"The Cyberwarfare Era is upon us", "Preparing for cyber-war", "It's time to get serious about cyber security". These headlines from the National Post suggest that in the realm of cyberspace, there are new storm clouds on the horizon. Fred Kaplan argues that a new era of attack and retaliation using the internet is upon us and western government are largely unprepared; Scott Knight makes similar claims about the Canadian Forces abilities to launch offensive actions in the digital realm; Ashley Dawson suggests that Canada's cyber-defensive infrastructure is also woefully inadequate to meet the challenges the modern digital landscape. The common thread through all of these articles is the looming threat of cyberwarfare.

The use of the internet as a means to achieve strategic, military goals is an emerging challenge to governments around the world. Canada has been wrestling with this issue for a number of decades now, with some success, attempting to create coherent, effective policies and responses, but the work is far from complete. This paper will examine some of the variety of cyberwarfare attacks and their potential effects; an overview of Canada's attempts to navigate the cyber defense and cyberwarfare realm; as well as recommendations on how future policy discussions, both at the national level and the international level, should be framed and instated and what Canada's role in the digital security and warfare environment should be.

For the purposes of this discussion, the term cyberwarfare will be used interchangeably with cyberattacks as there is very little in the way of practical distinctions between the two. Largely the differnces of cyberwarfare hinges on using methods of cyberattack to achieve strategic goals on behalf of a state entity; however due to the nature of internet based technology, such as IP spoofing, botnets, and many others, verification of the primary culprit can be almost impossible. Adding to this, defensive measures, both structurally and from a policy perspective, taken against these attacks, are broadly similar, meaning that the efforts made to prevent the attacks of hackers also help to prevent those of aggressive state entities. Furthermore the term "attacker" will be used as shorthand to describe the perpetrator of any cyber-attack, be they individual, group, or state entities.

Background

In Joseph Nye's work *The Future of Power*, the concept of the internet is discussed as an emerging method of power projection, particularly by non-state entities. Nye cites the low cost of entry, that is, the cost to acquire the necessary materials, as the primary reason for this, compared

to the production of other military hardware, such as aircraft carriers, tanks, or planes.[1] Computers have become powerful and cheap, and the internet is ubiquitous to the point where almost any individual with sufficient knowledge can launch cyber-attacks. This is also an important factor in the difficulty in applying hard and fast labels to the interactions surrounding cyberwarfare/cyber-attacks; the field is incredible diffuse but simultaneously offers a power and anonymity almost entirely unrelated with size, whether we are discussing individuals, organizations, or states. Obviously those with greater access to resources will be able to achieve greater and more specific goals than those without, but it nonetheless remains a truth universally known that only equipped with the most basic of devices, access to the internet, and the proper motivations, cyber-attacks can be launched and any policy enacted must discuss this reality.

The methods of cyber-attacks all focus on gaining illicit access to a computer or network in order to achieve whatever goals the attacker may wish, ranging from simple monitoring to total control of a system. Some of the most common forms of cyber-attacks include viruses, which infect and destroy data and limit usability; Direct Access Attacks, where an attacker simply attempts to gain physical access to information stored on a computer; Trojan Horses, where seemingly innocuous programs place malware, which could take the form of keylogging software (password tracking), bot programs (which run programs in the background of computers and can be linked together to coordinate further attacks), surveillance programs, or delivering viruses, in the system as it is being loaded or installed; Denial of Service (DOS), which overloads a system with useless requests and bogs it down to the point of uselessness; there is also a further refinement of a DOS attack which is a Distributed Denial of Service (DDOS) attack, by coordinating multiple computers, either personally or utilizing a bot network, to extend the duration and severity of a DOS attack. An important method frequently used, and discussed in this paper, by attackers which can hamper investigations include the Internet Protocol spoofing, which disguise an attacker's location by using a different IP address.[2] While there are others which can and are used, the above methods represent some of the more common forms these attacks take and are also some of the more present in the public consciousness.

