36-per-cent-of-canadian-businesses-study-says/article20096066/

[12] "Canada's weakling Web defences." The Globe and Mail, 12 Oct. 2014. <http://www.theglobeandmail.com/globe-debate/canadas-weakling-web-defences/article580145/>.

Threats of cyber attacks from countries such as China are current. In 2012, Canada awoke to the reality that Chinese hackers had been accessing Nortel's computer networks since before Y2K. This is simply a prime example of the private sector at risk. As hackers were able to access reports, business plans, confidential documentation amongst other "secure" information, there is a direct correlation as to how this could affect e-commerce (circa $49 billion of GDP in 2011). China also threatened Canada in the early 2000's when the same group of hackers sabotaged the Federal government; accessing data from the Canadian Treasury Board, Defence Research and Development Canada, the Federal finance department, and ironically the Department of National Defence.[13]

In 2012, the cyber attacks towards the Federal government may have been to close for comfort. The hackers were able to obtain "key passwords" capable of unlocking the entire Canadian government data system. An area for concern after these two listed attacks (non-confidential) is that CSIS intel officer and senior analyst Michel Juneau-Katsuya, said that any of these attacks would have to be directly linked to the Chinese government based on the complexity. Moreover, the cooperation of the Chinese government to work together to stop further attacks seemed contradictory to what CSIS had concluded about the standing of the Chinese government. Katsuya claims that such an attack that would be carried out by the Chinese government would only be done so if

[13] "Nortel hit by suspected Chinese cyberattacks for a decade." CBCnews. CBC/Radio Canada, 14 Feb. 2012. 12 Oct. 2014. <http://www.cbc.ca/news/business/nortel-hit-by-suspected-chinese-cyberattacks-for-a-decade-1.1218329>.

the Chinese government had sought a threat from Canada in which accessing secure and sensitive data would be the only way to secure their Chinese interests.[14]

Established in 2002, The information warfare Monitor (IWM) project was created at the Munk School of Global Affairs (University of Toronto) to assist civil society groups in best practice to maximize their cyber-security, influence global cyber-security policy, and apply evidence based research to the study of cyber espionage, computer network attacks, surveillance, and malware attacks. In 2009, a cyber espionage operation out of China (GhostNet) was discovered accessing nearly 1,300 computers in more than 100 countries (30% of which were high-value targets, including ministries of foreign affairs, embassies, international organizations, new media, NGOs, and over a dozen affected Canadian government computers). Further in 2010, IWM discovered an infrastructure known as " Koobface" which in one year had generated more than two million USD (money laundering).[15] The previous two examples emphasize the concern of cyber attacks on its national agenda being created by foreign states. Further the exponential growth rate of malicious attacks should be viewed as potentially the greatest threat to national security in Canada.

[14] Weston, Greg. "Foreign hackers attack Canadian government." CBCnews. CBC/Radio Canada, 17 Feb. 2011. 12 Oct. 2014. <http://www.cbc.ca/news/politics/foreign-hackers-attack-canadian-government-1.982618>.
[15] "The Information Attacks Monitor Project Publishable Summary." Information Attacks Monitor. 12 Oct. 2014. <http://www.infowar-monitor.net/reports/IWM-Project%20Publishable%20Summary.pdf>.

4. Client Description

This research focuses on the role and response of the Federal Government of Canada in its decision-making toward cyber threats. As such, I maintain that this client should pay strict attention to the threat of cyber attacks that could be undertaken by not only domestic attacks, but also from transnational threats. To understand the interminable opportunity this threat positions Canada in, this shall be looked at as no less than exceedingly unguarded and fragile. Ranked as only a top five priority on the National Security Agenda, the federal government does not provide enough reasoning as to why it shall not be placed as the number one threat to Canada, and if Canada is truly responding to the threat of cyber attacks effectively. By selecting the Federal government of Canada as the client for this research, this provides the opportunity for the policies and recommendations set out in this research to reach a large audience including, but not limited to; CSIS, RCMP, and DND.

Public Safety Canada has led and implemented the Building Resilience Against Terrorism: Canada's Counter Terrorism Strategy in 2013-2014; however the government of Canada (2013-2014) placed the emerging threats of cyber security as its second priority. Moreover, the Canadian government placed " increasing the efficiency and effectiveness of the criminal justice system through *innovative and cost-effective* approaches" their top priority. Understanding both of these priorities involve countering crime in Canada. The threats facing cyber security also entail national security and border

strategies. Further, both priorities will be explained as well as their measures for achieving the priorities, as well as the initiatives to be undertaken.[16]

In 2010-2015, the Federal government had outlined a 10.021 billion dollar budget for planned expenses to operate the cyber security in program that is claimed to entail partnerships from all levels of governments as well as its international counterparts (USA). Additionally, countering crime has budgeted over 205 million dollars, which will, if as intended; reduce criminal activity in Canada, however unclear how it is reducing threats posed internationally. Unclear of how the Counter Crime program has received more than 20x the budget of cyber security must be also furthered explored.[17]

A transparent analysis of the priorities set out by the Federal government will further the decisions for government decisions in the future. The need for developing a national security agenda is for the benefit of Canada's nationals, its multi leveled government, private and public sector stakeholders, as well as its transnational counterparts. Vulnerability for disaster must be eliminated to its furthest potential. Not doing so leaves Canada's national security in jeopardy.

[16] "Report on Plans and Priorities 2013-2014." Public Safety Canada. 13 Oct. 2014. <http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rprt-plns-prrts-2013-14/index-eng.aspx#a13>.
[17] "Report on Plans and Priorities 2014-15." Report on Plans and Priorities 2014-15.13 Oct. 2014. <http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rprt-plns-prrts-2014-15/index-eng.aspx#s2113>.

5. Preview of Findings and Recommendations

Cyber attacks pose major threats to Canadian National Security, in particular Critical National Infrastructure. Attacks have been unexpected, threatening, damaging and scary to date particularly in those by other states. In addition threatening the daily lives of every Canadian when relying on the Internet to maintain its privacy and security protocols. It is understood that cyber attacks are unlimited in it means of use, unlike traditional means of attacks. Traditional means of attacks were attacks made my land, sea, and air. However, with the new emergence of cyber attacks as a use of attack against nations, both in the public and private sector; it is no longer enough to send military vehicles or troops to the battlefront. Simply, threats from other states has put Canada as well as other nations in such a vulnerable position to attacks, due to cyberspace and its unlimited and ever growing "front" with no border, no front line, and no tactical vantage points.

