

*The Government of Canada and Cyber Security:
Security Begins at Home*

John Adams

Computers and information systems have become a fundamental part of Canadian life. Life, commerce and statecraft have gone digital. The associated information technology underpins nearly all aspects of today's society. They enable much of our commercial and industrial activity, support our military and national security operations and are essential to everyday social activities.

Data collection, processing, storage, and transmission capabilities are increasing exponentially. The interconnected networks, to include all levels of government, where billions of people are linked together to exchange ideas and services are known as cyberspace. Cyberspace is now conventionally used to describe anything associated with the Internet.

In today's global community, national security is not assured by having control over an area within recognized borders, it is dependent upon having the ability to navigate through the global commons. These commons – sea, air, space and cyberspace – facilitate the functioning of the global economy¹. Technologically advanced societies are becoming increasingly dependent upon the rapid and reliable transmission of ideas, information and data. A vast amount of data is constantly in motion and an

¹ Murphy, Tara. "Security Challenges in the 21st Century Global Commons", Volume 5, Issue 2, 2010, Yale Journal of International Affairs, available at <http://yalejournal.org/2010/07/page/2/>.

astronomical quantity is being stored. Furthermore, owing to market incentives, innovation in functionality is outpacing innovation in security and neither the public sector nor the private sector has been successful at fully implementing existing best practices. Consequently, data is vulnerable be it at rest or in motion. The potential for malicious activity is endless. National, commercial and industrial security are therefore threatened.




Canada is in Love With the Internet

Table 1: Proportion of Canadians using the Internet²

Online Landscape Worldwide in 2010

Canada maintained its position as the most engaged online audience, ranking highest among the top markets in average hours and visits per visitor in Q4 2010.

Location	Total Unique Visitors (000)		Average Hours/Visitor		Average Pages/Visitor		Average Visits/Visitor	
	Q4 2010	Q4 2009	Q4 2010	Q4 2009	Q4 2010	Q4 2009	Q4 2010	Q4 2009
Worldwide	1,314,031	1,206,146	23.1	23.7	2,133	2,252	53.0	54.6
China	287,451	232,037	13.5	15.6	1,238	1,599	38.6	57.7
U.S.	181,239	172,194	35.3	33.3	2,953	2,822	80.9	70.8
Japan	72,913	69,826	18.4	20.0	1,928	2,108	43.8	47.3
Germany	49,257	45,216	24.1	22.0	2,858	2,654	60.0	58.7
Russia	45,692	36,589	21.8	16.5	2,704	2,399	52.9	44.5
France	41,827	39,137	26.6	28.1	2,752	2,934	68.7	70.3
India	41,170	36,535	11.9	12.1	1,089	1,183	30.6	27.1
Brazil	39,335	32,849	25.8	27.0	2,089	2,672	56.5	58.8
UK	38,581	37,674	32.3	31.3	2,883	2,735	69.4	60.3
South Korea	30,155	29,424	27.7	35.6	4,093	4,986	50.1	72.5
Canada	22,945	23,138	43.5	42.2	3,349	3,793	95.2	88.8

© comScore, Inc. Proprietary and Confidential. 6
 Source: comScore Inc., Media Metrix, World Metrix, All Locations, Persons: 15+, 3 MO. AVG Q4 2009 & Q4 2010.

² <http://blog.suitcaseinteractive.com/2011/03/comscore-report-sows-that-canucks-are-internet-usage-stars/>

Canadians spend more time on the Internet than anyone in any other country, and the amount of time they spend online is nearly double the worldwide average, 43.5hrs/month versus 23.1³.

And the potential for continued growth is high. People aged 55 and older are now the fastest growing demographic of Internet users and now accounts for 1 in 5 Internet users⁴.

And there is virtually no aspect of Canadians' lives that is not touched by the Internet⁵.

³ Thomas, Knowlton. "Trends and Stats: Canadians use the Internet more than anyone else in the world", Mar 9, 2010, available at <http://www.techvibes.com/blog/trends-and-stats-canadians-use-the-internet-more-than-anyone-else-in-the-world-2011-03-09>

⁴ Ibid.

⁵ Statistics Canada, "Online activities from any location (% of internet users), Wednesday, October 12, 2011, available at <http://www.statcan.gc.ca/daily-quotidien/111012/t111012a3-eng.htm>

Table 2: Online activities from any location (% of Internet users)

	2010
	%
E-mail	93
Window shopping or browsing for information on goods or services	74
Electronic banking (e.g., paying bills, viewing statements, transferring funds between accounts)	68
Reading or watching the news	68
Travel information or making travel arrangements	65
Visiting or interacting with government websites	65
Searching for medical or health-related information	64
Using social networking sites	58
Researching community events	54
Using an instant messenger	47
Downloading or watching movies or video clips online	47
Obtaining or saving music (free or paid downloads)	46
Searching for employment	37
Formal education, training or school work	37
Listening to the radio online	37
Obtaining or saving software (free or paid downloads)	35
Playing online games	33
Downloading or watching TV online	33
Researching investments	27
Making telephone calls online	24
Selling goods or services (e.g., through auction sites)	19
Contributing content or participating in discussion groups (e.g., blogging, message boards, posting images)	19

In 2010, 51% of Internet users ordered goods or services for personal or household use. In total, Canadians placed in the order of 114M orders, valued at approximately \$15.3B⁶.

⁶ Ibid.

The average Canadian visits nearly 100 different websites over a three-month period, more than double the worldwide average of 42. 25M Canadians used the Internet in the last quarter of 2010.⁷

And the beat goes on. Worldwide tablet shipments rose more than 56% quarter over quarter at the end of 2011 to over 20M units, according to the International Data Corporation (IDC). That marks a 155% boost year over year, IDC says. 2011 saw just under 70M units shipped in total. In 2012 IDC expects more than 100M units to be shipped.⁸

An obvious impact of the digital world's evolution is evident in the near-total sea change with respect to how we communicate. In the order of 90% of Canadians use email at least weekly.⁹ Furthermore, the "digital native" generation is going to change how the world does business, according to Symantec CEO and President, Enrique Salem.¹⁰

Salem describes "digital natives" as people typically born in the 1990s who have never known a time before the Internet or smart mobile devices. Where the previous generation welcomed email into its business practices, these "natives" are entirely comfortable with a constant staccato of texting and messaging as a key means of communication. As a group, their social fabric is interwoven with media such as Facebook, LinkedIn and Twitter, and individuals' cyber security practices may be affected by shifting attitudes towards online privacy.