[1] Nye, Joseph S. *The Future of Power*. New York: PublicAffairs, 2011.
[2] Reveron, Derek S. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Washington, DC: Georgetown University Press, 2012. 7-9, 13, 40

Governmental awareness of the potential problems of organized cyberwarfare began in the early 1990s. In 1994 an Air Force laboratory in New York was subjected to over 150 attacks in a short period of time. Eventually a student in the United Kingdom and Israeli technician were discovered to be responsible, the student was charged and fined, the Israeli went free due to lack of applicable laws in that country.[3] This highlights an initial the lack of a coherent global strategy in dealing with cyber-attacks; while it is less present today gaps nonetheless still exist and attacks like this one and one of greater scale have motivated governments to craft policy which will allow them to protect themselves and prosecute the perpetrators of such assaults.

One of the biggest challenges to any reconciliation between the victim of a cyberwarfare attack and the perpetrator of same is that there is no current definition in international law about where such attacks fall, in terms of severity. Part of the reason for this is the gulf between the current noted effects of cyber-attacks and what they could *potentially* do. Thus far, cyberwarfare has, in practice, had very little effect beyond propaganda and mild disruption of service in modern conflicts. In 2008, during the Russo-Georgian war, several websites owned by both sides were defaced with messages supporting the attacker's side as well as others subjected to DDOS attacks, rendering them offline for the duration of the conflict. Several Georgian news sites covering the invasion were also attacked, preventing reliable information reaching the wider world.[4] While these attacks were undoubtedly effective at supporting an armed invasion, their scope was somewhat limited. They did not, or were unable to, gain access to and damage vital industries, such as a power grid or water system, there was no rampant chaos specifically because of a cyberwarfare assault or anything of that magnitude.

Yet this is what is feared by some in the military: an enemy nation gaining access to their countries most vulnerable systems and causing havoc. There are fears of nuclear reactors overloading, of an entire country being paralyzed, of a "digital Pearl Harbour", simply because we do not know what the upper limit of a full cyberwarfare attack could be.[5] The infection of Iranian nuclear enrichment facilities by the Stuxnet worm plays into these fears about a possible

[3] Blane, John V. *Cyberwarfare: Terror at a Click*. pg. 4
[4] Hollis, David. "Cyberwar Case Study: Georgia 2008." Small Wars Journal. January 6, 2011. Accessed March 24, 2016. http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008.
[5] Strand, Paul. "America's Cyber Defenses: A Digital Pearl Harbor?" *CBN News*, October 3, 2012. Accessed March 24, 2016. http://www.cbn.com/cbnnews/us/2011/december/americas-cyber-defenses-a-digital-pearl-harbor-/?mobile=false.

worst case scenario, but even that event provides very little solid and verifiable evidence. In this environment of limited hard knowledge, speculation abounds and creates a vast amount of uncertainty.

The worm was designed to affect systems with a particular hardware configuration, namely the ones used to aid in Iran's nuclear programme, which would sabotage and disable the centrifuges used in enriching uranium. The worm functioned by infecting the controlling computers, in this case Siemens model S7-417s, and intercepting normal command inputs. Interestingly, these controllers were not infected through the internet, but rather through an employee connecting a USB drive to a computer plugged into the local network. While giving the appearance of normalcy, the worm would gradually increase the speed of the centrifuges, until they failed.[6] This was only possible due to the unique nature of Iran's programme, which was a combination of outdated, yet still effective, technologies and several workarounds, which made it vulnerable to this specialized form of attack. Overall, however, the worm's general effectiveness is debatable: Stuxnet was only able to reduce the number of working centrifuges by about 10% for about a month, but it proved resilient and hard to remove.

