E-spionage: Developing Canada's Cyber Warfare Strategy

Dylan Powers
Graduate School of Public and International Affairs
University of Ottawa

INTRODUCTION

Cyber warfare is a serious and largely unacknowledged threat facing most developed nations. Though Canada is proud to be a global leader in communication technologies, and its public and private sectors are increasingly reliant on having access to cyberspaces, these systems are vulnerable to attack and infiltration from foreign nations. More insidious is that foreign nations have realized the possible benefits from stealing information for medium- to long-term economic and strategic gain. Canada's lack of a comprehensive approach for protecting our critical infrastructures and private systems from cyber warfare attacks makes strategic surprise more likely. The recent discovery of the Stuxnet virus in Iranian nuclear facilities and other critical infrastructures around the world has demonstrated that governments are investing time and money in cyber espionage (The Economist (b), 2010). Moreover, the attacks on Estonia have demonstrated the vulnerabilities that a modern, highly connected state faces from cyber warfare (Almann, 2008). These events have highlighted Canada's vulnerabilities to a government-sponsored cyber attack. While Canada has recently released its cyber security strategy, it deals mainly with cyber crime and protecting citizens from criminals, with little reference to critical infrastructures or state-sponsored cyber espionage. It is imperative that Canada develop a comprehensive strategy that utilizes intelligence services to protect Canadians.

This essay will recommend that Communications Security Establishment of Canada (CSE) be empowered to take more proactive measures in protecting private and public systems, as well as developing our offensive cyber capabilities. Moreover, CSE could utilize its FIVE EYES alliance to promote global cooperation and coordination

in the face of a cyber attack. Finally, the Canadian government should promote the need for greater collaboration among possible belligerents in cyberspace, namely China and Russia, and advocate for the creation of an international regime to limit and outline the acceptable usages of cyber weapons.

WHAT IS CYBERSPACE

Information technology has reconfigured the traditional battlefield by further reducing the fog of war, increasing intelligence gathering capabilities, and allowing instantaneous information sharing between field and command. Modern armies are heavily reliant on information technologies, as their weapons and defense systems are all computerized. More importantly, as a result, cyberspace has now become a fifth field of battle after land, air, water, and space. It is defined as "a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures" (US Department of Defense, 2006). Cyberspace has several characteristics that are of strategic importance to states. First, cyberspace is not inherently restricted to geopolitical boundaries, yet nations are actively erecting walls in an attempt to balkanize cyber space (The Economist (a), 2010). Second, it is tightly integrated into the operation of critical infrastructures, such as water, power, air traffic systems, early defense warning systems, and banking infrastructure to name a few (Baker, Waterman, and Ivanov, 2010). Third, it is created, maintained, and owned and operated by public, private, and government actors. Fourth, it exists across the globe, and is readily accessible to all nations. This makes it incredibly difficult to protect from a national defense standpoint. Cyberspace is more than just the internet; it includes many other networks, which are similar to the Internet, but in theory are separated from it (Clarke, 2010). These include transactional networks, which facilitate the sending of data on money flows and stock market trades. Also, some networks are control systems that allow machines to speak to one another,

The Economist (a), 2010

such as control panels talking to pumps, elevators, and generators (Clarke, 2010). Finally, actions in cyberspace can move at the speed of light. This makes detection of intrusion and adequate defense against an attack immensely difficult.

A central element to cyberspace policy making was the belief that the role of government in this new domain should be minimal (Lewis, 2010). This belief has had a detrimental effect on security. Cyberspace has been viewed as a type of global commons due to its lack of national borders; however, this belief should be re-examined. Many states assert that both the infrastructure and the content of cyberspace exist under the authority of national jurisdiction (see chart: The Economist (a), 2010). Pursuing this dream only undercuts national and international security, as foreign governments are seeking technology and policy solutions to gain a greater control of cyberspace.

