Volume 7 – Fall 2011
djim.management.dal.ca

E-Canada and Cyber-attacks: Peril and Policy

Craig MacEachern

Abstract: This paper examines the growing concern surrounding cyber-attacks and warns about the possible impacts of a cyber-attack upon Canadian e-government, economy, and infrastructure. This paper covers historical examples of cyber-attacks on a global scale, then focuses on Canadian e-government vulnerabilities, and suggests some ways in which the Canadian government must adapt its domestic security and Internet policies to confront the future inevitability of cyber-attacks.

About the Author(s): Craig MacEachern came tumbling up in the small mill town of Port Hawkesbury, Cape Breton. His interests lie in computer security, computer culture, and global politics. This paper was originally developed for INFO 5500: Information in Society. Craig is a first year Library and Information Studies student at Dalhousie, and currently works at Dalhousie's iLab as a Research Assistant.

E-Canada and the Emerging Cyber-attack Exigency

“Let's play Global Thermonuclear War”; this facetious remark introduced the concept of a cyber-attack to many film audiences in 1983, when the film *WarGames* was released (Internet Movie Database, 2010, para. 5). The Oscar-nominated movie portrays a young man who breaks into a U.S. military computer system and unknowingly nearly starts World War Three by arming and aiming nuclear weapons, all the while under the impression that he is playing a computer game. The movie’s tone is comic in places and carries that familiar sensationalistic 1980s Hollywood feel, although the subject matter is hinting at something more sinister. At the time of the movie's release, few if any moviegoers actually *owned* a personal computer, and the concept of a cyber-attack was largely unknown. The film preyed on the technological ignorance of its viewers to provoke a fear response and paranoia to a situation that most 2010 audiences would find implausible—or would they? In the last two years, cyber-attacks in Canada have doubled (Tibbetts, 2010). Since the release of *Wargames* in 1983, the digital landscape has changed tremendously. What once seemed like Hollywood science fiction is coming closer to being possible on the Internet in the 21st century. Cyber-attacks by organized groups or solo acts are increasing in frequency and in their potential to do real-world damage.

This paper will discuss the real rise of cyber-attacks in this new century, the so-called Information Age. We will explore cyber-terrorism and what, if anything, the threat means for Canada’s electronic governance and critical structure, which until recently has been sorely lacking a cohesive strategy for dealing with cyber-attacks. By drawing on contemporary Canadian and foreign examples of cyber-security breaches, Canada’s vulnerabilities will be shown and solutions to these threats will be suggested. The paper argues for a proactive approach to dealing with cyber-attacks that involves making resilient computing systems a top priority, and suggests some further government security and policy guidelines for dealing with cyber-attacks.

Defining the Threat

The first step in developing an appropriate approach to cyber-attacks is to further define them, followed by analyzing their strengths and weaknesses. In analyzing cyber-attacks, it is first necessary to disambiguate and demystify the concept. “Cyber-attack” is an umbrella term for several types of cyber-related activities, each of which has different motivating factors. “Hacktivism,” for example, is a cyber-attack motivated by political activism that often involves defacing a website for the explicit purpose of publicly shaming the target; “cyber-crime” may involve using cyber-attack as a means, but its sole motivation is to gain financially from the attack (i.e., using a cyber-attack to steal credit card information); and “cyber-espionage” involves an individual or team using various cyber-attack methods to capture sensitive foreign government information and plans, backed by a foreign state, and done by an individual or team. All of these forms of cyber-attacks are performed by what has been known popularly since the 1980s as a computer “hacker” or “hackers.” “Hacker” was originally used as a term of endearment and pride among individuals who loved programming and home-computing, and has origins as early as the 1970s at the Massachusetts Institute of Technology, but has since that time come to be better known to represent malicious individuals who break into computer systems (“Oxford English Dictionary,” 1989). Here, we will be using the term “hacker” strictly in the modern sense of the word, as representing someone who uses cyber-attacks as a means to achieve an end.