The total destruction of Iran's enrichment equipment may not have been the original goal. Ralph Langner argues that Stuxnet largely had the capability to completely destroy all the centrifuges connected to the system but its creators chose rather to continue to hamper Iran's goals, drawing out the development of nuclear weapons longer than would have otherwise been the case.[7] He points to Pakistan's recovery after an earthquake in 1981, where many of that country's centrifuges were also damaged but were nonetheless able to create fissionable material, whereas Iran has not.[8] This analysis ignores other factors which limit Iran's abilities in nuclear weapon creation, but nonetheless highlights the possibilities for what cyberwarfare could achieve. This certainly is a nightmare scenario for many policy planners and government officials, particularly those countries with nuclear capabilities

One of the challenges of the Stuxnet worm, the Georgian attacks, and cyber-attacks in general are the inability to conclusively prove its origins. Many theories abound to this day as to which country created it, most of which center on a collaboration between Israel and the United

[6] Langner, Ralph. "To Kill a Centrifuge A Technical Analysis of What Stuxnet's Creators Tried to Achieve.". Accessed March 31, 2016. http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf. Pg. 6-8
[7] Langner, Ralph. pg.13-14
[8] Langner, Ralph. Pg. 15

States, those who have the most to benefit and the most resources to contribute respectively. Ultimately unless a state comes forward and admits to an attack, positive identification is all but impossible. The very languages in which programs are written in do not lend themselves to regional dialects or any other kind of national identifier, and the diffuse nature of the internet further obfuscates any point of origin as well as providing potential attackers with a high level of plausible deniability.

International Legislation

It is clear, due to the disparate nature of the internet, that there is a need for a two pronged policy formation, not only for individual nation to create policies and guidelines to help protect themselves from cyber-attacks, but also for there to be internationally adopted policy as well. In 2013 the NATO Cooperative Cyber Defense Centre of Excellence with assistance from a group of international cyber experts, published the Tallinn Manual, which sought to examine the current rules of conflict and test their applicability in cyberspace. The document is quite exhaustive, covering the minutiae of international law and providing a coherent basis for future legislation in this matter, it also acknowledges some of the challenges in combatting this area of modern warfare, particularly in determining the identity of one's attackers and in the threshold of conflict.

One important area which this manual covers is the establishment of sovereign rights over cyber infrastructure located within a nation's territory (Rule 1: Sovereignty). Furthermore, the Manual also provides recourse for nation should this sovereignty be violated (Rule 9: Countermeasures), as well as the responsibilities nations have towards their fellows in regards to maintaining security of over this infrastructure (Rule 5: Control of Cyber Infrastructure and Rule 6: Legal Responsibility of States).[9] By affirming these rights, the Tallinn Manual would provide states with a certain level of protection against the challenges of the modern world, and, at bare minimum, would certainly be better than the current system of having nothing in place

While admittedly the Tallinn Manual does not hold binding power over the United Nations, NATO, or any other nation, it could certainly provide the framework for a new UN resolution on the application of cyber technologies in warfare. An internationally binding covenant on cyber technology in war would allow for the respect of national sovereignty, whilst

[9] Schmitt, Michael. "Tallinn Manual." Issuu. Accessed April 3, 2016. https://issuu.com/nato_ccd_coe/docs/tallinnmanual/1?e=0/1803379 pg. 15, 36, 26-29

creating and maintaining regulations governing its use in an international context, a task for which the UN is ideally suited. Obviously such a resolution would not cover the criminal or terrorist uses of these attacks, however as the designers of the Tallinn Manual point out, laws governing conventional warfare do not cover these groups either, nor would it cover cyber-attacks used separately from armed conflict.[10] But clearly some form of legislation is needed to govern this clear and emergent form of combat, and regulate it before there is a major violation, rather than in response to it.

In the meantime, agreements between nations to limit their cyberwarfare targets could be a possibility. Dr. Amitai Etzioni suggest the extension of a Mutually Assured Restraint agreement, already in place between China and the United States over conventional missile build-up, into cyberspace, promising not to engage in attacks against each other in any form.[11] While this amounts to nothing more than a state-level "gentleman's agreement" on the use of cyberwarfare, if applied to other nations, it could be an important first step in opening dialogs for further discussion, awareness, and legislation on this matter.

Domestic Legislation

At the national level, policy is much better developed than internationally, that is to say that some policy has been developed and implemented; it is still quite patchwork and needs serious attention. Canada's efforts in the realm of cyber conflict have been one concerned mostly with defense, particularly of that infrastructure which could easily find itself under attack. In the early 1990's it was recognized by the government that much of Canada's infrastructure was vulnerable to cyber-attack and efforts began to be made to rectify this deficiency. Changes to this trend, however, have not been quickly adopted and it would take well over a decade before tangible changes could be realized.