An array of issues arise from the lack of transparency and collaboration through the layers of the Canadian government are one of many issues and shortcomings of presenting as evidence that the urgency on cyber security is not being viewed as an urgent threat. An absence of communications between government agencies, military intelligence, public and private sector intelligence and cyber security regulatory authorities has also been established as a major issue on the Canadian Cyber Security Strategy that was established in 2010. Further with a very limited budget put forward by the federal government on cyber security and cyber attacks, limitations automatically

present themselves. With spending predictions up until and including 2017 at slightly over 10.021 million, there is a massive amount of opportunity missed to be able to respond to cyber security threats. Unfortunately, the 2010-2015 strategy had not understood the drastic issues; alas the budget will become a limitation as it fell over 180,000,000 dollars short as runner up for financial allowance on fighting domestic crime by increasing the effectiveness of the Canadian judicial system. The recommendations set out in this research are to create momentum on the creation of a new comprehensive cyber security agenda with focused improvements to be made by the Canadian government on handling cyber attacks presented by state actors.

6. Literature Review

In order to evaluate the level of threat and Canada's response it is first necessary to find proper definitions. A major problem when exploring cyber security and security defense mechanisms is differentiating an "attack" from a means of "warfare". Further understanding the motives for attacks and warfare, using the suitable definition and focusing on either state or non-state actors as the adversary. Cyber space is used in unlimited acts by actors to advance a political or profits agenda. Cyberspace can be of course used for peaceful purposes, daily life by any states nationals (unless forbidden by certain governments), research, medical, financial, and, but not limited to, political purposes. However, cyberspace continues to grow with negative connotation as cyber attacks become more frequent than ever before.

A Cyber attack refers to "a massively coordinated digital assault on a government by another, or by large groups of citizens. It is the action by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption. The term cyber attack may also be used to describe attacks between corporations, from terrorist organizations, or simply attacks by individuals called hackers, who are perceived as being warlike in their intent."[18]

In 2012, Ron Deibert (Munk School of Global Affairs) reflected on an outline for a comprehensive approach for Canada in cyberspace. Deibert understands the array of issues that the cyber security strategy needs to assess. A lack of transparency is set out in the strategy as to "what" needs to actually be secured and why. Understanding why cyberspace needs to be secured must be transparent. Further, the Canadian government certainly understands the necessity of protecting its borders and funding its judicial system with a budget twenty times greater than that of cyber security.[19] Through Deibert's research, the emphasis is put on the need to make more of a global effort, a need for the priority to become one of transnational interest. It is understood in Deibert's research for the Canadian Defense and Foreign Affairs Institute (CDFAI) that a new comprehensive strategy needs to be taken by the Federal government. Deibert clearly illustrates the threat that the infinite growth rate of cyberspace also means an increase in the threat of cyber attacks towards Canada.

[18] Cyber Attacks Law & Legal Definition. Retrieved November 19, 2014, http://definitions.uslegal.com/c/cyber-attacks/
[19] "Distribued Security as Cyber Strategy: Outling a Comprehensive Approach for Canada in Cyberspace." CDFAI. 14 Oct. 2014. <http://www.cdfai.org/PDF/Distributed%20S

As the potential for cyber attacks increases, Deibert advances the point that it will affect the entirety of all Canadian lives. Each day, Canadians use the Internet to access information from home, work, public places. The Internet is used to work on personal finances (online banking), data transfer of confidential information (including credit card info), which puts a lot of a Canadians life on the line in the event of an attack against Canada's most protected Critical National Infrastructure. A bold example is brought up in Deibert's research in regards to storing our personal and confidential information on " clouds". Cyber attacks by both state and non-state actors have the capability of accessing somebody's "cloud" and going completely undetected. The attack plainly happens unexpected, at any given time and can change somebody's life for the absolute worse, including the potential of death.

Deibert acknowledges what is very important " creating a foreign policy for cyberspace". The truth behind this recommendation for the Canadian government is as accurate as the determinants (measures and programs) that the Federal government seeks to understand when reducing or blocking the threat of cyber attacks. Indeed, if Canada does not create a foreign policy on cyberspace, it will no longer be a domestic threat, as the government has recently understood it, but factually a global threat; a threat where the countries such as India, Brazil, and China with the most users in the world will control the vulnerability of cyber security for Canada.

According to Avner Levin (Director) and Daria Ilkina (Research associate) from the Ted Rogers School of Management at Ryerson University (Privacy and Cyber Crime Institute), a multilateral approach needs to be taken from the Canadian government in

order to secure CNI from transnational threats. However, Levin and Ilkina suggest that doing so becomes risky as threats from Brazil, India, and China continue to increase. It becomes clear through this research that Canada is lacking in the ability and effort to become multilateral partners with major states (Australia, China, Finland, France, Germany, New Zealand, Norway, United Kingdom) and only creating an open dialog between the United States on combatting cyber attacks.

The bilateral effort between Canada and the United States is part of the " Beyond the Border" action plan.[20] The Canadian " Beyond the Border" action plan was created in 2011 as a way to enhance security measures between the USA and Canada. Further working together to form cooperation and work bilaterally on international cyber-security threats. Through the action plan, Canada seeks to be able to respond more effectively and increase response times to any national or international cyber attack. [21]

According to Scott Knight (Department Head of Electrical and Computer Engineering) at he Royal Military College of Canada, the current age of cyber attacks has gotten to the point where turning off a computer, disconnecting from the Internet is no longer a safe option. Knight identifies two types of adversaries; claiming there is 1). People who are trying to attack the general population, and 2). Groups or individuals who target Canada as a nation. Knight recognizes that if the first type of adversary is to carry out an attack, every single computer in Canada becomes vulnerable to an attack. This

[20] Levin, Avner , and Daria Ilkina. "Ted Rogers School of Management, Ryerson University." *Privacy and Cyber Crime Institute*. 17 Oct. 2014. <http://www.ryerson.ca/tedrogersschool/privacy/documents/Ryerson_International_Comparison_ofCyber_Crime_-March2013.pdf>.
[21] "Canada's Economic Action plan." *Government of Canada*. 17 Oct. 2014. <http://actionplan.gc.ca/en/page/bbg-tpf/beyond-border-action-plan-brief#sect2.4>.

provides an option for the adversary to carry out any amount of malicious attack including sabotaging financial information, or potentially identification theft. What is to be noticed about defense against these types of attacks is that there are multiple commercial applications that help stop these types of attacks. These include the use of firewalls, anti-virus software's, and multiple detection systems. What is of great concern, which Knight emphasizes, is the enormous risk that the effects of a cyber attack against Canada's CNI could have on its citizens. Knight recognizes these types of attacks as ones that would be carried out by organized crime groups, a military adversary, or a government backed adversary intelligence service (China, Nortel). The concern for these attacks against the nation; range from accessing critical information from the federal government, to the launching of military defense systems. Knight also understands that the risk that the Canadian forces face stands as immediate. Moreover, a potential policy recommendation is to expand the Canadian Forces cyber capabilities by strategizing a policy on cyber attacks.[22]