To "digital natives", there's no distinction between the Internet at work and the Internet at home. Thus, the trend we see emerging – primarily thanks to "digital natives" – is "BYOD" or Bring Your Own Device to work, blurring the lines between personal life and work.

⁷ techvibes Op. cit.

⁸ Poeter, Damon. "IDC: Strong Q4 iPads, Android Tablet Sales Push 2012 Forecast Upwards", March 13, 2012, available at <http://www.pcmag.com/article2/0,2817,2401531,00.asp>

⁹ Internet World Stats: Usage and Population Statistics (Canada), available at <http://www.internetworldstats.com/am/ca.htm#links>

¹⁰ King, Rachel. "Symantec CEO: 'Digital Natives' will change the way we do business", February 23, 2012, available at <http://www.zdnet.com/blog/btl/symantec-ceo-digital-natives-will-change-how-we-do-busiess/70395?tag=content;siu-container>

This will introduce more vulnerabilities that will clearly impact on the way we do business Salem suggests. It will add to the cyber challenge.

The Threat

Let me at the outset of this section spend a few minutes on terminology. I will start with “cyber- attack”. It is an umbrella term for several types of cyber related activities, each of which has different motivating factors:

- “Hacktivism” is a cyber- attack motivated by political activism that often involves defacing a website for the explicit purpose of publically shaming the target;
- “Cyber- crime” may involve using cyber attack as a means, but its sole motivation is to gain financially from the attack;
- “Cyber- espionage” is using cyber attack methods to covertly access information of national interest belonging to others;
- “Cyber- terrorism” is the systematic threat or use of violence, often across national borders, to attain a political goal or communicate a political message through fear or intimidation of non-combatant persons or the general public.¹¹

Threats from cyber-espionage, computer crime and attacks on critical infrastructure will surpass terrorism as the number one threat facing the United States, FBI Director, Robert Mueller testified before the Senate Select Committee on Intelligence on 31 Jan 2012.¹²

“I do not think today it is necessarily [the] number one threat, but it will be tomorrow.” Mueller said. “Counter-terrorism – stopping terrorist attacks – with the FBI

¹¹ Czinkota, M. R., Knight, G. A., Liesch, P. W., and Steen, S. (2005) Positioning Terrorism in Management and Marketing: Research Propositions. *Journal of International Management*, 11(4), pp. 581-604.

¹² Associated Press, “FBI Director Robert Mueller Talks Cyber Security: We must Find a Way to Stop the Bleeding”, January 3, 2012, available at http://www.huffingtonpost.com/2012/03/01/fbi-director-robert-mueller-cybersecurity_n_1315112.html

is the present number one priority. But down the road, the cyber threat, which cuts across all [FBI] programs, will be the number one threat to the country.”

United States’ officials estimate that there are 60,000 new malicious computer programs identified each day.¹³ This past June, the computer security firm Symantec released a report on a Trojan Horse¹⁴ program dubbed “Sykipot”.¹⁵ “The Sykipot attackers have a long running history of attacks against multiple industries. Based on these insights, the attackers are familiar with the Chinese language and are using computer resources in China. They are clearly a group of attackers who are constantly modifying their creation to utilize new vulnerabilities and to evade security products and we expect that they will continue their attacks in the future.” Symantec noted.

In the past several years, there has been a growing list of complex computer breaches that highlight the wide array of threats:

- The high-profile intrusions of Google’s Gmail in 2009 also targeted as many as 30 other high-tech companies including Yahoo, Adobe, Rackspace and Northrop Grumman. US officials believe China was attempting to gain access to these firms’ networks to obtain intellectual property and source code information.
- China is also believed to have hacked into computer systems run by \NASDAQ-OMX, the parent company of the NASDAQ stock exchange, and to have executed an intrusion last year into computers at the International Monetary Fund.
- Last year RSA, the security division of the EMC Corp., suffered a breach of the firm’s intellectual property, SecureID, which provides encrypted authentication services to defence contractors and the US government, including the FBI. Officials say Chinese entities compromised the RSA

¹³ Ryan, Jason. “FBI Director Says Cyber Crime will Surpass Threat from Terrorists”, January 31, 2012, available at <http://abcnews.go.com/blogs/politics/2012/01/fbi-director-says-cyberthreat-will-surpass-threat-from-terrorists/>

¹⁴ Trojan Horse: A standalone malicious program designed to give full control of an infected personal computer to another computer.

¹⁵ http://www.net-security.org/malware_news.pld?id=1975

Secure ID system to try to break into computers used by defence contractor Lockheed Martin.

- In 2007, Russia waged cyber-attacks against computer systems in Estonia and United States (US) officials have also cited Russia using cyber-capabilities in the conflict between Russia and Georgia in 2008.
- Non-state entities, such as Anonymous, a loose coalition of web-based “hacktivists”, have wreaked havoc recently with distributed denial of service attacks against the websites of the US Justice department, Universal Music, the Motion Picture Association of America, the Recording Industry Association of America and the FBI. Anonymous also has conducted sophisticated intrusions, breaching the computer systems of government contractor HB Gary, a cyber security firm, in early 2011. In that incident, they downloaded more than 50,000 emails from the firm and posted private information about the CEO on his own Twitter account.
- Canada’s Public Safety Minister, Vic Toews, was the latest in a string of public-policy targets to feel the wrath of Anonymous, who went after the minister for his approach in promoting the Government’s online surveillance bill.¹⁶

Impact on Canada

Nearly two thirds (63%) of Canadian users reported having experienced a computer virus at one point in the past. Of those who had experienced a virus, almost one half (49%) said that the virus (or viruses) resulted in the loss of information or damage to software.¹⁷

¹⁶ National Post Staff, “Anonymous revives Wikileaks, targets Vic Toews over online surveillance bill” <http://news.nationalpost.com/2012/02/20/vic-toews-anonymous-hackers/>

