March 2015

CYBERSECURITY CHALLENGES

FOR CANADA AND THE UNITED STATES

Alexander Moens | Seychelle Cushing | Alan W. Dowd

Contents

Executive summary

The Internet was designed not with security in mind, but rather openness and the free flow of information. The resulting globally connected nature of the Internet has brought unprecedented levels of information and commercial exchange, contributed enormous gains to individual prosperity, empowered individuals, and promoted and expanded individual liberty. Only in recent years have governments, militaries, industries, firms, and individuals come to grips with the importance of protecting this critical sphere of activity on which so much liberty, property, and security depends. How to protect legitimate activity in cyberspace without compromising its open character is the challenge.

Overemphasizing security can restrict freedom and stifle entrepreneurial potential. Conversely, liberty in cyberspace without an appreciation of cybersecurity presents rising commercial and governmental costs as well as unacceptable threats to national security. One study on the economic costs of cyberespionage and other forms of cyberattack estimates the global costs of "malicious activity" at between $375 billion and $575 billion annually, and a range of nation-states, state-linked groups, and non-state actors are exploiting cyberspace to conduct espionage, military operations, and large-scale theft of intellectual property. The most serious of these cases are examined in this report, including: "cyber-riots" against Estonia, cyberattacks to coincide with kinetic military operations against Georgia and Ukraine, cyberespionage and intrusion into Western energy firms—all traced to Russian sources; US-Israeli cooperation to develop and deploy the highly sophisticated and—importantly—narrowly targeted *Stuxnet* computer worm against Iran's nuclear program; Iran's *Shamoon* computer virus; and China's exploitation of its capabilities for cyberattacks to conduct political, military, and industrial espionage on a massive scale.

In a sense, cyberspace is the new Wild West, where the arm of international law has not yet arrived. Although there have been calls for international norms of behaviour and rules of the road in cyberspace, treaties, arms control, non-proliferation, and disarmament as developed and understood in the conventional, nuclear, and chemical realm are not easily transferred to the domain of cyberspace. However, the absence of formal international agreements on cybersecurity does not mean there are no rules or boundaries

in cyberspace. The rule of consequences and of self-interest is in play, as is the logic of cost-benefit in escalation. Even so, cyberattacks continue, increasing in quantity and quality, which is why resilience is the watchword of cyberspace. If deterrence is what kept the peace during the Cold War and the Nuclear Age, resilience may be the governing principle of the Digital Age. This being the case, this report argues that the level of North American resilience in cyberspace should be heightened, with government and industry playing collaborative and cooperative roles.

As in other zones of commerce and theatres of operation, Canada and the United States are deeply integrated in cyberspace. Both nations derive benefits from cybersecurity cooperation. Canadians should not underestimate the benefits they gain from US willingness to share advanced capabilities for cyberoperations. Canada draws a clear net benefit from close cooperation with the United States in cyberspace because both the nature of the evolving threat and the nature and cost of countering this threat are increasingly more difficult for a state to address on its own. At the same time, as it cooperates with the United States and other close allies, the Canadian government faces the challenge of finding a balance between security and the Canadian definition of freedom.

The expansion of the powers wielded by Canadian government agencies, as well as coordination with US agencies and other allied agencies, will likely mean more combined activity between domestic and foreign cybersecurity and intelligence. This task should not be left to the specialized agencies without a layer of oversight by elected representatives. As Canada updates its ability to deal with threats in cyberspace, it needs to enhance the ability of its representative government to oversee this important work. The idea of an all-party committee in Parliament, advocated by some observers, is a good one. Members of this committee would have security clearance and the ability to call informed witnesses to ensure that Canada's cyberactivities balance security with Canadian notions of the rule of law, liberty, and rights. The key is to build in sufficient and effective checks and balances on the government's role so that both security and resilience can be enhanced, while intrusions into individual liberty can be minimized.

Introduction

The Digital Age and the technologies that shape and propel it have empowered individuals and provided the impetus for the expansion of individual liberty and commerce. The accessible, open nature of cyberspace allows individuals to tap into stores of knowledge and information that can transform their economic, social, and political lives. To illustrate: e-commerce, which is only a small piece of the "cyber-pie", was estimated at $49 billion in Canada in 2011 (Deibert, 2012).