As established thus far, the Canadian government is lacking cyber security implementation to protect its CNI. The government of Canada refers to CNI as "Critical infrastructure 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. Critical infrastructure can be stand-alone or interconnected and interdependent within and across provinces, territories and national

[22] "Scott Knight: Preparing for cyber-war." *National Post Full Comment: Scott Knight Preparing for cyberwar Comments*. 17 Oct. 2014. <http://fullcomment.nationalpost.com/2013/02/08/scott-knight-preparing-for-cyber-war/>.

borders. Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects and significant harm to public confidence."[23]

Foreign policy on Cyber attacks has not been established, a military policy is absent, and multi-national cooperation by major powers has not yet been established. A most recent interview by Canadian networking company Phirelight (private IT security company) sat down with Michel Juneau-Katsuya (CSIS veteran) as well as Ray Boisvert (Ex-CSIS intelligence officer) collecting noteworthy expert perspectives. To begin, Katsuya reflects on the approach the public and private sector have both been sharing on the perspective of budgeting for security measures. Katsuya illustrated that both sectors continuously to view security as an expense, when they should be an understanding it as a "strategic investment." With this misunderstanding and skewed perception, the government can find itself in a vulnerable situation, acting after the problem has occurred. As explained, the attackers will always be in the strategic advantage, always two steps ahead, and always on to the next attack before the government can react. It comes down to the government under going a full risk - threat assessment. The allocation of funding would become potentially less of an issue for the federal government once it understands the vulnerable state, which it currently sits in and what potential catastrophes could erupt from a cyber attack.[24]

Katsuya and Boisvert share a common perspective on the lack of potential funding that is being allocated in annual budgets to help secure Canada against cyber

[23] Critical Infrastructure. (2014, March 20).http://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-eng.aspx

[24] "PhireLight." *PhireLight.com*. Communications Coordinator, 22 Sept. 2014.18 Oct. 2014. <http://www.phirelight.com/corporate-risk-canada-bugging-boardroom/#comment-888>.

attacks. There is clearly a lack of urgency being placed on a threat that is more than substantial. As a cohort, the Canadian government must assess risk from threat and establish synergy between all sectors of the federal government to create a force capable of countering cyber attacks. Recommendations set forth by Katsuya and Boisvert contain great validity in regards to creating a pro-active approach rather than a post crisis defense system. Simply, the financial costs for example could be exorbitant, as well as the threat Canada faces if a nation obtains classified Federal Government documents. As the Canadian government is consistently looking to secure its cyber security, evidently, they shall take measures so there is not a repeat of the act by China in 2011.

Martin Rudner, has examined the threats towards Critical National infrastructure (CNI), including the cyber threats posed towards CSIS infrastructure and has outlined that these systems are considerably vulnerable, particularly due to the "high inherent value." To begin, Rudner recognizes that tracing who the criminal is may be an impossible task. It cannot be understood easily who is setting out a cyber attack, simply based on complexity of the attack, and understanding motivations. These two elements of complexity and motivations make it an overly difficult task to point fingers towards if the attack has been carried out by a state, an individual, or by a malicious group.

What also must be noted in the rise of such terrorist groups such as ISIS must be the attention of cyber threats by international terrorist groups. Rudner defines cyber terrorism as the use of Web-based information technology to conduct enabling, disruptive, or destructive operations in the digital domain so as to create and exploit fear

through violence or the threat of violence at the behest of a militant belief system. (Rudner, 2013).

These forms of attack also enable the ability for terrorist groups to use their attack as a means of recruitment, financing and planning, and carrying out attacks against states or non-state actors. In 2012, Canada's counter-terrorism strategy identified the threats by Sunni Islamist extremism as the " leading threat to the national security of Canada. Moreover, the terrorist group listed its targets towards government property, global corporations, passenger flights, airports, banks, oil and natural gas towards USA and Canada. As a part of an "Economic Jihad," threats towards oil and natural gas of Canada was an attempt to weaken the economy. However, in 2012 another group of hacktivists called "Anonymous" (known for sabotaging WikiLeaks and PayPal) expressed an open interested in disrupting the Albertan oil as well as the Keystone XL pipeline.[25] Evidently, the threats Rudner focuses on explains a variety, an unconstrained array of possibilities from a multitude of groups and individuals for a variety of purposes. Complexity and motivations are on two spectrums that are infinite, unlike many other threats that face Canada (National Security Agenda).

Martin Rudner, in his article entitled, "Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge", Rudner follows the approach that Canada is essentially behind the times in its ability to take preventative measures against cyber attacks. Rudner states that the Canadian government is runner up to the USA in its approach; further falling short on its programs and resources and ability to carry out

[25] Rudner, Martin. "Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge." Taylor & Francis Online. 20 May 2013.18 Nov. 2014. www.tandfonline.com/doi/full/10.1080/08850607.2013.780552

proper cyber security training. The USA has the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) to deliver cyber security training from the department of Homeland Security. The ICS-CERT training is a state government effort that is responsible for training of the protection on all US CNI which includes energy, financial institutions, communications, emergency services, transportation, water systems, healthcare and public health, as well as defense bases.[26]

The literature suggests the Canadian government may not be responding to the threat of cyber attacks to the best of its ability. Throughout my findings in my literature review, even Canada's neighboring state and major allies present themselves as " leaps and bounds" ahead of Canada's current methods. As mentioned in the literature review, the USA has the ICS-CERT. Canada's approach to the ICS-CERT is the Canadian Cyber Incident Response Centre (CCIRC).

The CCIRC is a Federal government mission to be prepared, mitigate cyber threat risk and respond accordingly to cyber threats. The CCIRC mandate outlines its efforts by creating information shares between multi-level of governments, and in between the public and private sector. The CCIRC also performs CNI forensics and malware analysis using Government expertise. Moreover, the CCIRC aims to provide security on services in both public and private sectors cyber systems. The CCIRC works by creating

[26] Canada must ramp up cyber security in wake of alleged China-led attacks, experts say. (2013, February 19). http://privacy-assured.com/canada-must-ramp-up-cyber-security-in-wake-of-alleged-china-led-attacks-experts-say/

systematic information share between its provinces and territories and private sector organizations and a few international partners.[27]

Scholars and professionals, their perspectives and professional knowledge conclude of course that a greater focus needs to be placed on cyber security in Canada. As it comes to academics and professionals in the field; the current focus is being viewed as reactive and not proactive. This data helps build the case for the Federal government to restructure its national security agenda and perhaps allocate greater funding, create a military sector responsible for cyber security, engage in transnational efforts (larger than with the USA) and undergo a full risk-threat analysis.