To understand what kind of hacker is a cyber-terrorist, it is first necessary to define what is a meant by a “terrorist.” Czinkota, Knight, Liesch and Steen (2005) reviewed and synthesized three different academic definitions of terrorism to conclude that 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, coercion, or intimidation of non-combatant persons or the general public” (p. 582). This definition loses no significance when it is transported into the digital realm, and will serve as our working definition of cyber-terrorism, with an addendum that “cyber” implies terrorism occurring through the Internet. Having defined the concept of cyber-terrorism, we must address and resolve the debate over whether the concept really is a threat to Canada, or if it is an exaggeration, so that we are not analyzing a paper tiger.

The Fact or Fiction Debate

There exists some debate in the literature and on the web about the extent of the real threat of a cyber-terrorist attack. Stohl (2007) argues that there is a lack of any real evidence for cyber-terrorism:

> The vast majority of these releases discuss the threat and precautions, investments and critical needs of the cyber sector. Rarely, do such releases call attention to the lack of actual cyber terror events, as opposed to, cyber crime, hacking or hoaxes and rarely do they inform the reader that the same type of threat and the same “crisis mode” of release appeared in each of the previous years since the early 1990s. (p. 225)

Stohl makes the important distinction, as we have, between cyber-terrorism and other forms of cyber-attacks, arguing quite rightly that there is often conflation between the terms. However, Stohl downplays the real threat of cyber-terrorism as little more than alarmist profiteering by Internet security firms, and by those with a vested interest in seeing money poured into cyber-security software and hardware out of fear (Stohl, 2007). This is a favourite tactic among what we will call the “denialists,” or those who would deny that the threat of cyber-terrorism has any teeth.

Another popular tactic among the denialist camp is to frame the issue as an underhanded political move by governments which secretly want totalitarian rule, and use cyber-terrorism threats as leverage to reduce privacy and freedom rights. This mindset is rampant among comments left on political blogs and news stories—browse a few comments posted in reply to any online cyber-terrorism news and you will understand the type of arguments this camp espouses. Perhaps the most clear and thoughtful argument coming from the denialist crowd, which we must always be cognizant of when developing a cyber-strategy, is that there is always the tendency that fear of terrorism will drive citizens to request excessive measures of their governments in a fit of overreaction (Sunstein, 2003, as cited in Czinkota et al., 2005).

As the year 2000 approached, Y2K fear was palpable in the media; however, fear quickly dematerialized when the clock struck 12:01am and January 1, 2000 arrived without disaster. Having experienced the overblown Y2K threat, the public has every right to be cynical about the next big cyber-threat to come along, namely cyber-terrorism. Public mistrust and cynicism of government, especially so in the United States, is nothing new. Perhaps the refusal to believe in the possibility of cyber-terrorism is a cynical reflection of the times, or perhaps it was precipitated by lack of any Y2K "bang," so to speak. The media may equally share a role, by perpetuating fear and sensationalizing the threat.

Let us set the naysayer arguments aside, and proceed on the assumption that cyber-terrorism is certainly *possible*, and that if cyber-terrorism is possible, then governments should at least develop a strategy for dealing with that possibility. This paper will go further than arguing that cyber-terrorism is possible and submits that it is here now and has been for some years, as will be demonstrated from news stories.

Regardless of the perceived threat of cyber-terrorism, *cyber-attacks* are real as will also be demonstrated by modern occurrences; whether they are classified as “cyber-terrorism” or not makes little difference from a cyber-security standpoint, because they both use similar cyber-attack strategies. A government server does not care about the intent of a cyber-attack, only that it is happening. The important point to remember is that the methods by which cyber-attacks occur must be addressed, regardless of the originating motivation. Furthermore, we must assume that if there is a way to exploit holes in Canada's computer systems, the enemies of our nation will exploit these when they can. What is more, we must assume that what is publicly available online for non-terrorists will be also be available for terrorists to read.

Federal Bureau of Investigation Director, Robert Mueller, stated that cyber-attacks could harm “national security as much as other terrorist attacks have in the past” (Mueller, 2009). In Canada, the same warnings apply, and the Canadian Security Intelligence Service (2008) has stated that “[m]any Canadians may be surprised to learn that, with the exception of the United

States, there are more terrorist groups active in Canada today than in any other country in the world" (Canadian Security Intelligence Service, 2008a, para. 1). CSIS (2008a) noted as well that most terrorist operations in Canada are less obvious in nature and involve acts like funding and recruiting for terrorists internationally, often involving use of the Internet.