In 2004 the Liberal Government, under Prime Minister Paul Martin, published *Securing an Open Society: Canada's National Security Policy*. This document laid out a plan to Canada intelligence gathering capabilities, develop an infrastructure protection plan, and create a national taskforce on cyber-security policy, amongst other provisions unconcerned with cyberspace. However as far as concrete action is concerned, the *National Security Policy* had

[10] Schmitt, Michael pg. 4
[11] Etzioni, Amitai. "MAR: A Model for US-China Relations." Accessed March 25, 2016. http://thediplomat.com/2013/09/mar-a-model-for-us-china-relations/.

limited immediate effect beyond increasing the available funding to Canada's security agencies, Canadian Securities and Intelligence Service (CSIS), the Communications Security Establishment Canada (CSEC), by 30 and 25 percent respectively.

One of the results of this plan is the *National Strategy for Critical Infrastructure*, created under the Stephen Harper Conservative Government in 2009, where information and protection is folding into the wider aegis of disaster protection and infrastructure resiliency. The specific sectors which would fall under this protection are: Energy and utilities, Information and communication technology, Finance, Health, Food, Water, Transportation, Safety, Government, and Manufacturing. The overall tone of the document suggests that the government's approach to Canadian information security as well as other forms of terrorism is to treat them similarly to natural disasters.

The *National Strategy* also highlights the protections granted to federal data sources through amendments to the *Access to Information Act*, but notes that there is a lack of equivalent protections at the provincial level.[12] There is also a heavy emphasis on the need for cooperation between the federal and provincial governments to enact better legislation on these matters. The *Access to Information Act* while largely dealing with legislation around the disclosure of government information to member of the public, also empowers the Privacy Commissioner in a number of interesting ways to affect change in the cyber-security realm. Section 95 (2e) of the Act states that the commissioner will "take actions necessary to identify, promote, and where possible cause to be made adjustments to practices and procedures that will improve public access to information and protection of personal information."[13] This provides the commissioner, currently Daniel Therrien, with a great amount of influence over public affairs in the information policy sphere, should they choose to wield it.

Currently the most recent governmental approach to cyber-security has been the *Action Plan 2010-2015 for Canada's Cyber Security Strategy* which laid out a five year plan for implement Canada's cyber security. Many of the goals, particularly the Critical Infrastructure plan, have been adopted from previous legislation. The CSS focussed on three major pillars of cyber security: securing government systems, partnering to secure vital cyber systems outside the

[12] *National Strategy for Critical Infrastructure.* Report no. PS4-65/2009E-PDF. 2009. Accessed April 06, 2016. http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf. pg.9

[13] Access to Information and Protection of Privacy Act, 2015, SNL 2015, c A-1.2, s 95(2) <http://canlii.ca/t/52g4c#sec95subsec2> retrieved on 2016-04-06

federal Government, and helping Canadians to be secure online.[14] In 2012, however, the Auditor General of Canada produced a report in which much of was set out to be accomplished by this time had not occurred, citing specifics such as "f[inding] uneven progress in establishing working sector networks"[15], "departmental documents supporting the requests for funding also did not specify how much funding was expected to go toward cyber protection activities"[16], and " that sensitive information was being stored on government systems that did not meet appropriate information technology security safeguards."[17] This suggests that while the current policies are either insufficient to the tasks they set out to accomplish or they are not being followed in a timely fashion. A more recent audit in 2015 of Shared Services Canada, which is tasked to implement some of these initiatives, supports the findings of the 2012 audit, indicating continued issues in this area.[18]

One of the major issues affecting the implementation of these cyber-security goals is that much of Canada's infrastructure is not under government control but by that of independent companies, particularly that of the telecommunications industry, which makes legislating improved cyber protections quite difficult. To that end the federal government created the Canadian Cyber Information Response Centre in 2012, under the jurisdiction of Public Services Canada, with the express purpose of providing tools and information to Canadian businesses in order to help strengthen Canada infrastructure protection. The CCIRC also provides industry training and workshops as well as provides further research into cyber-security matters. CCIRC was originally designed as a 24 hour, 7 day a week service; however that has yet to be realized. In the same 2012 audit, the Auditor General noted that "a restriction on operating hours means that CCIRC is not able to monitor the cyber threat environment 24 hours a day, as was

[14] *Canada's Cyber Security Strategy For a Stronger and More Prosperous Canada.* Report no. PS4-102/2010E-PDF. 2010. Accessed April 6, 2016. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf.