The policy recommendations put forward in this research align with proposals other professionals have made in the field. These include creating an international framework and partnering with other countries including USA, Australia, France, Germany, UK, the creation of a CERT, synergizing government efforts domestically and with the USA (increasing efficiency of "Beyond The Border"). Further, based on the findings put forward; a gap in the Federal government expenditures should be filled to create a better understanding of the current 2014-2015 policies and strategies, and as to why cyber security is their number two priority. In addition, I seek to explore the scholarly understanding of how other countries such as China & USA are handling their defense strategies on cyber attacks and build a developmental case to address more opportunities to increase Canada's cyber security strategy and response to transnational cyber attacks.

[27] Canadian Cyber Incident Response Centre (CCIRC). (2014, December 12). http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-eng.aspx

7. Methodology

For the purpose of this research, all information will be gathered from publications, published journals, and expertise by state, and non-state actors through secondary research. The Canadian Federal Government has been selected for the purpose of this research, as a large focus by Canadian and international experts explore the heightened risk of cyber attacks towards Canada by state actors due to a lack of significance allotted towards countering cyber attacks and policies and objectives on Canada's National Security Agenda, as well as Canada's Cyber Attacks Strategy. A focus of data collection is to be on Canadian experts and academics in the field of cyber security and cyber attacks. The data collected for this project is qualitative. Moreover, the data that will be collected looks at reinforcing the policies and strategies that will be formed and drafted from this research. Concentrating on individualistic views from multiple professionals as well as states that have already advanced their policies and strategies on cyber security is utilized as a means to further recommendations for the government of Canada, as well as to create urgency. The scholars and experts in the field of cyber attacks and cyber security have approached the problem in an urgent manner; focusing on the direct need by the government to assemble a proper transnational approach as well as the right domestic efforts. There is no limitation on the understanding for the Canadian government to realign its national security agenda from the perspectives of those that are used for data collection in this specific study.

The data collected will be used in efforts in the creation and drafting of new recommendations for responding to the threat of cyber attacks on a comprehensive

Canadian policy on cyber security. Reflecting on the approach experts and academics have used on this issue is important to understand. There is a lot of focus from experts (governmental) on the issues the federal government is having a difficult time solving. Most of these addresses are based on personal perspectives created by an understanding from working with governmental bodies, including; the DND and CSIS. It is very important to utilize the perspective of these experts in favor of their primary knowledge and expertise in this field. In addition, the qualitative data on this matter is vast from both Canada and the international community. Recommendations have already been put forward from other commonwealth countries as well as experts from the United States. The recommendations that have been put forth will also provide as evidence and support for the purpose and objectives set out in this research. Adapting a historical and integrative approach to creating a strong policy recommendation best suits the purpose of this research as it explores two imperative points of interest that need reflection by the Canadian government. The first point is that historically, the threat of cyber attacks and its related threats against cyber security has increased and continues to increase at an exponential rate. The second is focusing on the collective evidence that scholars and experts have put forward on this threat.

The scholars and experts in this field have similarly focused on the same approach. The approach develops very significant information that would be necessary for the Canadian government to utilize during a threat-risk analysis. Furthermore, in regards to a threat-risk analysis, the collection of declassified documentation from the Canadian Government will provide transparency on how the Canadian Federal

Government has assessed the threats and risks created by not meeting the defense demands necessary by the Federal government and other levels of government to combat cyber attacks. Drawing on historical and pushing expert data continues to build strong cases for experts in the field of cyber security. The literature provides guidance as to where the opportunity for development is for the Canadian government. Further in the analysis, a concrete understanding of the exploration is disclosed which will push the agenda for the Canadian government. Moreover, the necessary information that needs to be gathered throughout this research must be done to from a qualitative approach seeking out the most intellectual information on these concerns. Data collection has been prepared through an un-biased approach, assuming no one scholar or expert holds the correct information to further the prioritization of a Canadian cyber security. To reach a conclusion, the contributions put forward by scholars and experts in this field followed a qualitative approach that fits the criteria necessary to create comprehensive strategies and recommendations.

The scholars and practitioners, experts and academics who have focused their research and practice on cyber attacks and cyber security have addressed the problem utilizing case studies and a historical data collection approach. The approach on historical case selection works on addressing the rise and merging development of the threat on a domestic level and on an international level. Moreover, this approach commonly used, seeks to develop an aligned perspective with my own on the severity of the threat and the need to develop more strict domestic and international policy agreements. These methods aim to provide evidence for developing Canada's Cyber attacks Strategy through pressing

new policy recommendations and exposing the deficiencies of the current strategies Canada has made in its current Cyber Warfare Strategy, as well as on its national security agenda. Both, the national security strategy and the cyber attacks strategy are of utmost importance in this research as the policies and recommendations that I will seek to develop will focus primarily on both.

These methods seem the most suitable for the purpose of this research as I, just as other experts have done, seek to create urgency and a new importance and severity on the issue of cyber attacks. Furthermore, just as I seek to do; the recent research and development in this field of expertise continues to use case analysis and grounded theory research to create advocacy for the adaptations that are thought to be needed.

The use of case analysis has presented itself as the best form of evidence collection as it allows researchers to understand clearly what exactly has happened, in addition to what is currently happening, and what may happen in the future. My case analysis is not specific into one case, rather an exploration of a number of attacks, particularly those attacks from China towards Canada that are assessed as to what happened during the attack/s and how Canada either responded or tried to prevent them from occurring.

By using multiple case analyses, I am able to consume a variety of information and historical data from multiple states which can lead to a greater understanding on Canada's position while facing the threat of cyber attacks. By understanding Canada’s position under going the threat of cyber attacks, this creates the opportunity to construct new strategies that can be implemented. Utilizing methods and practices used by other

states that face similar threats of cyber attacks can contribute to the formation of the strategies discussed in this research.

8. Case Selection

Focusing on scholars and experts from Canada who have current and past experience in the Canadian government and private sectors was chosen to help gain the closest relevant information necessary to put policy recommendations forward. The Methods spoken from CSIS Expert Boisvert and Katsuya mentioned previously should be assessed as strategically important to consider. In particular, former CSIS experts have provided a clear understanding on the pitfalls of the importance that the Canadian government has placed on cyber security. Very clear implementation strategies have been outlined and could be advantageous to explore these further. By exploring studies and implemented programs from the Munk Institute, a vivid recognition of the severity of cyber attacks presents itself urgently. Further, the scholars at Ryerson have taken this qualitative approach using similar data. The data selection has been taken under the approach to understand and utilize multiple approaches to the issue of prioritizing cyber security in Canada in order to create a comprehensive strategy. The cases selected for this research by experts and analysts prove to be most efficient in developing a sound proposal for the Federal government.

The cases in the selection also develop across a spectrum of recommendations and policy objectives that best suit the explanation of prioritizing cyber security as Canada's number one threat. The scholars and experts utilized in this research similarly have used

cases affecting Canada and strategies developed from academic institutes. Understanding the use of all domestic cases and data selection puts a scope of focus on the direct needs that are currently being addressed in the country as supposed to focusing on the developed programs other states (i.e. USA) have developed. Addressing the concern that the case and data selection has been filtered on a bias medium needs to be appreciated that, in fact bias has not been undertaken in the current research and only provides as most relevant to concluding with the policies and recommendations set out in this research in order to create comprehensive strategy recommendations.