Based on the findings of both the FBI and CSIS, two of the largest intelligence agencies in North America, we can be fairly confident that the risk of cyber-terrorism is indeed real, and proceed in our analysis with this in mind. However, we must first divert for a moment, and analyze why cyber-terrorism exists in the first place.

Motives for Terrorism

It must be mentioned that solving the problem of cyber-terrorism, means first solving the problem of terrorism in general. It is also worth noting that "the use of the term 'war on terrorism'" has a political bias. Terrorism is a means rather than an end" (Desouza, Koh & Ouksel, 2006, p. 125). A proper "war on terrorism" cannot be won with missiles and weapons. "One does not counter psychological warfare with high-tech weapons…psychological operations should be *the primary weapon* in the war on terrorism" (Post, 2010, p. 23). The long-term solution to reducing terrorism in all its forms is to combat it through psychological means such as education and exposure to critical points of view.

However we decide to combat terrorism, we must keep in mind that "[t]here is no known valid and reliable way to weigh the influence of predictive factors or model the pathways that might increase the likelihood that an individual will become a suicide bomber" (Victoroff, 2009, p. 399), and that "scholars have concluded that as individuals terrorists are psychologically normal" (Post, 2010, p. 15). Likewise, terrorists are "neither depressed, severely emotionally disturbed, nor are they crazed fanatics. Indeed, terrorist groups and organizations screen out emotionally unstable individuals. They represent a security risk" (Post, 2010, p. 15).

The motivating factors of terrorism are probably best described through a group psychology lens:

> Families of terrorists who were wounded, killed or captured enjoyed a great deal of economic aid and attention. And that strengthened popular support for the attacks. (Post, 2010, p. 20, quoting Hassan Salame, serving 46 life sentences for being behind suicide bombings in Israel in 1996)

Suicide bombers are portrayed in their communities as living martyrs (Post, 2010). As such, group psychology backed by religion strengthens the will of would-be terrorists. So, the question becomes: why would a terrorist choose instead to perform cyber-terrorism rather than a physical act, like blowing up a building? To understand, we must look at the benefits of cyber-attacks in furthering a terrorist cause.

The Internet as a Force Multiplier

The Internet is an excellent “force-multiplier…because there’s virtually no personal, physical risk incurred by an Internet attacker, and that one attacker could attack multiple facilities” (Gewirtz, 2009). 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 upon. Terrorists also use the Internet to gather detailed technical information, and use the Internet as a cheap and secure means of communication with each other and the media (Desouza, Koh & Ouksel, 2006). In fact, the Internet and national communications were used in the planning of the 9/11 attacks in New York (Desouza et al., 2006).

There are “[s]everal characteristics of cyberspace [that] create an enabling environment for persons or groups to promote their ideas: anonymity, confidentiality, accessibility, low costs, intelligent interfaces, ease of use, “force multiplier,” media attention, and psychological effects” (Goodman, Kirk & Kirk, 2007, p. 196). Cyber-terrorists share common traits with guerrilla warfare fighters in that they are relatively obscure, virtually anonymous, and their “attacks can be sporadic and unexpected” (Goodman et al., p. 196).

To date there have been few officially recorded cyber-terrorism attacks, because as Denning (2000) explains:

> Cyberterrorism also has its drawbacks. Systems are complex, so it may be harder to control an attack and achieve a desired level of damage than using physical weapons. Unless people are injured, there is also less drama and emotional appeal…Novelty and sophistication of attack may be much less important than assurance that a mission will be operationally successful. Indeed, the risk of operational failure could be a deterrent to terrorists. For now, the truck bomb poses a much greater threat than the logic bomb. (Denning, 2000, para. 17)

What Denning says holds true for the moment, although even less so in 2010 as hardware, software, and Information and Communication Technologies (ICTs) are becoming ubiquitous. The cyber-terrorism option will rise in appeal as the potential devastation it may cause increases in proportion with our reliance on computing systems for automation, communication, and governance.