¹⁷ Statistics Canada, “Individual Internet use and E-commerce”, Wednesday, October 12, 2011, available at <http://www.statcan.gc.ca/daily-quotidien/111012/dq111012a-eng.htm>

Over one third (37%) said they had received emails requesting personal information (such as bank account numbers or passwords) from a fraudulent source.¹⁸

These numbers are not surprising in that hacking isn't rocket science and needn't cost a fortune. An off the shelf desktop computer can test anywhere between one and fifteen million passwords per second. It would crack a password from a dictionary in less than 1 minute. A strong random password could be cracked in less than 15 minutes. The same computer, in combination with an off the shelf graphics processor can speed up the cracking process by a factor of 50 to 100.¹⁹

The threat issue is compounded by the fact that Canadians, despite being enthusiastic users of the technology, typically know very little about the Internet. The Canadian Internet Registration Authority released a report this past November entitled "The Internet and Canada's Future Opportunities and challenges". Some of the published results are revealing:

- 32% of Canadians could not identify a challenge faced by individual users of the internet;
- 18% claimed there are no challenges;
- among the clever half, 9% cited a lack of digital literacy and 7% cited slow Internet connection speed.²⁰

Compared to counterparts in the US and the United Kingdom (UK), Canadians demonstrate a greater willingness to publish and share their personal details and stories online. As an example, the National Director of Facebook Canada this year produced statistics on uptake in our country: nearly half of all Canadians actively participate on Facebook.²¹ It is no wonder, then, that Canada's Privacy Commissioner has been keenly

¹⁸ Ibid.

¹⁹ Password Cracking Wikipedia, available at http://en.wikipedia.org/wiki/Password_cracking

²⁰ Thomas, Knowlton. "Half of Canadians Don't Have a Clue About the Internet" November 10 2011, available at <http://www.techvibes.com/blog/half-of-canadians-dont-have-a-clue-about-the-internet-2011-11-10>

²¹ Breikss, Chris. "Mind Blowing Canadian Facebook Usage Statistics", May 3, 2011, available at <http://www.6smarketing.com/canadian-facebook-statistics>

interested in Facebook's privacy practices and has effectively challenged the popular giant on its compliance with Canadian law.²²

Yet basic security is not uppermost in the minds of most Canadian Internet users. Speaking of IT security more generally, most Canadians only change their passwords every 2-5 years. Up to 30% report that they never change their passwords.²³

Furthermore, in general, only 25% of smartphone owners use the auto-lock feature to protect their mobile devices. Less than 10% of people currently using their own tablets for work have "auto-locking" enabled. Barely 30% of lap top owners use the "auto-locking" feature.²⁴

Security firm Sophos has warned that malware writers and cyber criminals will switch their focus to the now more popular smartphones. While such attacks will target all smartphone operating systems, Android – which is becoming increasingly popular – is particularly vulnerable because of the way patches are distributed.

"Google will issue patches for vulnerabilities to network providers, who will decide when to make it available to users," said Mark Harris, global director of Sophos Labs.

"Many of those users won't be accustomed to patching their systems, which could mean an awful lot of users running versions that contain vulnerabilities," he added.²⁵

So we have a rich target with robust attackers using readily available commercial off-the-shelf products and having considerable success in taking advantage of the target. Consider the following, between 2010 and 2011:

²² Office of the Privacy Commissioner, News Release, "Facebook shows improvement in some areas, but should be more proactive on privacy when introducing new features", April 4, 2012, available at <http://www.priv.gc.ca>

²³ <http://www.symantec.com/region/can/eng/press/200>

²⁴ King, Rachel. "Most smartphone, tablet owners not concerned with locking devices: report", zdnet, March 26, 2012, available at <http://www.zdnet.com/blog/btl/most-smartphone-tablet-owners-not-concerned-with-locking-devices:report>

²⁵ Morgan, Gareth. "SOPHOS warns of rising Android malware threats in 2012", vs.co.uk, January 26, 2-12, available at <http://www.v3.co.uk/v3-uk/news/2141640/sophos-warns-rising-android-malware-threats-2012>

- There were 286 million unique variants of malware that exposed and potentially exfiltrated our personal, confidential, and proprietary data;
- Each data breach exposed, on average, 260,000 identities;
- There was a 93% increase in web-based attacks (compromised/hijacked websites where the visitor would become infected);
- The underground economy paid anywhere from \$.07 to \$100 for each of our stolen credit card numbers;
- Realizing that mobile payments and mobile platforms (e.g., smart phones and iPads) would be the newest vector of technology adoption, there was a 42% increase in mobile-operating-system vulnerabilities and subsequent exploitation.²⁶

An issue that warrants a few words is the idea of the Internet as a “force multiplier”.²⁷ It is, in fact, an excellent force multiplier. There is virtually no personal, physical risk incurred by an Internet attacker. There are no geo-spatial boundaries on the Internet, nor are there behavioural rules. There are no threats to the attacker who can use unpredictable techniques and is very difficult to find as he/she hides in plain sight among billions of users. The attacker is also able to recognize when their practices and techniques have been compromised and regularly change these to avoid detection.(Recall the “Sykjpot” Trojan Horse referred to earlier.) An individual could simply run a program from his/her home computer that could cause extensive interruption or damage to the computer systems that our governments increasingly rely on.

It is important to understand that cyber- attack’s ability to do harm is not limited to damaging electronic information. For example, there are some power distribution control rooms that run supervisory control and data acquisition (SCADA) systems. Rather than have an engineer on site, operating engineers can log in via the Internet to do their work remotely. The danger here is that a “hacker” may break into a SCADA

²⁶ Symantec Internet Security Threat Report: Trends for 2010, Volume 16, April 2011.

²⁷ Force Multiplier; Refers to an attribute or a combination of attributes which makes a given force more effective than that same force would be without it.

system and use it to damage, destroy or cripple the power distribution of a potentially large area. This represents a very real risk to critical infrastructure.

The Government of Canada (GOC) has not been spared. What has been seen more and more in recent years, particularly through the lens of our national cryptographic agency, the Communications Security Establishment Canada (CSEC), are attempts at cyber espionage and the presence of malicious emails on GOC networks.