9: Analysis of Data

Canada's assessment on undergoing attacks by state actors is increasingly high as reflected by the attacks that have been under taken since January 2011 when the Federal government underwent an attack from hackers using IP addresses from China. The scale of the damage created recognition to all levels of government that attacks are unlimited in their size; as portrayed as the Chinese hackers (Chinese gov't reps) were able to affect CNI, the Treasury board, the federal finance department, DND technology and the Canadian armed forces.

Further, in February 2011, PM Harper said that the government is working towards creating a sophisticated response to combatting cyber attacks as well as " cyber attacks are a growing issue of importance".[28] In addition Canadian Treasury board

[28] Chinese hackers try to access Canadian gov't data. (2011, February 16). http://www.ctvnews.ca/chinese-hackers-try-to-access-canadian-gov-t-data-1.608389

minister Stockwell Day said that “cyber attacks weren't the most significant attack, but it was a significant one, significant that they were going after financial records".[29]

The Harper government (CSIS, DND) also understands that cyber attacks can go unnoticed and untraced for a lengthy period of time, sometimes all they are left with is the attacks after math. Moreover, the Harper government suggests that this form of attack is significant and surely not over. This is clearly indicated in the types of responses (Beyond the Border, CCSS) that they have implemented as well as their prioritization on the national security agenda. The utmost urgent threat presenting itself in the evaluation by the Harper government is that of “espionage”. Espionage in the understanding that state actors have the ability to expose Canadian government classified information, and more. Espionage as displayed with the Chinese attack in 2011 has the ability to target all major CNI and government agencies. Problematically, as cyber space expands, the scope of threats expands simultaneously. Moreover, the more reliance the government places on cyberspace and its CNI, the more susceptible the government will become. Similarly, the higher a rock climber will climb, the more they will rely on their belayer, and the higher a distance they will fall when their belayer fails to keep the climber safe.

Vic Toews (Minister of Public Safety) outlined the Canada Cyber Security Strategy as a plan for meeting the current threat. The Strategy is built around utilizing all

[29] Canada says cyber-attack serious, won't harm budget. (2011, February 17). http://ca.reuters.com/article/topNews/idCATRE71G0RG20110217

levels of the Canadian government, as well as the government agencies and law enforcement bodies.[30]

As a result of my exploration, it is agreed upon that the Canadian government is making efforts towards responding to the threats of cyber attacks. Throughout my collected research I have assessed the current situation the Federal government faces is seemingly imminent and growing at an exponential rate. With the increasing rate of cyber attacks, it is transparent that the policy makers are missing the pro-active approaches. It is understandable that the government of Canada has been a re-active government when it comes to traditional means of warfare; protecting its land, borders, and sea when threatened, being the second to fire. Thus, it must me made clear; unlike if a nation were to fire a weapon from sea towards a naval port in Halifax, it would not paralyze the entire nation of Canadas operations. Moreover, a cyber attack does have the capability to definitely create a type of potential catastrophe, as witnessed with Stuxnet (2010). It is discussed through researchers, experts and all levels through the Canadian government that the response to cyber attacks needs to be improved. Policy recommendations have been created and suggested by many, and few and far are being agreed upon as being actually implemented or being successful. With that being said, I believe that Beyond the Border Strategy between Canada and the USA is a stepping-stone into bilateral efforts that defuse cyber attacks before they are actually able to present themselves as "risky" or "present". The USA and Canada have clearly been working together on multiple military

[30] Canada's Cyber Security Strategy. (2014, March 19) http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx

grade operations for decades, battling threats at sea, overseas, in the skies, at their borders, and now portraying that cyberspace is their "ground" to protect together. Canada and the USA both have exceptional intelligence agencies (CIA, CSIS) that could be making significant differences in the way not only Canada responds to cyber attacks, but also the US response. The Beyond the Border Strategy as explained and understood, essentially works until it needs to do work. By this, I have analyzed the Beyond the Border strategy as a very limited re-active approach. Dialogue is important between powerful nations, just as it is important between non-powerful nations. Moreover, when such a large nation is under such distress from these forms of attacks, dialogue does not create justice as a sufficient response to managing potential catastrophes on CNI. The United States and Canada have had a strong military alliance for decades, supporting each others front line, moving troops overseas to war torn countries, providing aid states in need, aligning strategies with the United Nations, and engaging in massive cross border trade of goods and services. If "Beyond the Border" would increase its mandates to include intelligence sharing, infrastructure and financing, not only would Canada be in a stronger responsive and pro-active position to cyber attacks, the USA would also be benefiting.

9.1 View of Security Measures

In March 2008, Suleyman Anil (NATO CNI protection) said that the level of security measures implemented for attacks such as missile defense should be just as high as those for cyber security. Anil has acknowledged the threat of cyber attacks as a serious problem for all of its NATO members and that the threat of attacks is not going away any time soon. In fact, Anil has looked at the situation as potentially grave, to the degree that it presents itself the potential to cause the same damage as a missile attack or an attack against a nations energy system. To add, David Davis (former Foreign Officer of the minister and shadow home secretary for NATO) agrees with Anil on the truth that cyber attacks will grow and become harder to prevent as technology continues to develop.[31]

Handling cyber attacks is increasingly difficult. Attacks of its nature are being treated as seriously as a missile attack against a nation; further now they may be looked as being handled through the one of the same methods. Under the UN charter Article 5 " A Member of the United Nations against which preventive or enforcement action has been taken by the Security Council may be suspended from the exercise of the rights and privileges of membership by the General Assembly upon the recommendation of the Security Council. The exercise of these rights and privileges may be restored by the Security Council."[32]

---

[31] Johnson, B. (2008, March 6). Nato says cyber warfare poses as great a threat as a missile attack. http://www.theguardian.com/technology/2008/mar/06/hitechcrime.uksecurity

[32] Charter, United Nations, Chapter II: Membership. http://www.un.org/en/documents/charter/chapter2.shtml

In March 2015, NATO SEC GEN. Jens Stolenberg proposed to the alliance annual planning summit that perhaps these attacks need to be handled under Article 5. Under his assessment, cyber attacks are linked to all forms of conflicts, or vice versa that all attacks or conflicts from state to state have a form of cyber connected to their agenda. By this, Stolenberg has indicated a form of "hybrid war" which includes the use of conventional weapons and now as to what should be considered as "conventional" are the uses of cyber space to carry out an attack.[33] Based on these two statements, creating deterrence methods is what needs to be implemented similarly to the types of reprimands carried out by the UN to member states when they act against the charter through uses of early 21st century means of conventional warfare.