[15] *Report of the Auditor General of Canada to the House of Commons Fall 2012 CHAPTER 3 Protecting Canadian Critical Infrastructure Against Cyber Threats.* Report no. FA1-2012/2-3E-PDF. 2012. Accessed April 7, 2016. http://www.oag-bvg.gc.ca/internet/docs/parl_oag_201210_03_e.pdf. pg. 13

[16] *Report of the Auditor General of Canada to the House of Commons Fall 2012*. Pg. 10

[17] Ibid. Pg. 22

[18] *Reports of the Auditor General of Canada Fall 2015: REPORT 4 Information Technology Shared Services.* Report no. FA1-2015/2-4E-PDF. 2015. Accessed April 8, 2016. http://www.oag-bvg.gc.ca/internet/docs/parl_oag_201511_04_e.pdf.

envisioned in its mandate."[19] As this has yet to be corrected even by 2015, CCIRC is continues to lag in this regard.

Another area which has been almost entirely overlooked is the operational capacity of the Canadian Forces in cyberspace. The CF has almost no presence in the digital realm beyond the maintenance and security of their own networks and there has been very little progress in recent years to rectify this. As part of the Cyber Security Action Plan 2010-2015, one of the recommendations made was the establishment of a Cyber Task Force to evaluate the needs of the CF in this area, conducted by Brigadier-General Roberto Mazzolin and Greg Loos in which they recommended to the Standing Senate Committee on National Security and Defence that an expansion of the CF to improve modern capabilities include a cyber-security/warfare division.[20] However, despite presenting their case quite well and the committee seemingly sympathetic, this appears to be as far as the Cyber Task Force has been able to go in terms of effecting meaningful change.

One of the major concerns to come out of the committee hearing was an overlap in duties between the Canadian Forces and that of CSEC, which currently holds the mandate of defending Canadian cyberspace. Senator Janis Johnson voiced this possible conflict, asking what role the Generals foresaw for the CF. They responded with a suggestion that the CF limit itself to battlefield roles in this regard, but lend its expertise in during emergencies.[21] It is likely that this concern is largely what has led to the stalling of any progress in this area.

Despite these continued failures one area which has been well funded and quite success in its mandate has been CSEC. CSEC in particular has been quite effective in providing other governmental departments IT support and resources for cyber-defence and was one of the few positive sections of the Auditor General's 2012 report.[22] In that same report, however, there were issues with information sharing between CSEC and CCIRC, largely due to misunderstandings and disputes of the nature of classified information. Both departments claim that these issues have now been resolved as of November of 2012.

---

[19] *Report of the Auditor General of Canada to the House of Commons Fall 2012* pg. 16
[20] Parliament of Canada. "National Security and Defence, Evidence, November 5, 2012" Accessed 5, 2016 http://www.parl.gc.ca/content/sen/committee/411%5CSECD/49784-e.HTM
[21] "National Security and Defence, Evidence, November 5, 2012" Accessed 6, 2016
[22] *Report of the Auditor General of Canada to the House of Commons Fall 2012*. pg. 17

Recommendations

It is very much apparent that Canada is at risk of having a major cyber-attack inflicted upon it and that actions must be taken in the immediate future to rectify this imbalance. In understanding this reality, Canada has an opportunity to become a model nation in cyberwarfare policy and aid our allies across the world in building a protective cyberspace. The following are recommendations, additions, and alteration which should be made to this nation's current cyber-defence and cyberwarfare policy in the very near future. The goal is to be proactive and responsive to changes before they need to be made.