Acts of espionage to clandestinely access the secrets of others is nothing new. The use of spies or various forms of intelligence to access a state's political, military and economic secrets or a company's industrial and business secrets have been practiced since time immemorial. Cyber-espionage is ultimately the same as traditional espionage: the covert access of information of national interest belonging to others, only accessed electronically.

The threat to Canada's security, and to the security of our allies, is much greater than it might appear to be at first glance. More than 100 countries are capable of conducting cyber operations against technologically advanced countries such as Canada. The attempts are constant and relentless. Many countries are prolific, unconstrained by resource, legal, or policy limitations. With our advanced economy, connected government services, important international role and our proximity to the United States, Canada is an extremely attractive target. And as we experienced in January/February 2011 in the case of Treasury Board and the Department of Finance, undetected compromises can be both expensive and time consuming to address, to say nothing of lost productivity in the meantime.

The potential for harm to our way of life through the exploitation of the Internet is boundless. States, organized crime, terrorists, and individuals use the Internet for a range of illegal activities. They attempt to steal our industrial and national security secrets and our personal identities and they work relentlessly to penetrate our critical infrastructure networks, potentially disrupting our daily lives and forcing us into costly clean up.

And the implications do not stop there. They could lead to our closest allies questioning whether we are the weakest link to their own information infrastructures.

The compounded impact of these activities is a very real threat to the sovereignty of our nation on the cyber front.

Government of Canada Approach

The GOC has a critical and unique role. It is responsible for the defence of Canada's physical and economic security, in addition to being the guardian of sensitive national security, economic and personal information. It must therefore lay the foundation upon which Canada's defence of its cyber livelihood will be built.

But the GOC cannot do this alone. They do not control all things critical to national security. For example, other levels of government and industry control approximately 85% of Canada's critical infrastructure²⁸, providing energy, and water and essential services such as police, medical care, financial services and air traffic control. They also store sensitive personal and economic information.

National security and critical infrastructure are not the only concerns. As has been made clear above, large commercial organizations are prime targets for cyber attacks. And our adversaries, be they state actors, criminals or non-state actors, have aggressively targeted them, thereby threatening our economic prosperity.

The GOC has devised a cyber strategy²⁹ that will provide the leadership and guidance that will ensure a coordinated approach, both domestically and internationally, to all aspects of cyber security.

The three pillars of the strategy are founded on:

- securing government systems;
- partnering to secure vital systems outside the GoC; and
- helping Canadians to be safe online (public awareness).

²⁸ Canada's Critical Infrastructure: When is safe enough safe enough? Andrew Graham. The MacDonald Laurier Institute, National Security Strategy for Canada Series, Volume 2

²⁹ Public Safety Canada, Canada's Cyber Security Strategy, available at <http://www.publicsafety.gc.ca/prg/ns/cbr/ccss-scc-eng.aspx>

Security

Clarity of roles and responsibilities is the first intent of the Strategy. It is a whole of Government approach and it is a complex web. Public Safety Canada will provide central coordination for assessing emerging complex threats and developing and promoting comprehensive and coordinated approaches to address risks within the GOC and across Canada.

An indication of the evolving breadth and complexity of GoC roles and responsibilities can be drawn from both the Cyber Security Strategy and the IMP, with the latter reflected in Annex A.

Any discussion of securing government systems must start with the Communications Security Establishment Canada (CSEC). Their mandate, *inter alia*, states that the CSEC is:

to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructure of importance to the Government of Canada.³⁰

CSEC's technical knowledge and capacity to fulfill this mandate is assisted by the fact that they are also mandated:

"to acquire and use information from the global information infrastructure (GII) for the purposes of providing foreign intelligence, in accordance with Government of Canada intelligence priorities."³¹

While an aside, it is important to note that CSEC's multi-faceted mandate is bound by a robust authorities framework, designed to maintain focus on GOC priorities while taking measures to protect the privacy of Canadians. Further, these unique activities are subject to review for lawfulness by the CSE Commissioner³².

I highlight these particular responsibilities because the second compliments the first, and this combination gives CSEC a distinct advantage in its challenge to help

³⁰ Canada's National Defence Act (NDA) Part V.1 273.64(1)(b), available at <http://laws.justice.gc.ca/eng/acts/N-5/page-100.html#docCont>

³¹ *Ibid.* Part V.1 273.64(1)(a).

³² *Ibid.* Part V.1 273.63(2)(a).

secure GOC networks. This is an advantage also enjoyed by Canada's Five Eyes partners (US, UK, Australia and New Zealand). I will speak of this partnership later.

Working in the GII to acquire the signals intelligence in support of GOC policy priorities³³ enables CSEC to anticipate and understand the capabilities of foreign state sponsored threat actors, enabling the crafting of a defence well before they reach the GOC networks. This technical know-how is mirrored in and leveraged by the Information Technology Security staff³⁴, who applies similar skillsets closer to home, on the perimeter of the GOC networks. These combined capabilities enable CSEC to see the threat coming and to prevent it from reaching its potential victims on the GOC's systems. By leveraging classified signals intelligence data, CSEC can recognize foreign intrusions that are undetected by commercial technologies.

Leveraging the knowledge and capabilities of the Five Eyes partners, who are doing the same things for their systems, enlarges the database of exploiters and their tradecraft such that the partnership can collaborate on defences and mitigation methodologies.

But this challenge is a complex one, as even one of the best-resourced cryptographic agencies in the world would attest. General Keith Alexander, Commander, United States Cyber Command/Director, National Security Agency/Chief, Central Security Service, in speaking at the International Conference on Cyber Security sponsored by the Federal Bureau of Investigation this past January, told the conference that the Pentagon's complete infrastructure is too chaotic and archaic to be successfully defended from cyber-espionage, cyber-terrorism or cyber-warfare assault. He went on to say that the National Security Agency (NSA) "can't see them all (interconnected networks) [let alone] defend them all."³⁵

The GOC has a patchwork of networks of unique architecture and configurations such that the same threat in each network requires a unique mitigation approach. If this

³³ Ibid. PartV.1 273.64(1)(a).

³⁴ Ibid. PartV.1 273.64(1)(b).