Governments are increasingly asserting their sovereignty in cyberspace. The most prominent example is the Great Firewall of China, which is an effort to balkanize the Internet in order to gain greater control over what their citizens can access online. Moreover, the physical infrastructures are all located within national territories and are all subject to proprietary interests. Societies' exuberance for incorporating the Internet into our daily lives neglected the realities that the Internet was never designed to be secure or to become a global infrastructure that millions of people would depend on.

ORIGIN AND DEFINITION OF CYBER WARFARE

> "One hundred victories in one hundred battles is not the most skillful. Seizing the enemy without fighting is the most skillful."
>
> - Sun Tzu, 6th century B.C.

> "War is thus an act of force to compel our enemy to do our will"
>
> - Clausewitz

Sun Tzu's assertion that the best form of warfare is to take down the enemy without fighting is becoming a reality through society's growing dependence on computer and information networks. As the capabilities to wage war have been increased, so too have the vulnerabilities to digital attacks. Moreover, cyber war must be distinguished from cyber criminals and cyber terrorism. State action must be involved, however

it can also include "hacktivists"—computer hackers that choose their targets based on nationalistic beliefs. This is because states often blame rogue citizens if they are accused of cyber attacks since it is very difficult to prove if a state directed the attack or not. Thus, through combining the essences of the two great military theorists quoted above, cyber warfare can be defined as the instance when a state "is capable of compelling the enemy to [their] will by inducing strategic paralysis to achieve desired ends...this seizing of enemy is done almost without an application of physical force"(Sharma, 2009). A similar definition, which incorporates the espionage aspect of cyber warfare is as follows:

> Attacks and infiltrations by either state or organized non-state actors against government and critical infrastructure systems (privately and publicly owned) to gain knowledge of a national security value and/or attempt to degrade/disrupt such systems (Hare, 2009)

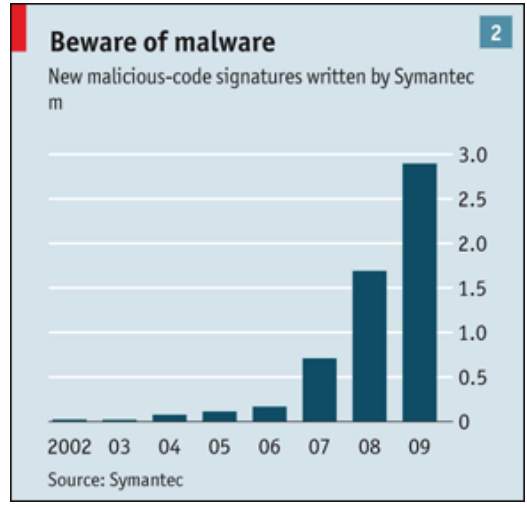
From an intelligence stand point, there are three principal aspects to be consider: information theft, compromising defense systems, and developing the capacity to attack critical infrastructures. Already, the international community has witnessed cyber attacks from one country directed against another country.

FIRST CYBER WAR: A LOOK AT THE ESTONIA CASE

A well-documented instance of cyber war happened in 2007 against Estonia. Tensions between Estonia and Russia have been high ever since the nation declared independence at the end of the Cold War. These tensions came to a head over a dispute surrounding a monument dedicated to Russian sacrifices during WWII in Tallinn, the capital of Estonia. Estonia is one of the most wired countries in the world, ranking far ahead of Canada and the US in broadband access and penetration of the Internet in daily lives (Clarke, 2010). The same night that tensions within Estonia between ethnic Russians and Estonian nationalists finally erupted into a riot, Estonia was hit with the largest distributed denial of service (DDOS) attacks ever witnessed in history. A DDOS is "a preprogrammed flood of internet traffic designed to crash or jam networks... it is distributed in the sense that thousands, even hundreds of thousands, of computers are engaged in sending the electronic pings to a handful of targeted locations on the Internet" (Clarke, 2010). Often, the attacking computers have no idea that they have become weaponized; malicious software has turned these computers into "zombies" under remote control from a single source. Suddenly, Estonians could not access their government websites, Internet

banking services, or their newspapers' websites. Then, the DDOS attack shifted to attacking parts of the telephone network, the credit-card verification system, and the Internet directory. The Estonia national bank, Hansapank, was overwhelmed and its web services crashed.