Despite all the efforts we can make as a society to deter and prevent terrorism, terrorism is likely to never go away “as long as terrorism is likely to yield tangible, far-reaching results, it will be attractive to those who wish to create fear, coercion, or intimidation” (Czinkota et al., 2005, p. 583). The Internet compounds the problem because it provides a quick and effective means of acting on violent political impulses, with relatively few consequences compared to a suicide bombing. Examples of cyber-attacks will further demonstrate the potential effectiveness of cyber-terrorism acts.

Modern Examples of Cyber-attacks

In 2007, Younis Tsuli and two of his cohorts, who ran a site that featured beheadings and al-Qaida propaganda, were the first known people to be arrested and tried for cyber-terrorism in the United Kingdom (Oliver, 2007). “In Estonia in 2007 and Georgia in 2008 cyber-attacks shut down most of the country’s websites, including those of the parliament, ministry of foreign affairs, banks and newspapers” (Holbrook, 2010, p. 8). In 2008, someone inserted a virus-infected flash drive into a U.S. military laptop. The virus spread quickly across the base, exposing sensitive information (Holbrook, 2010). More recently, a much publicized cyber-attack was launched on Google:

> In mid-December [2009], we detected a highly sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in the theft of intellectual property from Google…As part of our investigation we have discovered that at least twenty other large companies from a wide range of businesses—including the Internet, finance, technology, media and chemical sectors—have been similarly targeted. (Drummond, 2010, para. 1 & 2)

The Google example can be understood as, depending on how you read China's motivations for launching the attacks, either cyber-espionage or cyber-warfare. Either way, the example highlights the potential power and success of cyber-attacks, against even the largest technology-savvy corporations like Google.

It is important to understand that cyber-attacks are 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 system and use it to damage, destroy, or cripple the power distribution of a potentially large area (Branscomb, 2004). This scenario is not a far cry from the devastation our *WarGames* hacker of 1983 nearly set in course. It is this side of cyber-attacks that bears the most real threat to average citizens, as they could see and feel the tangible effects of this sort of cyber-attack. Dycus (2010) argues that,

> Cyber weapons bear a striking resemblance to nuclear weapons in some important ways. An enemy’s cyber attack would, like a nuclear strike, probably come without a clear warning. There are as yet no reliable defenses against either a cyber attack or a nuclear attack. Collateral damage from a nuclear attack would almost certainly be very extensive and would linger for an extended period.

> The direct and indirect effects of a cyber attack, while different in kind and degree, still could be widespread and indiscriminate. (p. 163)

While a nuclear weapon could take up to thirty minutes to reach a target, and thus provide some time to prepare a counter-attack or interception, a cyber-attack would arrive instantaneously, stressing the need for superior security measures and resilient systems (Dycus, 2010). Using “spoofing” techniques, a cyber-attacker might appear to be launching an attack from another country, provoking the cyber-attackee into a defensive strike against the innocent country and provoking wider conflict, should improper cyber-security procedures and policy exist (Dycus, 2010). Given the immediate nature of cyber-attacks, it is even possible that a cyber-war could start and end before the word of its beginning ever reached state executives, thus strengthening the argument that states need to “lay down clear guidelines, with as much flexibility as prudence requires, for executive branch officials to follow if consultation is not reasonably possible” (Dycus, 2010, p. 164).

We now understand the real threat of cyber-terrorism and cyber-attacks on our critical infrastructure, the motivations behind the acts, and the possible effectiveness of these attacks. It is beyond the scope of this paper to examine every possible consequence of cyber-attacks on critical infrastructure, so we will focus on an analysis of only one sector: electronic governance, or e-Canada.

E-Canada and Canadian Government

1. Defining E-Government

Halchin (2004) says there is “no single, widely agreed upon definition” for electronic government (p. 407). While this may be true, inasmuch as the Internet is changing all the time and definitions may be obsolete rather quickly, most understand the term to mean broadly any government services available online. Understanding the scope of e-government, it is easy to understand why it is economically beneficial, as it improves “efficiency, effectiveness, response times, and one-stop access to information and services” (Halchin, 2004, p. 417).