³⁵ Fitsanakis, Joseph. "US Pentagon computers cannot be protected, says NSA head", January 13, 2012, available at <http://intelnews.org/?s=International+Joseph+Fital+Cyber+Security+Conference+>

isn't indefensible, it is very close to it. Shared Services Canada, the Treasury Board and Public Works Government Services Canada, among others, are working to consolidate and streamline the delivery of GOC information and technological services thereby improving its defensibility.

The new system will be designed such that security will be enhanced by built in redundancies and resiliencies. This effort will be further leveraged by a profound reduction, hopefully from thousands down to hundreds, in the number of GOC network connections to the Internet.

It must, however, be stressed that the threat, as has been highlighted earlier, is growing unhindered by resource concerns or legal and policy constraints. The same cannot be said for the defenders, who are constrained by resources, and legal and policy issues. None of these limitations are impossible, however, the current fiscal reality will limit how much can be done quickly. This combined with the challenge of finding properly qualified Canadians motivated to work in the field of cyber security will be a limitation.

Nevertheless, CSEC's legislation does give Canada an advantage over our neighbours to the south. I return to the B Mandate as written in the legislation: "... to help ensure the protection of electronic information infrastructures of importance to the Government of Canada;"³⁶

It is noteworthy that the scope of CSEC's mandate is not limited to military networks or even government networks. It has the legislative authority to protect/defend any information or information infrastructures of importance to the Government of Canada. Its focus, at this point in time, is Government of Canada systems but critical infrastructure could be included were the Government of Canada to so decree and should resources permit.

In the US the responsibility for government systems is shared. The NSA is responsible for Department of Defense systems (.mil) and the Department of Homeland Security (DHS) for the rest of government (.gov). The matter of responsibility for critical infrastructure is before Congress and has not yet been resolved. The NSA is currently

³⁶ (36) NDA, Op. cit., PartV.1 273.64(1)(b).

the only US organization with the capabilities and monitoring infrastructure to protect US information infrastructure. Partnering with the DHS is an option but is it the optimal solution?³⁷

Partnering

Critical infrastructure, much of which is controlled by Internet-connected systems and susceptible to cyber-attack, is high on the Canadian list of national security concerns. Accordingly, the GOC must do more with the provinces, the private sector and non-governmental agencies, who own and operate 85% of the critical infrastructure, if they are to address this matter. Canada’s National Plan for Critical Infrastructure³⁸, in conjunction with the Action Plan for Critical Infrastructure³⁹, is intended to meet this need.

The intent is to substantially expand the GOC’s engagement activities with the ten critical infrastructure sectors. The relatively newly created Canadian Security Telecommunications Advisory Council was the first of the National Cross-Sector Fora intended to promote collaboration across the sector networks, address interdependencies and promote information sharing across sectors.

Comparable fora have been, or soon will be, created for the other nine sectors listed below. Opposite each is the GOC lead.⁴⁰

Sector	Federal Lead
Energy and Utilities	NRC
Finance	Finance Canada

³⁷ [Gorman, Siobhan. “NSA Chief Seeks Bigger Cyber Security Role”-WSJ.com, available at http://jamadots.olhblogspace.com/?tag=keith-alexander](http://jamadots.olhblogspace.com/?tag=keith-alexander)

³⁸ Public Safety Canada, Canada’s National Strategy for Critical Infrastructure, 2011, available at <http://www.publicsafety.gc.ca/prg/ns/ci/ntnl-eng.aspx>

³⁹ Public Safety Canada, Canada’s Action Plan for Critical infrastructure, 2011, available at <http://www.publicsafety.gc.ca/prg/ns/ci/ct-pln-eng.aspx>

⁴⁰ Ibid.

Health	Public Health
Water	Environment Canada
Transportation	Transport Canada
Safety	Public Safety Canada
Manufacturing	Industry Canada
Government	Public Safety
Food	Agriculture and Agri-Food Canada

Further partnering initiatives include Public Safety Canada (PS) initiating ongoing dialogue on strategic cyber security issues with provincial and territorial interlocutors. PS has also reoriented the mandate of their Canadian Cyber Incident Response Centre⁴¹ to focus on national issues and on supporting the provinces, territories and industry. At the same time, PS has transferred the GOC incident response coordination to CSEC.

Public Awareness

PS has taken the lead for the third pillar with a national awareness campaign to provide Canadians with information on cyber threats in order for them to protect themselves and their personal information online.

More needs to be done in this regard. The GOC must reach out to the business community and work with them based on a layered approach to security. Vince Plaza,

⁴¹ CCIRC's Former Role: responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to any cyber security incident. Its focus is the protection of national critical infrastructure against cyber attacks.

Vice President Information Technology at Team Logic IT, offers the following advice that could certainly be the basis of an approach.

- Protecting the internal network, at the external level: Having hosted anti-spam and/or hosted email services will protect against most, if not all, email borne threats.
- Protecting the gateway layer: One of the most vulnerable spots in a network is the point at which the company connects to the Internet. An up-to-date security appliance with gateway anti-virus and web content filtering is absolutely necessary to curbing threats to the Internet.
- Protecting the end-point, the computer: Downloading and keeping spyware and anti-virus software up-to-date on all in-network computers will minimize risk. In addition, proper risk management is critical. Finally, password management must be enforced.
- Vulnerability and penetration testing: You only know how secure you are if you test.
- Vendor diversity: Diversify security tasks. If one vendor doesn't have the necessary tools, in all likelihood someone else will.
- Training, training, training: Regular employee training is absolutely essential for the security health of any network. Annual or bi-annual practices will pay for themselves many times over.⁴²

The Canadian Forces and Cyber Security

Consistent with the current policy within the GOC for all departments, the Department of National Defence (DND) and the Canadian Forces (CF) are responsible for all aspects of securing their own systems. Furthermore, they are responsible for the provision of defence intelligence to inform the GOC threat and risk assessment process.

⁴² Savitz, Eric. "6 Ways to Protect Any Size Business fro Cyber Threats, Forbes, 26 Jan, 2012 , available at <http://www.forbes.com/sites/ciocentral/2012/01/26/6-ways-to-protect-any-size-business-from-cyber-threats>

They provide cyber security information from military allied sources, in-theatre monitoring and reporting on technical information technology threats and providing options analysis for potential military responses.⁴³

In the wake of Canada's Cyber Strategy, DND and the CF are currently analyzing the cyber challenge from their own perspective and with the functions of other community stakeholders in view. This thinking will assist the Department in effectively organizing its approach, prioritizing its needed partnerships and external dependencies, and articulating their contribution to cyber security.