This attack persisted for weeks, until Estonia had to appeal to NATO for support in disrupting the attack. Using trace-back technology, experts were able to trace the attacks coming from Russia, however it could not prove that the attacks were state-sponsored. Russia denied any involvement in the attack, claiming it could have been the work of patriotic Russians acting unilaterally. Russia also denied Estonia's formal diplomatic requests for assistance in tracing the attacks, despite a bilateral agreement requiring Russia to do so (Almann, 2008). It is difficult to determine if this attack was the first attack of cyber warfare between states, or a well-organized attack from an underground, nationalist community. Without further information, experts will never know who orchestrated the attack on Estonia or be able to conclude if it was an act of aggression from Russia. What is known is that Russia was engaged in a domestic propaganda campaign against Estonia before the attack, it had helped facilitate the attacks by refusing to find the culprits, and then refused to investigate or punish suspects that were found by NATO (Almann, 2008). To Estonians unable to access their banking services, withdraw money from ATMs or complete phone calls, the distinction is merely academic.



The Economist (a), 2010

ANALYSIS/ KEY ELEMENTS OF THE PROBLEM

International

In cyber war, threats to information systems arise from foreign intelligence services and militaries. Foreign intelligence services have used cyber tools as a means to conduct their espionage activities against Canada. Over 120 countries are currently aggressively developing information espionage capabilities (Adams, 2008). The

threat landscape has changed significantly over the years. Originally, the goal of cyber attacks was to disrupt services, as witnessed in the Estonia case and the many early computer viruses. However, through the growing role of foreign intelligence services, the threat strategy has shifted from disruption for short term gain to stealing information for exploitation in the mid to long term (Adams, 2008).

These exploitative programs are called Malware and their creation has been exploding in recent years (see chart: The Economist (c), 2010). This can include stealing intellectual property information from organizations, stealing personal information of private citizens entrusted to the government, and instilling fear in citizens. The goal of foreign intelligence services is to acquire sensitive information without detection. This will pose a challenge to governments and businesses. Already, China has been accused of attempting to access secret Pentagon files and Chinese hackers were found stealing Barrack Obama's confidential policy platform during the US election in 2008 (Clarke, 2010). China has also been accused of creating GhostNet, which is a cyber espionage system that has infected government ministries and embassies in over 103 countries (Information War Monitor, 2009). And China is not the only country that has engaged in cyber espionage; France, Russia, and North Korea are also notorious for exploiting cyber space for national purposes (Clarke, 2010). Foreign governments have demonstrated a willingness to develop and use cyber espionage capabilities and they pose a serious threat to the Canadian government and businesses.

There are many diverse threats and vulnerabilities in a cyber dependent world. Yet, the most devastating threat to any state would be a concerted cyber attack carried out by a prepared nation. As Admiral Mike McConnell has noted, "information managed by computer networks—which run our utilities, our transportation, our banking and communications—can be exploited or attacked in seconds from a remote location overseas. No flotilla of ships, intercontinental missiles, or standing armies can defend against such remote attacks located not only well beyond borders, but beyond physical space, in the digital ether of cyberspace"(Clarke, 2010). The greatest fear among US officials is an "electronic Pearl Harbor", where an adversary "could strike a sudden, crippling blow against the information systems on which the US military forces, financial institutions, and society depend. The result would be chaos and destruction" (Center For Strategic and International Security, 1998). There is a great drive within many nations to develop offensive cyber capabilities because

it represents an equalizer in the field of intelligence. States no longer need to spend billions of dollars on high-tech satellites to pursue high-level intelligence gathering; they can simply achieve this via the web at a very low cost.