The term “e-Canada” will be used instead of “e-government” to represent all the Canadian government services that are available online, including both the publicly accessible information and services, and the services and information that are kept, ostensibly, private between departments and agencies of the government. Additionally, “e-Canada” will be expanded herein to comprise all Internet-enabled or capable technologies within the public or private sectors, such as SCADA power station systems, whose failure in the face of a cyber-attack would mean hardships for Canadian citizens.

2. Why E-Canada is Vulnerable

When Coates (1996) looked to the future of terrorism, he saw that government was ultimately responsible for preventing it, using tried and true means of intelligence gathering and information (Coates, 1996). Coates' argument is equally as valid in the digital realm as it is in the real world; government policy and preventative methods have the best chance of combating and preventing cyber-attacks. As we have seen, distribution, logistics, and in the long run Gross Domestic Product, can all be affected by major cyber-attacks (Czinkota et al., 2005).

The economic impact of cyber-attacks is definitely a major problem for Canada, because as of 2007, 87% of Canadian businesses made use of the Internet; in 2008, 59% of personal tax filings were done electronically; and, in 2009, 67% of Canadians banked online (Government of Canada, 2010). Should these trends towards use of electronic services continue, this means that e-Canada will become increasingly part of our economic makeup. It follows then, that as relative computing power gets cheaper and as high-speed Internet expands its range to rural areas, more and more people will depend on e-Canada.

In November of 2010, Postmedia News was able to receive a previously secret government report through access-to-information laws that detailed the doubling of cyber-attacks in the last two years. The redacted report revealed that 86% of Canada's large corporations have been the target of cyber-attacks, with an estimated half of these attacks coming from China (Tibbetts, 2010). CBC News learned that in late September of this year, users of a Service Canada website, due to a glitch, were able to access other citizens' information, including social insurance numbers and banking information. It took Service Canada three days after being alerted of the issue to notify the Privacy Commissioner, highlighting the strange fact that reporting privacy breaches are not required by Canadian law (CBC News, 2010).

Halchin (2002) pointed out that details such as "fuel capacities, aircraft dimensions, and maximum passenger loads" are available on aviation companies' websites (p. 245). As an example, Air Canada has detailed fleet specs on its website that most customers would never need to know, such as altitude, range, fuel capacity, engine, and cruise speed. This public information can be harnessed easily to plan and coordinate terrorist attacks in the real world. Floor plans for the Centre Block of the Canadian parliament are easy to find with just a few minutes spent searching Google. These examples serve to illustrate how easy it is for any malicious individual or group seeking to plan either a cyber-attack or a physical attack to find potentially compromising information online.

Current security mandates in Canada are a problem in fighting cyber-attacks. For instance, "CSIS confines its investigation to computer intrusions conducted with a "political motivation." Whether a hostile intelligence service is hacking into Canadian computer systems, or an extremist group is targeting a government Web site, there must be a political aspect to the computer intrusion in order for CSIS to be involved" (Canadian Security Intelligence Service, 2008b, para. 3). This policy is vague and limited. How can CSIS determine explicit political motivation during a cyber-attack? The motives of a cyber-attack would be difficult to uncover, leaving CSIS unable to react to cyber-terrorism until they somehow determine a "political aspect," which could take months or could even never materialize. A strong legislative stance should be taken against cyber-attacks allowing CSIS the leverage that it needs to prevent cyber-attacks on e-Canada, and allowing it to investigate any case it deems necessary.

3. Securing E-Canada

The Canadian government will be ultimately responsible when public or private critical infrastructures fail due to a cyber-attack, and therefore Canadian government policy must do all it can to ensure due diligence in the private sector. Certainly, the private sector should be allowed to incorporate its own security measures, but it should have to meet a nationally-recognized security evaluation.

Since 2002, the FBI has created a checklist for government officials to evaluate the information on their websites, something that Canada is lacking (Halchin, 2002). However, there is a delicate balance that needs to be considered: the promise of e-Canada and its more transparent, efficient, and timely government, has to be constantly weighed against possible exploitation of those very factors by hackers.