A partnered approach between the cryptographic and defence organizations appears to be a logical approach and potential model for Canada. For example, the US Department of Defense (DOD) partnered similarly with the NSA to take advantage of the NSA's unique Signals Intelligence/Information Assurance platform.

Within Canada, the CSEC is the only organization capable of the full spectrum of cyber network operations (CNO).⁴⁴ It would be prohibitively expensive, if even logistically possible, for another government department to duplicate the full spectrum of CSEC capabilities in CNO. Aside from the complexity of the cryptographic infrastructure required, subject matter experts would not likely be available in sufficient numbers in our country to consider staffing a second agency.

A promising option from the perspective of efficiencies and appropriate authorities would be to enable the CF to leverage CSEC's capabilities and platform.

While certainly not the only possible approach, this option does efficiently leverage the GOC's current capabilities and it can learn from and build upon the US's experience in a manner tailored to the unique Canadian reality.

⁴³ Cyber Security Strategy, Op. cit.

⁴⁴ Computer Network Operations (Government of Canada terminology): CNO comprises three categories of activity;

- Exploitation or Signals intelligence within CSEC, for intelligence gathering purposes;
- Defence or Information Technology Security within CSEC, defending the GOC or critical infrastructure;
- Attack or Cyber Warfare, as part of modern military operations.

The International Scene

Dr. Paul Cornish, Professor of International Security at the University of Bath, suggests that, "Technological strength and superiority has, unfairly though it might seem to its originators and beneficiaries, prompted what military analysts would describe as 'asymmetric vulnerability', where a fleet-footed and sharp-witted adversary can manoeuvre so fast and decisively that the strongest and most elaborate defences are turned into a cumbersome liability and a disadvantage."⁴⁵

Is the situation we find ourselves in beyond the capacity of the 'nation state' to deal with? Is it a strategic liability that demands a co-operative approach among nation states?

The initial attempt to such an approach was the two-day conference of early November 2011, hosted by UK Foreign Secretary William Hague. Although the goal of the conference was initially billed as a major advance in an urgent quest for a 'treaty' to govern international conduct on the Internet, it finally settled on the goal of non-binding norms, which would set out the broad "rules of the road" for interactions in cyberspace. The hope is that such an approach would promote safe, predictable and consistent interactions while ensuring the Internet's accessibility and openness. The idea would be to seek support for the concept that existing principles of international law (e.g. human rights law, the law of armed conflict) apply equally in cyberspace.

Mr. Hague, supported by the US and Canada among others, pushed the concept forward but China and Russia would not be moved from their preference for a cyber-arms control regime set up by the UN.

One could surmise, that it is the difference between information security and cyber security that may underpin the conceptual impasse between Russia, China and the Western nations in cyberspace. Cyber security, the preferred focus of Western countries, centers on the technical security of hardware, software, data and its transmission. Information security includes all aspects of cyber security but also delves

⁴⁵ Cornish, Paul. "The Vulnerabilities of Developed States to Economic Cyber Warfare", Working Paper, June 2011, available at <http://www.chathamhouse.org.uk>

into the content of cyber data – usually for the purposes of censorship. The Chair addressed this issue head on in his concluding remarks.

“The fourth message is that, while working together to defeat threats in cyberspace, you should not imagine for an instant that you can resist the growing force of the tide now flowing for transparency, open information, and the free exchange of ideas. Those Governments that try to do so are in my view certain to fail.”⁴⁶

Even if “non-binding rules of the road” could be agreed to, one wonders if signatories would eventually be tempted to design a corresponding range of punitive actions. Were that to be entertained, it is unclear how such action would be instigated or endorsed, and what court of higher appeal would exist to ensure just and proportionate action.

Much work remains to be done in these matters, and discussion will continue to pursue a way forward. Hungary and Korea accepted to host the next iterations of the conference in 2012 and 2013 respectively.

In the meantime, Melissa Hathaway, President of Hathaway Global strategies LLC and special advisor of Harvard Kennedy School’s Belfer Center, and John Savage, the An Wang Professor of Computer Sciences at Brown University, suggest that nations pursue the thought that ISPs must accept additional responsibilities such that they ensure the reliable delivery of an essential service, such as the Internet.

They argue that the gap between written and implied responsibilities for ISPs needs to be closed such that they become explicit duties. They define eight ISP duties:

- Duty to provide a reliable and accessible conduit for traffic and services;
- Duty to provide authentic and authoritative routing information;
- Duty to provide authentic and authoritative naming information;
- Duty to report anonymized security incident statistics to the public;
- Duty to educate customers about threats;

⁴⁶ London Conference on Cyberspace, Closing Press Conference, Foreign Secretary William Hague, November 2, 2011, available at <http://www.fco.gov.uk/en/news/latest-news/?view=PressS&id=685663282>

- Duty to inform customers of apparent infections in their infrastructure;
- Duty to warn other ISPs of imminent danger and help in emergencies;
- Duty to avoid aiding and abetting criminal activity.⁴⁷

Is Canada Doing Enough?

A new benchmarking of 19 of the world's leading economies (G20 – EU) which ranked countries in their ability to withstand cyber attacks and to deploy the digital infrastructure necessary for a productive and secure economy, the Cyber Power Index, is one measure. Each country's ranking is a weighted mean of scores from four categories: legal and regulatory environment, economic and social context, technology infrastructure and industry application.

The study concluded that the top five countries exhibiting cyber power, as measured by the index – the UK; the US; Australia; Germany and Canada – illustrate that developed Western countries are leading the way into the digital era. The top five performers rated highly across the board, ranking in the top seven in all four categories⁴⁸.

Conclusion

Computers and information systems are an integrated component of Canadians daily lives. They are an essential service to our social lives, our commercial and industrial activity and they are our interface with our governments. And Canadians are among the world's leaders in embracing cyber technology and the advantages it offers. At the same time, we have not been as enthusiastic in understanding its vulnerabilities and embracing secure operating procedures. This combination of factors leaves us ripe for exploitation.