One problem that exists internationally is a lack of a clear consensus of what constitutes cyber warfare and there have been few attempts to define international mechanisms on how states should respond (Kanuck, 2010). The Estonia case was never declared an act of war and for that reason NATO never invoked Article 5, which stipulates that an armed attack against one member is an attack against them all (Kanuck, 2010). A proper definition of cyber warfare must be formulated in order to create a common understanding of what constitutes a cyber attack and how to respond to such an attack. This deficiency has been noted by President Obama when he stated that "the Nation needs a strategy for cyber security designed to shape the international environment and bring like-minded nations together on... acceptable legal norms regarding territorial jurisdictions, sovereign responsibility and use of force"(White House, 2009). In the absence of historic precedents, new international norms surrounding cyberspace are being created by government officials, which might have an interest in derailing international efforts in order to gain a strategic advantage. Moreover, no current international institutions—Interpol, Cybercrime convention, NATO's CyberCentre of Excellence—are properly established or mandated for the exchange of ideas and best practices needed in this area. Without a proper institution to facilitate the flow of information concerning cyber security issues, the prospects for escalation will increase. A proper forum is needed that can allow for dialogue on cyber security concerns, or else escalation of minor skirmishes in cyber space might result in full-blown war.

Secondly, there have been no treaties aimed at restraining the proliferation of cyber weapons, or outlining the proper use of such weapons. A United Nations group of governmental experts attempted to reach a consensus on possible cooperative measures to address potential threats in the sphere of information security. This attempt failed, stating that "given the complexity of the issues involved, no consensus was reached on the preparation of a final report."(UN Secretary-General, 2005). Moreover, there has been a lot of debate about whether cyber warfare falls under the Law of Armed Conflict and the Geneva Convention. Some academics and policy makers believe that cyber warfare falls neatly under these categories, while others believe that there is a need for an entirely new set of international laws and treaties (Hughes, 2009).

Domestic

Domestically, there is a belief that there is little that government regulations can achieve in cyberspace due to the multitude of actors engaged in maintaining the system (Lewis, 2010). Globally, the digital infrastructure is fragile. More than nine-tenths of Internet traffic flows through undersea fibre-optic cables, which are dangerously concentrated into a few, small choke points around New York, the Red Sea, or the Luzon Strait in the Philippines (The Economist (d), 2010). Other areas of vulnerabilities are frequently arising; weakly governed areas of Africa are being connected to fibre-optic cables, which potentially create new, easily accessible intrusion points (The Economist (d), 2010). There are many vulnerabilities facing a highly connected and advanced country such as Canada. An important vulnerability is the speed at which digital attacks can strike. In 2004 the Sasser virus spread to every core Internet router in less than an hour, causing an estimated $3.5 billion in damages. The ability of an attack to cripple a system at great speed means that reactive measures to counter cyber attacks are inadequate on their own. Proactive measures must be in place, such as automatic fail safes, to protect against an attack. Another glaring vulnerability comes from our critical and non-critical infrastructures. Recently, the Stuxnet virus was detected within critical infrastructures around the world; however, it was only designed to render a specific part of the Iranian nuclear weapon development program inoperable (The Economist (b), 2010). After analyzing the virus, experts have concluded that the only likely developer was a national military, due to the sophistication of the code and the specific nature of its mission. This attack demonstrates that national militaries are investing resources in developing offensive cyber weapons.