Senior Government Officials in Ottawa have began to fuel more financing into the threat that is most recently becoming one coming from the Chinese. In January 2015, officials from Ottawa said that they need to expand their Cyber Security Strategy past 2015 with an increase in spending. The level of security implemented in the previous five year plan and its success vis a vis the funding allocated previously, is a direct reflection as to why they have now decided to exceed a new $100 million dollar budget, as supposed to the 10.021 million in 2010. China struck Canada hard in 2011, and again in 2014 when they tried to access computers at the National Research Council. The Harper government understands that the threats and attacks are becoming more severe saying in

[33] McLeary, P. (2015, March 25). NATO Chief: Cyber Can Trigger Article 5. http://www.defensenews.com/story/defense/policy-budget/warfare/2015/03/25/nato-cyber-russia-exercises/70427930/

early 2015 “It was the most sophisticated thing we’ve seen”. [34] The Harper government is in a difficult position undoubtedly. To reflect on the Cold war, Russia and USA used deterrence to keep the upper hand and peace until the end. If Canada is to use this to approach of deterrence to prevent and create a resilient cyberspace against nations such as China; they may be making themselves more vulnerable. By showcasing Canada’s abilities, Canada limits its means of surprise defense and countries learn what Canada is capable of, therefore giving the adversary the competitive edge.[35] Security Measures must be taken through strategic alliance between the USA and Canada and funding/ intelligence support across the border be increased to create increased resilience. Unlike USA, UK, China, Russia, Israel, and France, Canada is behind on its sophistication on defense mechanisms from cyber attacks. Not only is China a state with superior cyber capabilities, but also it is listed as the top intruder into government CNI in Canada and USA. China has developed something known as " Advanced Persistent Threats" (APT) that are threats that continuously grow in complexity and presence. Thus, as Canada continues to try to create strategy, with NATO, and even with the USA, China's attacks are rapidly changing in complexity. [36] Creating a resilient cyber strategy is a learning

[34] Chase, S. (2015, January 14). To guard government computers from hacking, Ottawa to spend $100-million on security. http://www.theglobeandmail.com/news/politics/guarding-government-computers-may-cost-ottawa-more-than-100-million/article22441439/

[35] CyberSecurity Challenges for Canada and the USA. (2015, March). http://www.fraserinstitute.org/uploadedFiles/fraser-ca/Content/research-news/research/publications/cybersecurity-challenges-for-canada-and-the-united-states.pdf

[36] CyberSecurity Risks and Costs of North American Cyber Security. (2015, March). http://www.fraserinstitute.org/uploadedFiles/fraser-ca/Content/research-news/research/publications/cybersecurity-challenges-for-canada-and-the-united-states.pdf

process, a game of cat and mouse. As Canada continues to face thousands of new threats every year, being positioned to take only reactive measures seems to be hard to avoid.

9.2 Decoding the Past

Canada continues to face threats from state sponsored cyber attacks. In 2006, Canada fell victim to "Operation Shady Rat" (OSR), which was an attack backed by the Chinese government that worked on stealing government data. Canada was not the only country hit by OSR, rather USA, South Korea, Taiwan, Vietnam were also amongst countries that were targets and hit. Operation Shady Rat offers a clear example as to the sophistication of the attack. RAT is actually an abbreviation for a remote access tool, which means that malicious software was placed into computers to carry out espionage. OSR Started in 2006 and continued into the end of 2011. What made OSR such a success targeting Canada was that it was an APT (Advanced Persistent threat), which utilized techniques, and hackivist strategies that the Canadian government could not keep up with.[37] The cyber attacks are lining themselves up for attack against Canada, coming in from every which angle. The attacks happen spontaneously, rapidly and in a unique fashion, most times unrelated to a previous attack. Analyzing the past is not an overly tricky task to undergo. Rather, a simple understanding of how vulnerability allows an attacker (state) to succeed in their attack. If we use a school yard analogy; a child being bullied will stop being bullied and feel safe going to school in one of the following

[37] Masters, G. (2011, August 3). Operation Shady Rat reveals vulnerability to cyber intrusion. http://www.scmagazine.com/operation-shady-rat-reveals-vulnerability-to-cyber-intrusion/article/208997/

situations. First, the bully gets suspended from school; second, the child and his/her friends fight back together; and third, the child learns new coping mechanisms to prevent the bully from bullying him or her. This may seem of a childish example but a lot can be learned and from this. For example, the first situation of resolving the bullying case institutes action from the United Nations. This action involves suspension from the P-5 for nations that have threatened Canada in the past (i.e. China). The second situation institutes international cooperation. Looking back on the international cooperation that was in place particularly between 2010-2015, limitations under Article 5 were present and no penalty was instituted; further only there are only discussions to current day under Article 5 and what penalization to members should be implemented. Situation 3 institutes Canada building new cyber infrastructure built off grass roots governance approach utilizing all levels of government to construct defensive systems. Further, the third situation involves the utilization of reliance of more of the private sector institutions and corporations. There has been an increase on all of these efforts without a doubt, moreover P-5 membership needs to be taken seriously as the risk of losing a position in the P-5 if caught in a cyber stack presents itself as a major loss for any state, including China and Russia.

9.4 State vs State

Canada is not the only country that undergoes a numerous amount of cyber attacks. The United States government and the Department of Homeland Security (DHS) have special enforcement agencies integrate into the DHS that have specialized divisions

that are focused on fighting cyber crime. There are two major sectors of the DHS that are used to identity and locate where the cyber attacks are coming from and to what scope the attack falls under (espionage, sabotage). The U.S. Secret Service has been a major contributor to the USA combatting cyber attacks. Due to its intelligence sector the DHS has defended the USA from over six hundred million in losses from banks and retail business in the USA. In addition, DHS holds the U.S. Immigration and Customs Enforcement (ICE), Cyber Crime Center (CCC) and the Homeland Security Investigations (HSI), which work together to build technical service and combat international cyber crime as well as cross border crime. ICE has been also known for its training and supports all law enforcement agencies in the USA as well as international agencies.[38] Moreover when it comes to protecting US CNI, DHS provides a 24/7-response team and communications through all public and private sectors, intelligence and law enforcement to mitigate cyber threats and risk through the National Cyber security and Communications Integration Center (NCCIC). In addition the DHS has a National infrastructure coordinating center and a Critical Infrastructure Cyber Community Voluntary Program which are both aimed to increase CNI resilience and awareness and support businesses and those who own CNI to manage their cyber security in a more effective way.[39] In relation to Canada, just the DHS seems to have more defense response mechanisms than the Federal Government of Canada. Similarly, Canada does have government agencies responsible with specialized intelligence units designed

[38] Homeland Security. (2015, April 15). http://www.dhs.gov/topic/combating-cyber-crime

[39] Homeland Security. (2015, April 17). http://www.dhs.gov/topic/protecting-critical-infrastructure

to respond to the threat of cyber attacks; however the sophistication on the US response leaves their state in a stronger and more resilient position against threats from nations like China.