⁴⁷ Hathaway, Melissa E. and John E. Savage, Stewardship of Cyberspace Duties for Internet Service Providers, March, 2012, available at <http://belfercenter.ksg.harvard.edu/files/cyberdialogue2012-hathaway-savage.pdf>

⁴⁸ (48) Booz/Allen/Hamilton, "The Cyber Hub", available at <http://www.cyberhub.com>

And exploitation comes from a multitude of sources; states, organized crime, criminals, pedophiles, hacktivists, terrorists and adventurers/joy seekers. And they attack indiscriminately. We are vulnerable as individuals, as organizations/associations, as businesses and as governments. All of have a part to play in addressing this challenge to what is a fundamental part of a modern society.

We have a responsibility to understand the technology and its vulnerabilities, we have a responsibility to understand the threat and its impact on our way of life, we have a responsibility to do our part as individuals, as businessmen and business women and as citizens to address this challenge to what is precious to us.

As citizens we must press our governments; municipal, provincial and federal to ensure that they lay the foundation upon which a 'whole of country' cyber security effort can be built.

That foundation has its beginnings at the federal level. Canada's Cyber Security Strategy is the Federal Government's action plan to secure cyberspace for Canadians. The start point has to be the security of Government systems. At all levels, there is evidence that governments' ability to deliver services could be threatened by attacks on the supporting IT infrastructure.

The strategy calls for a 'whole of government' approach to achieve the level of security required to assure Canadians that the Government can effectively serve Canadians and safeguard their personal data while so doing. The effort is broad based but has its beginnings in further enabling the CSEC's unique cryptographic capabilities and global partnerships to address the sophisticated (state sponsored) cyber threat.

This effort will need to be implemented through the efforts of numerous other departments and agencies, including but certainly not limited to, those departments and agencies who are key to designing and assembling a federal government network that is more easily defensible.

At the same time the GOC has the lead in partnering with other levels of government and the private sector to strengthen Canada's cyber resiliency, including that of its critical infrastructure.

Finally the GOC is responsible for negotiations at the international level. An international resolution in the form of a treaty or a 'rules of the road' approach may well be needed, regardless of what we are able to accomplish domestically.

Industry, for its part, must accept that security is essential for the long term health of its relationship with its clients. In this regard, the ISPs could set a positive example by closing the gap between regulated responsibilities and the unwritten, yet expected ones. Should this not happen, nations may need to impose this approach through legislation and regulation.

All businesses can improve security through four actions on a consistent basis: a layered approach to security; that is, protecting at the external to network level, protecting at the level of the gateway and at the end point, the computer and wherever information is held/stored. This in combination with regular testing of defences, vendor diversity and training will vastly improve on the current reality.

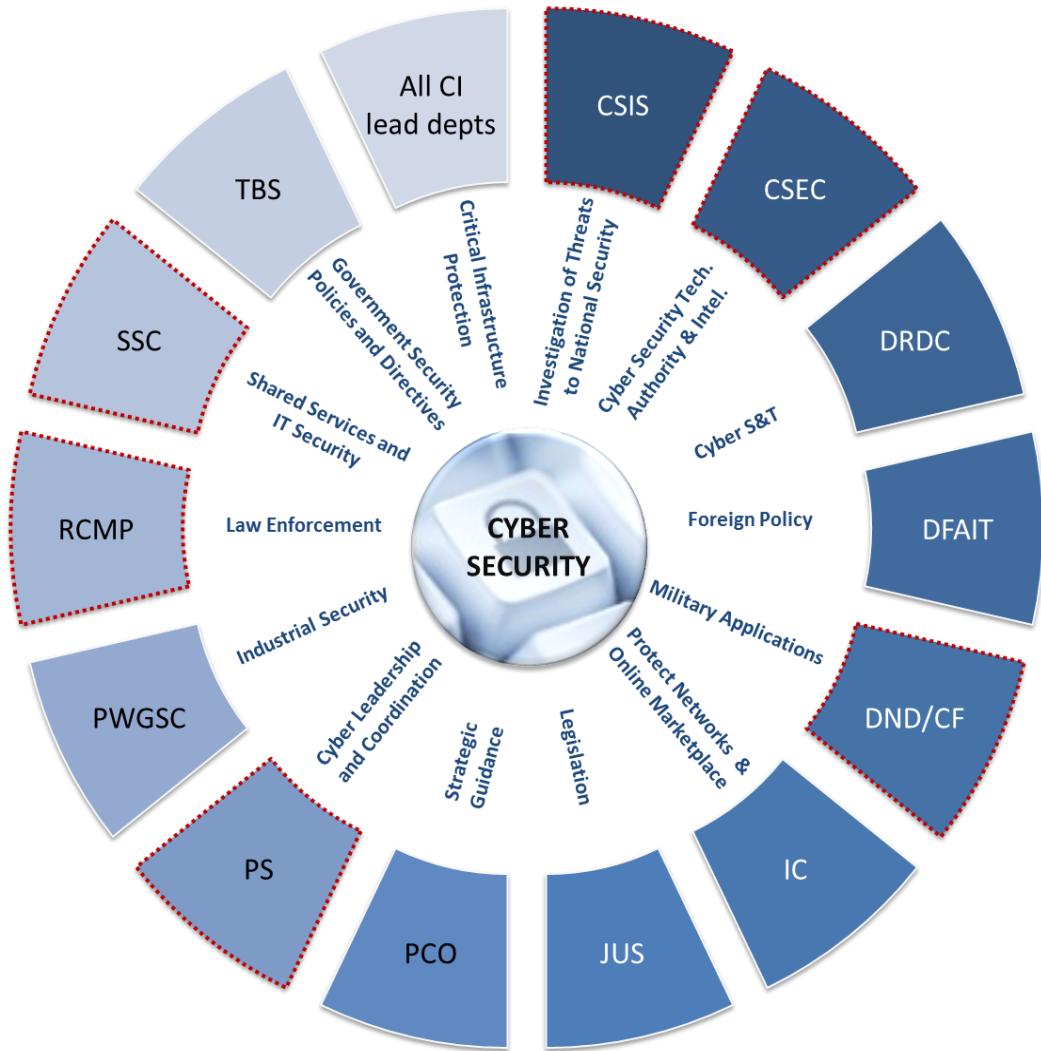
As individual users, two simple improvements will address up to 80% of the compromises; strong passwords changed regularly and prompt patching/updating of software. As well, citizens must reconcile the ease and comfort with which they live online with the need to defend against cyber threat. A populace that arms itself against even small-scale attacks helps its government to project a secure cyber front thereby encouraging the average attacker to seek out softer targets elsewhere.