Due to its complex structure and the importance that private sector actors (such as Internet providers and the banking sector) have in building the networks, governments cannot move forward without consulting and co-opting the help of these actors. Indeed, governments cannot ensure complete cyber protection without the support of the private sector. However, their expertise and resources are needed for several reasons and it is imperative that the private sector fully understand the need for a greater government role. A sophisticated military and intelligence services will overwhelm the capabilities of private efforts to secure their networks (Lewis, 2010). The private sector cannot match the resources or effort of a determined national military or intelligence service; these organizations invest hundreds of millions of dollars and employ thousands of people to defeat any security measure

(Lewis, 2010). Second, without government intervention, cyber security will not be provided. Cyber security is a public good and returns on investment for providing this security are difficult for individuals to capture. Thus, government intervention is necessary, despite the belief among policy makers that this area is beyond their reach, control, or jurisdiction.

Finally, a public dialogue is needed to raise awareness about cyber war. No major security policy school—such as Havard's Kennedy School, Princeton's Woodrow Wilson School, or Texas' Lyndon Johnson School—have any courses on cyber war policy or strategy (Clarke, 2010). Moreover, there have been few books dedicated to the subject. This might partly be due to the fact that much of the material is secret. In the 1950s and 1960s, many security theorists were told that nuclear war was something that could not really be discussed publicly (Clarke, 2010). In response to this, Herman Kahn wrote Thinking about the Unthinkable (1962), which contributed to a public debate about the moral, ethical and strategic aspects of nuclear war. This was built upon thorough and open research and writing by academics on the topic. Because of their work and the ensuing public debate, military doctrine had to move beyond its original focus of first-strike and tactical use of nuclear weapons, to second strike and deterrence capabilities[1].

TOWARD A NATIONAL STRATEGY: WHAT HAS BEEN DONE ALREADY

> "Short-term thinking drives out long-term strategy, every time"
> - Herbert Simon (Clarke, 2010)

In light of the threats and vulnerabilities highlighted above, Canada would benefit from a comprehensive strategy for cyber war. This will require the collaboration and coordination of all Canadian federal government departments, as well as international and military engagement, and the involvement of intelligence and law enforcement agencies.

Canada's attempts at creating this strategy have thus far been unimpressive. Canada's Cyber Security Strategy is built upon three pillars: securing government systems, partnering to secure vital cyber systems outside the federal government, and

1. In nuclear strategy, first strike is a pre-emptive nuclear surprise attack with overwhelming force designed to neutralize an opponent. A second strike capability counters a first strike through the assured ability of the country to respond with a powerful nuclear attack. Second strike capabilities are essential to deterrence.

helping Canadians to be secure online (Department of Public Safety Canada, 2010). Public Safety Canada (PSC) is be responsible for coordinating and implementing the Canadian strategy, and a whole-of-government approach has been adopted by giving authority to various departments within PSC. However, this disperses responsibility and diverts accountability to a plethora of departments. Furthermore, the strategy aims to mitigate the effects of lesser threats, such as cyber crime and cyber terrorism; yet effective mitigation of lesser threats does not mean that more consequential threats, such as cyber war, are also mitigated (Cutts, 2009). The strategy fails to create a central command centre for cyber operations; the closest thing is the Canadian Cyber Incident Response Centre, however, it only provides advice and monitors cyber threats – it has neither the expertise to thwart attacks, nor the ability to conduct cyber operations. Given the scale at which foreign intelligence services are investing in their cyber capabilities, Canada cannot afford to disperse responsibility among various organizations with ingrained cultures and organizational biases. Furthermore, the strategy does not discuss the promotion of cyber war concerns on the international stage, addressing the possibility of cyber war escalation, or creating forward-thinking policy that can direct international law. Finally, there is no discussion about how Canada can promote public dialogue or encourage research so as to create a sustainable military doctrine aimed at dealing with issues of cyber security.

Essentially, the existing national strategy has neglected to address any of the core concerns that this essay argues are necessary. Accountability is also very important and one department needs to take ownership of protecting Canada from cyber threats. This essay will argue that Communications Security Establishment of Canada (CSE) is the department that should be accountable and mandated to protect Canadian information systems, as well as developing offensive capabilities.