10. Recommendations for the government of Canada on proceeding with creating a resilient future defending CNI against cyber attacks from state actors

The recommendations set out in this section aim to provide policy actions to be taken by the Canadian government as well as to provide what further investigations and research should be carried out in the threat of cyber attacks. As Canada continues to face the ever-growing threat of cyber attacks by state actors, creating a resilient framework on protecting its CNI is imperative for future defense success. Establishing a framework on protecting Canada's CNI against cyber attacks by state actors must be done in a particular manner in that growth and development will not be limited by mandates, by-laws, international and domestic law, as well as limited financial resources, logistical resources that include cyber capability, governance and international cooperation.

To begin with, governance is a crucial pillar for success in protecting CNI. By creating multi-level governance through municipal, regional, provincial and federal governing bodies, Canada could see itself having less obstructions from provinces and territories including (Quebec, Northwest territories) on allowing certain bills to be authorized. For this to be successful, a transparent comprehension on the severity and imminent threat of cyber security must be created to help prioritize why a governing body would be interested in allocating any aid in its nations defense against cyber attacks. By creating a solid understanding of the threat through a full threat-risk analysis, governments on all levels should be able to become a single governing body working in cooperation to protect their own interests, as well as the Canada’s best interests. Following good governance on the domestic front comes global governance and

international cooperation. Canada has currently positioned itself strategically and beneficially aligned with US interests as well as creating strong partnerships with the EU. International cooperation must be done so that collaborative benefits are given to each nation Canada cooperates with. Moreover, I am referring to creating a justification for as to why nations would want to cooperate on protecting Canada's CNI, rather than just focus on their own nations CNI. The resolution for international cooperation on protecting global CNI (Canada's and its cooperative nation partners) is that Canada offers a vast amount of intelligence through CSIS, RCMP, and DND which countries (specifically USA) can continuously benefit from have access to. As mentioned previously, Canada and the USA have a strong relationship dating far back before cyber security and cyber threats was of any concern. The current relationship between Canada and USA is more of an open dialog relationship since the signing of the "Beyond The Border Action Plan" in 2011. Both the Canadian and US government have successfully worked together on international issues such as going into Iraq in 2003 and fighting terrorism including current threat "ISIS". On a closer domestic front for Canada and USA, NAFTA is a great example of cooperation where all governing bodies involved found cause and reason for the signing of NAFTA. Protecting Canada's CNI and US CNI should be approached in the same manner in which both parties seek to maximize its nations resources to benefit each other's nation. Maximizing resources between Canada and the USA, as well as Canada and other nations include having open dialog about intelligence gathering, creating support either via cyber capability, militarily, and/or financially.

As international cooperation as a major pillar for success in my recommendations, international law must always be considered, and upheld to the highest level. As I have mentioned, cyber attacks can be done by both state and non-state actors through the use of espionage and/or sabotage to seek gain. Canada must uphold its international integrity and commit to upholding international law and not creating risk by undergoing espionage or sabotage on another state (I.E China) as it seeks to improve its resilience. International law does create limitations for Canada as to its outreach approaches on protecting its CNI from state cyber attacks, however international law also creates deterrence from the attacks becoming more harmful than current day attacks. By seeking to further the international relationships already established, not only can all nations benefit, but also perhaps acts of espionage will be decreased as nations form a unity on cyber security and protecting all of its CNI.

Moreover, financial allocation and government spending on cyber security and establishing resilience on Canada's CNI is the third major pillar that needs further exploration and implementation. With over 205 million dollars allocated for countering domestic crime in Canada and only 5% of a budget that size being allocated for cyber security requires a new threat-risk analysis by all levels of the Canadian government. If the attacks by state actors from the millennium until current day are not enough evidence to consider that 10.021 million was not enough financial support, perhaps revisiting the financial damage some of the largest attacks in the decade have caused will show that in fact, Canada not only spent just 10.021 million on cyber security, but lost billions of dollars, particularly from attacks against Nortel, and the Chinese cyber attacks on the

Federal government in 2011. Risking espionage and sabotage to a budget as small as the budget between 2010-2015 is that risky of a formula 1 race car racing with only three of its four wheels and perhaps only half a tank of gas and assuming a WIN for that car during a race. Doing what a government is considered "good enough" or "hopeful" does not create resilience. Resilience is created by creating global strategies and allocating funding that leaves Canada in the "green" regardless of the level of attack carried out by a state actor. If a state is to attack Canada and that attack launders 22 million CAD from the Department of Treasury (DOT), Canada will be upheld by its much larger budget that in fact will have created opportunities through comprehensive safeguards that could actually return that money back to the DOT vis-à-vis international cooperation and intelligence sharing. Concluding on these crucial recommendations, the Federal government of Canada has substantial duties to uphold if creating resilience is of even the littlest priority. The threat of state-to-state cyber attacks will not be going away any time soon and creating the same importance and strategy theory used to protect Canada's air, sea, and land must be used to protect the cyber world that Canada depends on so heavily. If the Federal government cannot become flexible, the government limits itself. Adapting to change and ensuring flexibility on its national security agenda is of utmost importance.

11. Conclusion

Throughout my research I sought out to create an understanding of the current measures the Canadian government has created for itself in the past as well as to explore the current security state on CNI in Canada from being attacked by state actors. My research was shaped around the question of how Canada has positioned itself on the defense and response to cyber attacks by state actors against its CNI. Concluding on my studies, I have gathered evidence to create acknowledgement and urgency on the position of Canada and its defense and response to the previously mentioned. By creating acknowledgement and urgency on current state practice by Canada and how it has positioned itself in line with states that have threatened Canada in the past (such as China), Canada can create advancement to its current means to defend. Moreover, by understanding what Canada has done and where other states have been successful carrying out cyber attacks to Canada's CNI, it becomes evident that the past means of defense have positioned Canada in a vulnerable state in need of a policy corrective. The research carried out in this project was based on creating policy recommendations for the Canadian government on continuing to defend from this form of attack by state actors.

As previously mentioned in the recommendations above (section 10); the three major pillars, or recommendations, include: incorporating multi-level governance, improving and developing international cooperation, and increasing financial allocation. These three pillars are not conclusive on means of exactly how much spending needs to be incorporated, rather these three recommendations are developed to push on government flexibility on its security agenda. Throughout a reflection on the history of

cyber attacks by state actors directly and indirectly on CNI, all attack types mentioned have been sporadic, independent, and increasingly complex and harmful-- either financially or operationally to the Canadian government and its citizens. This research has highlighted the ways in which the Canadian government on various levels (bottom-to-top) is currently unprepared and vulnerable, lacking foresight of cyber attacks on CNI, and seemingly unconcerned with the extent of this threat. These inferences are based on the measures Canada has taken out over the past decade and how they failed to craft the resilience they were capable of designing, evidenced above by way of multiple cases of previous attacks against Canada.