The cyber world in which Canadians live, work and play lacks the regimes of law and order that govern our physical world. The long-term objective for cyberspace must be to foster an environment where online threats are known and managed to the greatest extent possible. Achieving this will require sustained and coordinated collective action and investment by the federal Government, its international allies, industry, academe and individual Canadians. It must be a team effort.

The Government of Canada and Cyber Security:

Security Begins at Home – Annex A

Roles and responsibilities with respect to cyber security



Departments outlined in red dotted line play a role in the *Government of Canada IT Incident Management Plan*

UNCLASSIFIED

All critical infrastructure lead departments

Includes Finance Canada, Environment Canada, Health Canada, Transport Canada, Natural Resources Canada, Agriculture and Agri-Food Canada, and Public Safety Canada.

Treasury Board of Canada Secretariat

Establishes and oversees a whole-of-government approach to cyber security, including: setting government-wide direction and establishing priorities for securing government IT systems and networks; providing direction and advice to lead security agencies on the approach and implementation of measures for managing IT security incidents; and providing oversight of IT incident management, including post-mortem reviews and lessons learned.

Shared Services Canada

Streamlines and consolidates ICTs in the areas of email, data centres and networks, and for ensuring the confidentiality, integrity and availability of common IT services provided to departments.

Provides common information technology (IT) security services and other solutions to enable departments to exchange information with citizens, businesses and employees.

Gathers, analyzes, consolidates and facilitates the sharing of operational threat and vulnerability information related to common IT services and Government IT critical infrastructure managed by Shared Services Canada, and communicates the information to the Canadian Cyber Incident Response Centre and, as authorized, to departments and cyber security partners.

Royal Canadian Mounted Police

Leads the criminal investigative response to suspected criminal cyber incidents involving critical information infrastructure (i.e., unauthorized use of computer and mischief in relation to data). Leads the investigative response to suspected criminal national security cyber incidents.

Assists domestic and international partners with advice and guidance on cyber crime threats.

Public Works and Government Services Canada

Provider of shared and common services. As part of its Industrial Security Program activity, ensures security in contracts awarded by the Department or when requested by other Government departments.

Ensures the protection of foreign and NATO classified information within the private sector in Canada.

The Industrial Security Sector maintains relationships with allies and negotiates Memoranda of Understanding on industrial security matters, including cyber security, in contracting.

Public Safety Canada

Leads and coordinates the implementation of *Canada's Cyber Security Strategy*, including the design of a whole-of-Government approach to performance measurement and reporting; engagement with provinces and territories, critical infrastructure, and international allies on strategic cyber security policy issues and national cyber incident management; and public awareness activities to inform Canadians of the risks they face and the actions they can take to protect themselves and their families in cyberspace.

The Canadian Cyber Incident Response Centre acts as Canada's national CERT (Computer Emergency Response Team) in providing assistance and mitigation advice to domestic partners and coordinating the national response to any cyber security incident.

Privy Council Office

Houses and provides support to the National Security Advisor to the Prime Minister.

Coordinates activities among members of the Canadian security and intelligence community, and promotes a coordinated and integrated approach to national security issues.

Communications Security Establishment Canada

Monitors and defends Government of Canada networks by detecting, discovering and responding to sophisticated cyber threats to the Government, and provides mitigation and/or recovery advice and/or guidance to Government departments to help them recover from cyber incidents.

Government of Canada's cryptologic agency responsible for the collection of cyber foreign intelligence and Canada's interface with the Five Eyes cryptologic community. Undertakes classified research and development for cyber security.

Canadian Security Intelligence Service

Conducts national security investigations. Reports to and advises the Government of Canada of activities constituting a threat to the security of Canada as defined in the *Canadian Security Intelligence Service Act*.

Provides analysis to assist the Government of Canada in understanding cyber threats, and the intentions and capabilities of cyber actors operating in Canada and abroad who pose a threat to the security of Canada. This intelligence enables the Government of Canada to improve its overall situational awareness, better identify cyber vulnerabilities, prevent cyber espionage or other cyber threat activity, and take action to secure critical infrastructure.

Defence Research and Development Canada

Leads the development of military cyber security S&T in support of the Canadian Forces.

Leads domestic Public Safety Canada cyber security S&T efforts not specifically assigned to another department or agency through the Centre for Security Science and with domestic security partners in the Public Security Technical Program.

This is delivered in partnership between Government, industry, academia and allies.

Department of Foreign Affairs and International Trade

Supports international bodies in mitigating cyber threats and assisting foreign governments in improving their cyber security profile and capabilities.

Contributes to diplomatic engagement in order to help shape the multilateral regulatory space that is emerging with respect to cyber security. Enables the Government to better position Canada on the international stage to defend and promote its foreign policy and cyber security-related interests.

Department of National Defence / Canadian Forces

Responsible for the provision of defence intelligence to inform the Government of Canada threat and risk assessment process.

Contributes to Government situational awareness during the monitoring and analysis, mitigation, and response phases of the *GC IT IMP* by providing cyber security information from military allied sources, monitoring and reporting on technological IT threats, and providing options analysis for potential military response.

Industry Canada

Responsible for spectrum management in Canada and for fostering a robust and reliable telecommunications system. Develops policies to ensure a safe and secure online marketplace. Helps to ensure the continuity of telecommunications during an emergency.

Department of Justice Canada

Supports initiatives of client departments and agencies through the provision of legal advice on matters relating to cyber policy and law.

In respect of certain matters, especially those relating to criminal law policy and information sharing, Justice plays a leading role. Departmental Legal Services within the Communications Security Establishment Canada had been designated as the centre of excellence on cyber-related legislation.

Departments outlined in red dotted line play a role in the *Government of Canada IT Incident Management Plan*