CANADA'S NEW CYBER SECURITY STRATEGY

A serious national cyber security strategy must seek an appropriate balance of resources, energy, and focus between threats that are most frequent and those that are most consequential (Cutts, 2009). Without a government agency to take the lead and be accountable on cyber security, Canada's response to cyber warfare will not move beyond the response to frequent threats and will be caught unprepared for the most consequential.

Domestic Strategy

In order to construct a national strategy, there are three principal aspects to consider: information theft, compromising defense systems, and developing the capacity to attack critical infrastructures. These three areas should be the priority of a national cyber strategy. The Canadian agency that is best suited to fulfill these objectives and lead Canada's cyber security strategy is CSE. Currently, CSE is on the front lines of cyber warfare and has been actively protecting Canadian networks from foreign intrusion (Adams, 2008). This role is consistent with its current mandate of safeguarding Canadian security to ensure the protection of information. Its mandate is three-fold—to provide foreign SIGINT according to the Government's intelligence priorities; to safeguard Canada's security by providing advice, services, and protection of infrastructures of importance to the government; and to assist law enforcement and security agencies in their duties (Communications Security Establishment of Canada, 2008). Moreover, its defense responsibilities include (Adams, 2008):

a) Its foreign intelligence program, which is an information source for understanding these threats.
b) The requirement that CSE designs the government of Canada's networks and employ strong security technologies to make it difficult for cyber attacks to succeed. Also, proactive by studying the most sophisticated attacks.

There are several reasons why CSE should spearhead all of Canada's efforts to secure its cyber space. CSE's IT security program (ITS) is at the forefront of cyber protection (Adams, 2008). They have developed the expertise and knowledge of how to handle cyber threats and work closely with military and law enforcement agencies to monitor the evolution of threats. Also, CSE is part of a FIVE EYES alliance that actively shares information on all aspects of cyber security. CSE will be able to utilize its FIVE EYES alliance to collaborate internationally with our allies. Therefore, they are already integrated into a sophisticated and historical alliance that would be capable of monitoring compliance of any international cyber arms treaty. Building a similar alliance from a different agency would take years and would be unnecessary; rather, resources would be best spent bolstering this existing alliance. Also, consistent with their mandate, CSE has already been providing guidance and has developed close links with private security firms and firms associated with Canada's critical infrastructures. Finally, in accordance with its defense mandate A, CSE has the authority to construct offensive capabilities and prepare for foreign cyber warfare operations (Adams, 2008).

Therefore, this essay recommends that Canada mandate CSE to lead the whole-of-government efforts to secure its cyberspace by transforming its ITS division into a cyber command, with increased responsibility and budget. This cyber command will report to the Chief of CSE, who in turn reports to the Minister of Public Safety, Privy Council Office and Department of Defense. This is because cyber warfare concerns are both civilian and military problems. Furthermore, ITS will be responsible for developing offensive cyber capabilities to act as a deterrent to future attacks. Its counter intelligence goals will be to: identify adversary intent, targets, and capabilities; exploit adversary cyber operations; and, provide threat warning (US Department of Defense, 2006). These short-term goals will need to be coupled with long-term strategic thinking. CSE has experience with the analytical skills and practices in long-term strategy formulation to make it the ideal department to house Canada's cyber command.

A problem surrounding Canada's ability to engage in and defend against cyber attacks is a lack of governance at a senior level. A departmental body should be mandated to be a high-level hub for sorting out issues related to "network architecture, software development standards, information assurance, and the testing and clarification of new capabilities" (Information Operations and Cyber Space Newsletter, 2010). This will include consulting and creating standards for the creation of software, providing the tools and information needed for the private sector to adequately defend its networks from intrusion, and to design Canada's cyber weapons moving forward. Fortunately, Canada has already mandated CSE to be accountable for many of these issues; however, it requires more support and funding as well as robust government regulation in order to fulfill these goals.