Canada needs to make security of its vulnerable systems the number one priority in its cyber-strategy. Canada can develop a stronger e-Canada by: using teams of faux-cyberterrorists to test vulnerabilities in systems; creating stronger criminal laws against cyber-attacks; increasing deterrence of attacks by declaring a high possibility that attackers will be caught (similar to anti-theft measures a retail store or home might take); increasing the capability to intercept attacks in progress; strengthening physical systems with features like electro-magnetic pulse protection; enabling automatic shutdown procedures to limit damages when attacks are detected; and, creating redundant backups of assets (Goodman et al., 2007).

The key word to understanding all these measures is *resiliency.* The concept of a "resilient system" acknowledges this simple fact: cyber-attacks will occur no matter how much prevention is in place, or how well designed the system. Granting that cyber-attacks will occur no matter what measures are put in place, it is of the utmost importance that e-Canada be resilient by design, so that we are relatively unhurt by cyber-attacks.

The beginning of a resilient approach to e-Canada starts with individual computer systems and networks. Engel (2010) suggests first to identify, locate, and classify information assets, to prioritize them using some sort of scale (i.e., 1 to 5), and to conduct threat exercises using commonly attempted cyber-attacks. Finally, he suggests reviewing the data and working on the biggest risk first (Engel, 2010). There are many other strategies that can be used to assess any network or computer system for vulnerabilities. This paper is more concerned with policy than the specifics of computer science. Having said that , further study in the strengths and weaknesses of various security assessment tools would be a prerequisite for any strong e-Canada policy. Regardless, the success of any proper assessment is borne out of proper intelligence work, which is itself the product of proper information management, which is a four-step process that includes the collection, validation, analysis, and assessment of information (Dearstyne, 2005).

It has been revealed that the U.S. Defense Department is “heavily engaged in preparations for cyber warfare, having recently announced the establishment of a new U.S. Cyber Command” (Dycus, 2010, p. 161). This Cyber Command is a step in the right direction if we are to believe the seriousness of cyber-attacks, and we do. It is thus a model that Canada should consider adapting to its needs.

4. E-Canada and Promises for the Future

On October 3, 2010, Stephen Harper announced *Canada's Cyber Security Strategy*, and promised funding of $90 million dollars over a five year period to create an Information Protection Centre. The Strategy is also aiming to “protect government systems from hackers, work with the provinces and businesses to ensure private information is properly encrypted, and to help educate Canadians about cyber-safety” (Tibbetts, 2010, para. 8).

The *Cyber Security Strategy* unveiled by Harper contains vague or general wording such as: “[t]he Government will put in place the necessary structures, tools and personnel to meet its obligations for cyber security” (“Canada's Cyber Security,” 2010, p. 7). Naturally, it is difficult to get concrete details on what this means, as it rightly should be. Anything that it available publicly must be assumed to be read by enemies of the state, thus revealing details of our strategy to the public would be self-defeating. The Strategy offers three “pillars” upon which it is built: 1. Securing government systems; 2. Partnering to secure vital cyber systems outside the federal government; and 3. Helping Canadians to be secure online (“Canada's Cyber Security,” 2010, p. 9). Note that the second “pillar” acknowledges, as we have, that e-Canada must include vital non-government systems.

The long past due strategy to help protect vulnerable e-Canada services against cyber-attacks is an important first step, as it acknowledges that e-Canada is vulnerable, and that something must be done. Whether the money and protection promise will come to fruition is yet to be seen; for as one government leaves and another takes its place, the next Canadian government may drastically cut funding or scrap the current strategy altogether. Canada needs to look beyond a five-year plan of action, and develop a central Cyber Command, drawing on the US model for ideas, and altering it as we see necessary. Canada is taking a small step in the right direction, but it is hazardous and myopic to leave the security of e-Canada under the purview of an Information Protection Centre which is only guaranteed a five-year term.

When we speak of future warfare forces, we will speak of cyber-divisions, and what is happening on the cyber-front. We need to include a cyber-force as part of our defensive and offensive military strategy. The United States is already taking the necessary steps towards this inevitability, and as Dycus (2010) posits: “[t]he very future of the Republic may depend on our ability not only to protect ourselves from enemies armed with cyber weapons, but also to use such weapons wisely ourselves” (p. 156). A central Cyber Command's mandate for e-Canada would be twofold: 1. proactive security of e-Canada during times of peace, and, 2. in times of war coordinating and launching our own cyber-attacks as an apparatus of the military.