Internationally, Canada could and should take a leading role in sponsoring the creation of a resolution adopting the tenets of the Tallinn Manual during a future session of the General Assembly of the United Nations. This could likely the First Committee of the General Assembly, Disarmament and International Security (DISEC) due to the military nature of the Tallinn Manual. The DISEC committee will meet later in the fall of this forthcoming year, giving ample time to form the basis for this resolution and up this writing, cyberwarfare has not been discussed to a very large extent. The committee has not have any overt discussion of cyberwarfare resolution for at least the past five years, based on examining the resolutions passed since 2011, but has made previous efforts into the field of cyber-security, such as Resolution A/C.1/69/L.26: *Developments in the field of information and telecommunications in the context of international security*, suggesting that DISEC is the ideal area for the adoption of a Tallinn resolution.

The Tallinn Manual is one of the better options to use to form the foundation of any possible resolution as it merely applies the currently agreed to standards of conventional warfare and applies it to the digital realm. It does not prohibit any cyber-attacks except that which would unduly affect citizens and allows for limited forms of cyber-espionage. In short it effective ratifies much of what already occurs between states, but imposes limitation on targets and protects civilians from overt harm by aggressive state entities.

As Canada is not currently a member of the Security Council this would be the ideal place for this to occur. No other country is currently making headway in this regard, and Canada has always occupied a position of unique esteem with the various nations of this planet and can use this to leverage support to bring a resolution forward. By having Canada be one of the major sponsors of this resolution one could avoid some of the opposition that may be encountered

should one of the more hegemonic powers, the United States, United Kingdom, China or Russia, create the resolution instead. In this way, Canada can act as a middleman, facilitating the resolution's creation and helping to bring this issue to the fore.

Domestically, there is also much to be done. It cannot be denied that some progress has been made to increase Canada's cyber-security; however these have merely been foundational. There is a serious need of additional funding for many key projects and much of what has been put in place is poorly implemented. Therefore the recommendations of the 2015 audit of Shared Services Canada should be followed; many of which were set to be completed by the end of March 2016 so it remains to be seen if they have done so. Furthermore an additional audit should be made to evaluate the CCS 2010-2015 Action Plan and make recommendations as to new programmes on which to embark.

Funding should also be increased for CCIRC to fulfill its original goal of being a 24 hour operation. CCIRC has the potential to be a valuable resource, not only for industry in need of support in methods of cyber-defense but also for average Canadians as well. Certainly the critical infrastructure needs of the nation must be attended to, but citizens as well should have an official governmental advocate on these matters as well; a role which CCIRC could more than adequately do.

Daniel Therrien, the Privacy Commissioner can also take a more active role in advocating for increased awareness, not only on the part of the government, but also in the public consciousness of Canadians as well. Cyber-security and cyberwarfare have the potential to fade away from both of these areas until something major occurs. Whether the "digital Pearl Harbour" takes the form of an attack by a foreign power or coordinated group of stateless hackers, legislators and citizens alike should not wait for such an event to occur before concerted efforts are made. The Commissioner's mandate requires him to take be this advocate and he should not be lax in this arena. Advocacy also cost very little relative to other legislation methods; keeping the cyber security in the public consciousness.

In terms of the Canadian Forces, despite concerns of duplication of services or overlap of responsibility with CSEC, there should be concrete effort made to follow the recommendations of Brigadier-Generals Loos and Mazzolin in establishing a Canadian Cyberwarfare division. In doing so the government will show that it recognizes the realities of the modern battlefield, but also provide an additional layer of security to Canadians at large as well as adding other minds

and ways of thinking to an ever changing and diverse field. This is not to say that CSEC, CSIS, or the RCMP are doing a poor job of protecting Canadians nor that the military should be solely in charge of protecting Canada's digital infrastructure, but instead acknowledges that no one organization can police or defend cyberspace, even in a comparatively lightly populated country as Canada, therefore having as much redundancy as possible is actually beneficial. Obvious all four organizations will need to develop further policies for cooperation and information sharing as there will be a great deal of jurisdictional overlap, but even this is not an insurmountable problem.