A crucial aspect of these suggestions however, is the need for the Canadian government to more effectively regulate cyber space. Until now, Canada has followed the trend of most developed countries and has been reluctant to place regulations on how the private sector engages with cyberspace, preferring to allow it to grow and develop without government intervention. This is an unsustainable position. Regulations must be put into place that will, for instance, dictate the level of Internet security that critical infrastructure must employ. Laws should also be put into place that will allow CSE to fulfill its mandates. These could include having CSE monitor and regularly test private sector security systems and issue fines to non-compliers. Also, it should be allowed to conduct "stress tests" on private sector

security systems. The important aspect is that the government shed its reluctance to create regulations on cyberspace.

International Strategy

The question that should drive Canada's foreign policy towards cyber warfare is: "What steps can be taken both today and into the future to forestall a major arms race and interstate competition in cyberspace"(Hughes, 2009)? Toward this end, Canada should push forward on a 3-pronged front. First, it needs to help resolve the debate around whether cyber warfare falls under existing international treaties or if it requires an entirely new international regime. This can be done by hosting and organizing conferences and debates in Canada and The Hague, where NATO and the International Court of Justice (ICJ) are housed. As an active contributor to NATO, Canada could utilize this alliance to create an international debate around the subject. Second, whether the conduct of war in cyber space is governed by existing treaties or not, a necessary component at the international level is a comparable arms treaty to the Strategic Arms Limitation Treaty (SALT). Its goal would be to limit cyber war, not to ban hacking activities or intelligence gathering. This treaty would accept that national intelligence gathering is inevitable and states have a right to non-interference in gathering intelligence. The history of arms control treaties shows that they start modestly and then their scope is expanded in subsequent agreements as confidence in their success grows and greater monitoring capabilities develop (Clarke, 2010). Thirdly, and finally, Canada should utilize its FIVE EYES alliance to combat potential adversaries in cyberspace. This alliance, if managed effectively, could present a strong deterrent against solitary, belligerent states. At this forum, Canada should work with its allies to develop new, offensive cyber capabilities, as well as share best practices for effective defense.

CONCLUSION

Canada would be at a strategic disadvantage if it chose to neglect the gathering cyber storm. Cyber warfare is here and states are preparing their militaries and intelligence agencies to engage over this 5th domain. The threats and vulnerabilities to a country as highly connected as Canada are numerous and complex. Moreover, there are serious domestic and international hurdles that must be overcome in order to build robust cyber warfare preparedness. For this to be accomplished, CSE needs to be mandated to be the leading force on Canada's cyber initiative. It has the technical expertise, existing infrastructure, and strong international alliances that

are imperative to creating a comprehensive cyber program. However, they cannot do this alone and lawmakers need to place greater regulations on the Internet, as well as work actively to create an international regime to manage developments in cyber space. The stakes for failure are high and it is important that Canada prioritizes these issues through demonstrating international and domestic leadership. There is sufficient strategic warning that a risk of cyber warfare exists. Yet, these signs are not being fully appreciated. Even if Canada fully learns from the lessons of Estonia, history has shown that one should never prepare for the last war, but the next one.

WORKS CITED

Adams, John. (Chief, Communications Security Establishment Canada), "Canada's Cyber Security Issues – What's Here and What's Coming", address delivered to the Conference Board of Canada's seminar Cyber Security: Proactive Defence of Critical Systems and Information. Decemebr 2008 [online] available from http://www.conferenceboard.ca/e-library/abstract.aspx?did=2800

Almann, Lauri. (Permanent Undersecretary of Defense, Republic of Estonia), "External Cyber Attacks on Government and Infrastructure Operations" address delivered to the Conference Board of Canada's seminar Cyber Security: Proactive Defence of Critical Systems and Information. Decemebr 2008 [online] available from http://www.conferenceboard.ca/e-library/abstract.aspx?did=2800