My first example is based off of the Chinese (2000) attack to the Canada Treasury board, Defence Research and Development Canada, the Federal finance department, and the Department of National Defence. Despite the time that has elapsed since this specific attack, Canada has experienced similar cyber-assaults including the year in which Nortel (2012) was attacked by Chinese state-backed actors. Moreover, I maintain that the 2000 attack clearly demonstrates vulnerability, unpreparedness, weakness, misrepresentation of security priorities, and a lack of resilient defense systems in place.

Overall, this project demonstrates that the mechanisms of defense which allowed for the cyber-attacks in the previous decade are a strong reflection of neglect of the three pillars of recommendations outlined. Additionally, this research exemplifies the consensus upon researchers and academic professionals on the alarmingly unsecured platform in which Canada's CNI relies on for security. The consensus that was shown in this project was not of surprise as the attacks mentioned were public information. By this,

I am referring to public access and awareness on the ability of every Canadian and its nationals to obtain information on the attacks that caused harm (either through espionage or sabotage). The consensus was evident as it has been seemingly clear that something had gone wrong in protecting Canada's CNI, and that not enough security measures have been implemented. Finally, this work infers that Canada will continue to face the threat of cyber-attacks by state actors either directly or indirectly to its CNI, a threat which remains to be accounted for by policy makers in the Federal Government (client). As such, there exists a public sector prerogative to adapt, continue to be informed, focus on preventative measures and work towards creating a national security agenda that reflects the utmost detrimental threats to the security of Canada and its nationals.

APPENDIX A

Terminology

Cyber Security - The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.

Cyber Space - The interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Cyber attacks - A massively coordinated digital assault on a government by another, or by large groups of citizens. It is the action by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption. The term cyber attacks may also be used to describe attacks between corporations, from terrorist organizations, or simply attacks by individuals called hackers, who are perceived as being warlike in their intent.

Espionage - Espionage is used to disable computers, networks, software, steal or acquire data for military, financial or political gain.[40]

Sabotage - the disruption of a normal operation.

Threat -A circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society.

Threat Analysis - The detailed evaluation of the characteristics of individual threats.

Virus - A computer program that can replicate itself, infect a computer without permission or knowledge of the user, and then spread or propagate to another computer.[41]

Critical National infrastructure - processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of

[40] "What is Cyberattacks (Cyber War)? - Definition from Techopedia." 27 Sept. 2014. <http://www.techopedia.com/definition/1360

[41] "Cyber Glossary | National Initiative for Cybersecurity Careers and Studies (NICCS)." 22 Oct. 2014. http://niccs.us-cert.gov/glossary#letter_c>.

Canadians and the effective functioning of government. Critical infrastructure can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders. Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects and significant harm to public confidence."[42]

[42] Critical Infrastructure. (2014, March 20).http://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-eng.aspx

Works Cited

"2012 Canada Digital Future in Focus." *comScore, Inc*. N.p., n.d. Web. 12 Oct. 2014. <http://www.comscore.com/Insights/Presentations-and-Whitepapers/2012/2012-Canada-Digital-Future-in-Focus>.

"Action Plan 2010-2015 for Canada's Cyber Security Strategy." *Action Plan 2010-2015 for Canada's Cyber Security Strategy*. N.p., 4 Mar. 2014. Web. 10 Oct. 2014. <http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/index-eng.aspx>.

"Canada's Economic Action plan." *Government of Canada*. N.p., n.d. Web. 17 Oct. 2014. <http://actionplan.gc.ca/en/page/bbg-tpf/beyond-border-action-plan-brief#sect2.4>.

"Canada's weakling Web defences." *The Globe and Mail*. N.p., 18 May 2011. Web. 12 Oct. 2014. <http://www.theglobeandmail.com/globe-debate/canadas-weakling-web-defences/article580145/>.

"Cyber Glossary | National Initiative for Cybersecurity Careers and Studies (NICCS)." *Cyber Glossary | National Initiative for Cybersecurity Careers and Studies (NICCS)*. N.p., n.d. Web. 22 Oct. 2014. <http://niccs.us-cert.gov/glossary#letter_c>.

"Distribued Security as Cyber Strategy: Outling a Comprehensive Approach for Canada in Cyberspace." *CDFAI*. N.p., n.d. Web. 14 Oct. 2014. <http://www.cdfai.org/PDF/Distributed%20Security%20as%20Cyber%20Strategy.pdf>.

Knight, Scott. "Scott Knight: Preparing for cyber-war." *National Post Full Comment Scott Knight Preparing forcyberwar Comments*. N.p., n.d. Web. 17 Oct. 2014. <http://fullcomment.nationalpost.com/2013/02/08/scott-knight-preparing-for-cyber-war/>.

Levin, Avner , and Daria Ilkina. "ï¿¼Ted Rogers School of Management, Ryerson University." *Privacy and Cyber Crime Institute* . N.p., n.d. Web. 17 Oct. 2014. <http://www.ryerson.ca/tedrogersschool/privacy/documents/Ryerson_International_Comparison_ofCyber_Crime_-March2013.pdf>.

"Nortel hit by suspected Chinese cyberattacks for a decade." *CBCnews*. CBC/Radio Canada, 14 Feb. 2012. Web. 12 Oct. 2014. <http://www.cbc.ca/news/business/nortel-hit-by-suspected-chinese-cyberattacks-for-a-decade-1.1218329>.

"PhireLight." *PhireLight.com*. Communications Coordinator, 22 Sept. 2014. Web. 18 Oct. 2014. <http://www.phirelight.com/corporate-risk-canada-bugging-boardroom/#comment-888>.

"Report on Plans and Priorities 2013-2014." *Public Safety Canada*. N.p., n.d. Web. 13 Oct. 2014. <http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rprt-plns-prrts-2013-14/index-eng.aspx#a13>.

"Report on Plans and Priorities 2014-15." *Report on Plans and Priorities 2014-15*. N.p., n.d. Web. 13 Oct. 2014. <http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rprt-plns-prrts-2014-15/index-eng.aspx#s2113>.

"The Information Attacks Monitor Project Publishable Summary." *Information Attacks*

Monitor. N.p., n.d. Web. 12 Oct. 2014. <http://www.infowar-monitor.net/reports/IWM-Project%20Publishable%20Summary.pdf>.

Weston, Greg. "Foreign hackers attack Canadian government." *CBCnews*. CBC/Radio Canada, 17 Feb. 2011. Web. 12 Oct. 2014. <http://www.cbc.ca/news/politics/foreign-hackers-attack-canadian-government-1.982618>.