Lessons Learned and Conclusion

“He does fit the profile perfectly. He's intelligent, but an under-achiever; alienated from his parents; has few friends. Classic case for recruitment by the Soviets,” FBI agent George Wigan quips during *WarGames* about our precocious, naïve, young hacker (“WarGames,” 2010, para. 3). The comment was clearly a tongue-in-cheek jab at Cold War paranoia, but it serves the double purpose of implicitly stating the most dangerous threat to e-Canada: the insider. No computer system will ever be secure as long as there is access to it somehow, either physically or remotely, because there is always the possibility of an “inside job.” Regardless, e-Canada must forge ahead with making its systems as secure as possible, and the insider example serves to further strengthen the argument for resilient systems.

The recent WikiLeaks release of secret government cables, popularly called “Cablegate,” gives testament to the power of the insider to do damage (WikiLeaks, 2010). Credence must be given to the persistent possibility of cyber-attacks coming not from the outside, but from within. Internal sabotage can often be pernicious in a way that external threats are often not: a saboteur may understand the particular resiliencies of a system, and possibly how to work around these security measures. Developing any cohesive cyber-strategy for e-Canada means acknowledging the destructive power of a saboteur, and designing systems that limit the damage this kind of treason can do.

Canada must join the United States on the frontlines of cyber-defence. This must be achieved by taking a proactive stance against cyber-attacks because in a time-sensitive environment like the Internet, taking a passive, defensive stance against cyber-attacks will make e-Canada into a target for cyber-terrorism. Canada can harden its stance against cyber-attacks by using the following method: developing national Internet standards designed with resilient systems in mind, that are under the purview of a central Cyber Command, and that operate under extended laws and policies enabling a more aggressive proactive stance against cyber-attacks. Canada has taken the first steps towards making this action a reality, but it is quickly running out of time. As cyber-attack frequency gains momentum in the coming years, our economic, even physical, security is contingent upon developing a long-term vision for protecting e-Canada.

References

Branscomb, L. (2004). Protecting civil society from terrorism: The search for a sustainable strategy. *Technology in Society, 26*(2-3), 271-285. doi: 10.1016/j.techsoc.2004.01.004 CrossRef

Canadian Security Intelligence Service. (2008a). *Terrorism*. Retrieved from http://www.csis-scrs.gc.ca/prrts/trrrsm/index-eng.asp

Canadian Security Intelligence Service. (2008b). *Working Against Information Security Threats*. Retrieved from http://www.csisscrs.gc.ca/prrts/ nfrmtn/wrkng-eng.asp

CBC News. (Nov. 10, 2010). *Federal online glitch leaked private info.* Retrieved from http://www.cbc.ca/canada/ottawa/story/2010/11/10/privacy-glitch-111.html

Coates, J. F. (1996). A thriving future for terrorism. *Technological Forecasting and Social Change, 51*(3), 295-299. doi: 10.1016/0040-1625(95)00198-0 CrossRef

Czinkota, M. R., Knight, G. A., Liesch, P. W., & Steen, J. (2005). Positioning terrorism in management and marketing: Research propositions. *Journal of International Management, 11*(4), 581-604. doi: 10.1016/j.intman.2005.09.011 CrossRef

Dearstyne, B. W. (2005). Fighting terrorism, making war: Critical insights in the management of information and intelligence. *Government Information Quarterly, 22*(2), 170-186. doi: 10.1016/j.giq.2005.01.001 CrossRef

Denning, D. E. (2000). *Cyberterrorism*. Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, May 23, 2000. Retrieved from http://www.cs.georgetown.edu/~denning/ infosec/cyberterror.html

Desouza, K. C., Koh, W. T. H., & Ouksel, A. M. (2006). Information technology, innovation and the war on terrorism. *Technological Forecasting and Social Change, 74*(2), 125-128. doi: 10.1016/j.techfore.2006.07.006 CrossRef

Drummond, D. (2010). *Official Google blog: A new approach to China.* Retrieved from http://googleblog.blogspot.com/2010/01/new-approach-to-china.html