Baker, Stewart. "In the Crossfire: Critical Infrastructures in the Age of Cyber War", published by McAfee Inc., 28 January 2010 [online] available from http://csis.org/event/crossfire-critical-infrastructure-age-cyber-war

Center For Strategic and International Security, Cybercrime, Cyberterrorism, and Cyberwarfare, (The CSIS Press, 1998)

Clarke, Richard A. Cyber War: The Next Threat to National Security and What To Do About It. (HarperCollins Publishers, 2010),

Cutts, Andrew. "Warfare and the Continuum of Cyber Risk: A Policy Perspective" in The Virtual Battlefield: Perspectives on Cyber Warfare eds., C. Czosseck and K. Geers (IOS Press, 2009)

Department of Public Safety Canada, Canada's Cyber Security Strategy, 5 October 2010 [online] available from http://www.publicsafety.gc.ca/prg/em/cbr/ccss-scc-eng.

Globe and Mail, China's Got RebBerry, Apr.11th 2006, [online] available at http://www.theglobeandmail.com/report-on-business/article819974.ece

Hare, Forrest. "Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security?" in The Virtual Battlefield: Perspectives on Cyber Warfare eds., C. Czosseck and K. Geers (IOS Press, 2009)

Howard, Michael and Paret, Peter. eds., On War (Princeton University Press, 1984) Book I, Chapter I, section 2,

Information Operations and Cyber Space Newsletter, 7th Annual US Army Global Information Operations Conference, Vol. 10, Issue. 7 (January/March, 2010), p 16 available online http://www.phibetaiota.net/2010/03/information-operations-newsletter-vol-10-no-07/

Information War Monitor, Tracing GhostNet, March 29 2009, (SecDev Group, Munk Centre for International Studies) [online] available at http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network

Kanuck, Sean. "Sovereign Discourse of Cyber War and International Security", in Texas Law Review, Vol. 88 Issue. 7 (Jun 2010, p. 1571-1597)

Lewis, James A. "Sovereignty and the Role of Government in Cyberspace", in Brown Journal of World Affairs, Vol. 16, Issue. 2 (Spring/Summer, 2010 p. 55- 65)

Raisinghani, Mahesh. "Bits and Bytes vs. Bullets and Bombs: A New Form of Warfare", in Cyber Warfare and Cyber Terrorism eds., Lech J. Janczewski & Andrew Colarik (IGI Global, 2008),

Sharma, Amit. "Cyber Wars: A Paradigm Shift from Means to Ends" in The Virtual Battlefield: Perspectives on Cyber Warfare eds., C. Czosseck and K. Geers (IOS Press, 2009)

The Economist (a), The Future of the Internet, Sept. 2nd, 2010 [online] available from http://www.economist.com/node/16941635

The Economist (b), The Stuxnet Outbreak, Sept 30th, 2010 [online] available at http://www.economist.com/world/international/displaystory.cfm?story_id=17147818

The Economist (c), The Threat from the Internet: Cyberwar, 1 July 2010 [online] available from http://www.economist.com/node/16481504

The Economist (d), War in the Fifth Domain, July 1st 2010, [online] available at http://www.economist.com/node/16478792?story_id=16478792

Tzu, Sun translated by Samuel B. Griffth, The Art of War. (Oxford University Press, 1963)

UN The Secretary-General. Group of Governmental Experts on Developments in the Fieldof Information and Telecommunications in the Context of International Security, 5, delivered to the General Assembly, U.N. Doc, A/60/202 (Aug. 5, 2005) [online] available at http://disarmament.un.org/Library.nsf/c0996f411fc369518525704c00502170/e67ac010a7a6434985257088007l6e75/$FILE/exgr60.202.pdf

US Department of Defense, National Military Strategy for Cyberspace, December 2006 [online] available at http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf

White House Cyber Space Policy Review (2009) [online] available at http://www.whitehouse.gov/assets/documents/Cyberspace_Policy„Review_final.pdf