Inspiration for the creation of a Canadian Forces cyberwarfare arm could come from the US Cyber Command (USCYBERCOM), which was formed in 2010 in response to many of the aforementioned issues and joined together a number of pre-existing organizations under a single umbrella Army Cyber Command (ARCYBER). ARCYBER's operational strength consists of over 21,000 soldiers spread over a brigade (780th MI) and three commands (1st IO Command, NETCOM, and INSCOM), with the mandate of defending US Army networks, providing operational cyberwarfare support to other branches of the military.[23] While it would be impractical to exactly replicate USCYBERCOM as the United States military is several orders of magnitude larger than Canada's, but structurally a similar organ of the Canadian Forces could be easily be created, all that is lacking is the political will. There is some good news in this regard: Brigadier- now Major-General Loos was promoted to Chief of Staff to the Assistant Deputy Minister of Information Management in February 2015 and Brigadier-General Mazzolin became the Liaison Officer to the US Cyber Command, providing both these men with the opportunity and knowledge base to advocate for future changes to the Canadian Forces.[24] Having a dedicated military-based cyberwarfare and cyber-security organ will also aid in coordinating with our regional and NATO allies, allowing for advance warning of potential threats, new theories and changes which could be applied to a Canadian context, and a wider knowledge base to improve our existing defensive measures.

---

[23] U.S. Army Cyber Command. "Establishment of U.S. Army Cyber Command." Accessed April 6, 2016. http://www.arcyber.army.mil/Organization/ARCYBERHistory.

[24] Canadian Infantry Association. "2015 General Promotions and Appointments | Canadian Infantry Association." March 25, 2015. Accessed April 7, 2016. http://www.ducimus.com/newsnouvelles/2015-general-promotions-and-appointments/

Along this vein, based on the Auditor General's reports inter-departmental communication has been a serious stumbling block. Therefore, further cooperation should be encouraged and facilitated between the various federal agencies which have a stake in cyber-security. CSEC and the Department of Public Safety, as they hold the broadest public mandate for external security (in the case of the latter) and civil security (in the former), can take a leading role integrating these services. They should ensure the creation of a detailed organization of responsibilities between all participating members and work to remove any impediments in work and intelligence sharing. CSIS should also be encouraged to continue and expand its liaisons with other departments to ensure its continued assistance in cyber-security matters.

In conclusion, the overall recommendations for future policy legislation on Canadian cyber-security and cyberwarfare policy are as follows:

Internationally

- Advocate for the adoption of the provisions of the Tallinn Manual into international law.
- Create draft resolutions to the effect of the above with the assistance of like-minded nations.
- Support international dialogues on the subject of cyberwarfare and cyber-security issues.

Domestically

- Increase resources available to federal and provincial agencies, particularly CCIRC, as well as private companies, particularly those owning critical infrastructure, to support the creation of secure networks.
- Further cooperation with regional and NATO allies in cyber defense initiatives.
- Ensure that barriers to information dissemination and cooperation between federal agencies are removed.
- Use the Office of the Privacy Commissioner to support and advocate for cyber-defense strategies and keep such issues in the public eye.
- Create a Canadian Cyber Command to provide operational support for the Canadian Forces as well as emergency aid to CSEC and civilians in the event of a major cyber-attack.

Largely many of the problems associated with Canadian cyber-security and cyberwarfare do not come from a lack of research or knowledge, but simply a lack of effort on the part of Canada's political leadership. The election of a new Liberal government has the potential to revitalize these discussions, but there must also be effort made from the electorate as well, to ensure that these challenges to not fade from view. Canada needs to be prepared to deal with these issues proactively and with purpose to ensure the safety of all its citizens.

References

Access to Information and Protection of Privacy Act, 2015, SNL 2015, c A-1.2, <http://canlii.ca/t/52g4c> retrieved on 2016-04-06

Access to Information and Protection of Privacy Act, SNL 2002, c A-1.1, <http://canlii.ca/t/jz5d> retrieved on 2016-04-06

Action Plan 2010-2015 for Canada's Cyber Security Strategy. Report no. PS9-1/2013E-PDF. 2013. Accessed April 4, 2016. http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/ctn-pln-cbr-scrt-eng.pdf.