Dycus, S. (2010). Congress's role in cyber warfare. *Journal of National Security Law & Policy, 4*(1), 155-171. Retrieved from http://search.ebscohost.com/login.aspx? direct=true &db=tsh&AN= 22049795&site=isc-live

Engel, P. (2010). The 5 steps of a cybersecurity risk assessment. *Risk Management (00355593), 57*(8), 39-39. Retrieved from http://search.ebscohost.com/ login.aspx?direct=true &db=tsh&AN=22049795 &site=isc-live

Gewirtz, D. (2009). How critical infrastructure is at risk of a cyber attack. *Journal of Counterterrorism & Homeland Security International, 15*(2), 8-10. Retrieved from http://search.ebscohost.com/login.aspx?direct=true &db=tsh& AN=22049795&site=isc-live

Goodman, S. E., Kirk, J. C., & Kirk, M. H. (2007). Cyberspace as a medium for terrorists. *Technological Forecasting and Social Change, 74*(2), 193-210. doi: 10.1016/j.techfore.2006.07.007 CrossRef

Government of Canada. (2010) *Canada's cyber security strategy.* Retrieved from http://www.publicsafety.gc.ca/prg/ns/cbr/ccss-scc-eng.aspx

Halchin, L. E. (2002). Electronic government in the age of terrorism. *Government Information Quarterly, 19*(3), 243-254. doi: 10.1016/s0740-624x(02)00104-1

Halchin, L. E. (2004). Electronic government: Government capability and terrorist resource. *Government Information Quarterly, 21*(4), 406-419. doi: 10.1016/j.giq.2004.08.002 CrossRef

Holbrook, E. (2010). Cyberwarfare: WWIII or exaggeration? *Risk Management (00355593), 57*(8), 8-10. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=22049795&site=isc-live

Internet Movie Database. (2010). *Wargames (1983) – memorable quotes*. Retrieved from http://www.imdb.com/title/tt0086567/quotes

Kohlmann, E. F. (2006). The real online terrorist threat. *Foreign Affairs, 85*(5), 115-124. Retrieved from http://search.ebscohost.com/login.aspx?direct=true &db=tsh&AN=22049795&site=isc-live

Lee, J., & Rao, H. R. (2007). Perceived risks, counter-beliefs, and intentions to use anti-/counter-terrorism websites: An exploratory study of government-citizens online interactions in a turbulent environment. *Decision Support Systems, 43*(4), 1431-1449. doi: 10.1016/j.dss.2006.04.008 CrossRef

Lin, C.-H., Liou, D.-Y., & Wu, K.-W. (2007). Opportunities and challenges created by terrorism. *Technological Forecasting and Social Change, 74*(2), 148-164. doi: 10.1016/j.techfore.2006.02.004 CrossRef

Mueller, R. (2009). *YouTube – Cyber-terrorism*. Retrieved from http://www.youtube.com/watch?v=Y2uNxpqo7CE

Oliver, M. (2007). *'Internet jihadist' jailed for 10 years.* Retrieved from http://www.guardian.co.uk/technology/2007/jul/05/terrorism.uknews

Oxford English Dictionary. (1989). *Hacker, n. -- Oxford English Dictionary,* Retrieved from http://dictionary.oed.com/

Post, J. M. (2010). “When hatred is bred in the bone:” The social psychology of terrorism. *Annals of the New York Academy of Sciences, 1208*(1), 15-23. doi: 10.1111/j.1749-6632.2010.05694.x CrossRef

Stohl, M. (2007). Cyber terrorism: A clear and present danger, the sum of all fears, breaking point or patriot games? *Crime, Law & Social Change, 46*(4/5), 223-238. doi: 10.1007/s10611-007-9061-9 CrossRef

Tibbetts, J. (2010). *Report exposes 'economic damage' caused by hackers.* Retrieved from http://www.ottawacitizen.com/news/Report+exposes+economic+damage+caused+hackers/3875625/story.html

Victoroff, J. (2009). Suicide terrorism and the biology of significance. *Political Psychology, 30*(3), 397-400. doi: 10.1111/j.1467-9221.2009.00704.x CrossRef

Wikileaks. (2010). *Cable Viewer*. Retrieved from http://www.wikileaks.ch/cablegate.html