Blaney, Steven, Hon. Report no. PS1-8/2014E-PDF. 2014. Accessed April 05, 2016. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rprt-plns-prrts-2014-15/rprt-plns-prrts-2014-15-eng.pdf

Blane, John V. *Cyberwarfare: Terror at a Click*. Huntington, NY: Novinka Books, 2001.

Canada's Cyber Security Strategy For a Stronger and More Prosperous Canada. Report no. PS4-102/2010E-PDF. 2010. Accessed April 6, 2016. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf.

Canadian Infantry Association. "2015 General Promotions and Appointments | Canadian Infantry Association." March 25, 2015. Accessed April 7, 2016. http://www.ducimus.com/newsnouvelles/2015-general-promotions-and-appointments/.

Communication Security Establishment. "Assistance to Federal Law Enforcement and Security Agencies." Web Experience Toolkit. Accessed April 6, 2016. https://www.cse-cst.gc.ca/en/inside-interieur/assist-assistance.

Etzioni, Amitai. "MAR: A Model for US-China Relations." *The Diplomat*, September 20, 2013. Accessed March 25, 2016. http://thediplomat.com/2013/09/mar-a-model-for-us-china-relations/.

Hollis, David. "Cyberwar Case Study: Georgia 2008." Small Wars Journal. January 6, 2011. Accessed March 24, 2016. http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008.

Langner, Ralph. "To Kill a Centrifuge A Technical Analysis of What Stuxnet's Creators Tried to Achieve." November 2013. Accessed March 31, 2016. http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf.

National Strategy for Critical Infrastructure. Report no. PS4-65/2009E-PDF. 2009. Accessed April 06, 2016. http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf.

Nye, Joseph S. *The Future of Power*. New York: PublicAffairs, 2011.

Parliament of Canada. "National Security and Defence, Evidence, November 5, 2012" Accessed 5, 2016 http://www.parl.gc.ca/content/sen/committee/411%5CSECD/49784-e.HTM

Public Safety Canada. "Cyber Security Technical Advice and Guidance." Accessed April 4, 2016. http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/tchncl-dvc-gdnc-eng.aspx.

Report of the Auditor General of Canada to the House of Commons Fall 2012 CHAPTER 3 Protecting Canadian Critical Infrastructure Against Cyber Threats. Report no. FA1-2012/2-3E-PDF. 2012. Accessed April 7, 2016. http://www.oag-bvg.gc.ca/internet/docs/parl_oag_201210_03_e.pdf.

Reports of the Auditor General of Canada Fall 2015: REPORT 4 Information Technology Shared Services. Report no. FA1-2015/2-4E-PDF. 2015. Accessed April 8, 2016. http://www.oag-bvg.gc.ca/internet/docs/parl_oag_201511_04_e.pdf.

Reveron, Derek S. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Washington, DC: Georgetown University Press, 2012.

Schmitt, Michael. "Tallinn Manual." Issuu. Accessed April 3, 2016. https://issuu.com/nato_ccd_coe/docs/tallinnmanual/1?e=0/1803379.

Securing an Open Society : Canada's National Security Policy. Report no. CP22-77/2004E-PDF. 2004. Accessed April 5, 2016. http://publications.gc.ca/collections/Collection/CP22-77-2004E.pdf.

Strand, Paul. "America's Cyber Defenses: A Digital Pearl Harbor?" *CBN News*, October 3, 2012. Accessed March 24, 2016. http://www.cbn.com/cbnnews/us/2011/december/americas-cyber-defenses-a-digital-pearl-harbor-/?mobile=false.

U.S. Army Cyber Command. "Establishment of U.S. Army Cyber Command." Accessed April 6, 2016. http://www.arcyber.army.mil/Organization/ARCYBERHistory.

Ventre, Daniel. *Cyber Conflict: Competing National Perspectives*. London: ISTE, 2012.