At the same time, cyberspace is a medium that has opened a deep store of opportunity for individuals, groups, and foreign governments to inflict harm on others and to acquire property illegally. That, in turn, invites governmental action, which can have the effect of limiting individual liberty. As in other domains of political and commercial activity, there is a trade-off: as government intervention increases, there is a promise of greater security, but that security comes with economic costs and can limit liberty. Some trade-off, it seems, is inescapable.

Some call for keeping cyberspace as open, diversified, and global as possible and for a global network of cooperative behaviour called "distributed security" to provide the needed restraints on illegal behaviour. Others urge governments to collaborate more extensively at the international level and to seek "arms control" agreements on cyberoperations. Both arguments have merit, but also assume significant incentives for cooperation that we do not observe in the arena of cybersecurity. We argue that national security actions by governments, such as Canada and the United States, focused on upholding the rule of law and acting in accordance with the rule of law, will remain an indispensable part of security in the evolving theatre of cyberspace. Cybersecurity efforts in constitutional democracies, such as Canada and the United States, thus face a stiff challenge: how to reduce vulnerability, optimize commercial and national security, and respect individual liberty.

While government has no monopoly on the means of access to cyberspace, it has a duty to provide cybersecurity as citizens' expectations of freedom in cyberspace include the freedom from cyberattacks against life, liberty, and property. There is no such thing as complete cyber security or cyber defence because computer code will always be vulnerable. The challenge is

to obtain maximum advantage in a realm of shared vulnerabilities. The logic of cybersecurity calls for governments, firms, and even individuals to maximize their resiliency.

Without national security action in cyberspace, threats to life, safety, and property will increase. The costs of insecurity and business disruption are too great and rising too rapidly to conclude that cybersecurity is not needed or that no trade-offs with privacy can be tolerated. This study shows the dominant patterns of cyberattacks and makes estimates of costs to business. There is no data available as of yet to do an authoritative study of the costs. In any case, a failure of cybersecurity is costly and recent trends suggest costs will continue to rise.

National action to protect a country's cyberspace requires "checks and balances" on the governmental role so that security can be enhanced and intrusions into individual liberties minimized. This is no mean task and cannot be entrusted solely to appointed officials but must include an oversight role by the elected representatives of the people, which is currently not the case in Canada. Our study supports the need for a discussion in Canada to form a parliamentary oversight committee over security, intelligence, and cybersecurity that includes members from all political parties who must have security clearance to review sensitive material and security obligations to handle such material responsibly.

Conclusions and recommendations

The focus of this report is on cybersecurity. Without a robust level of security, the benefits of the extended liberty provided by the Internet would dry up. The high vulnerability level at all points in society, the deficiency of international governance in cyberspace, and the need for sustained expertise point to a continuing role for the national government. The federal government's role is to protect national interests, including key infrastructure, and to support businesses and individuals in their quest for cybersecurity.

The high degree of anarchy in international cybersecurity requires both national resources but also points to the need for international "arms control" in cyberspace. However, the sprawling nature of the actors in cyberspace and the fluidity between defensive and offensive actions in cyberdefence make this quest very challenging.

Cybersecurity is best understood as gaining and keeping maximum overall resiliency. Given the track record of foreign intrusions into Canadian and American assets in cyberspace, especially those originating in China, the level of North American resilience should be heightened.

The research on quantifying the cost of failures in cybersecurity is still in its early stages. The two cost categories discussed in this paper (cost

to business and cost to government) have only a few studies, and these offer estimates rather than measurement. Canadian data lags behind US data. The cost to government and business from cyberattacks should be systematically recorded and analyzed and should include a bilateral component in order to measure the magnitude of the problem and the effectiveness of counteraction nationally and jointly in the Canadian-US market and security space.[1]

Given the integrated and global nature of cyberspace, the Canadian government depends on both the Five Eyes arrangement and on close Canadian-American cooperation on intelligence and cybersecurity. Even the much larger US government derives benefits from cybersecurity cooperation with key partners such as Canada. National sovereignty and national control within these networks are crucial objectives but they are also relative and not absolute, and require trade-offs to maintain benefits for all national parties involved.

Canada draws a clear net benefit from close cooperation with the United States in cyberspace because the nature of the evolving threat and the nature and cost of countering this capacity is increasingly more difficult for a state to address on its own. At the same time, the Canadian government faces a complicated trade-off between security and the Canadian definition of rights and freedoms as it cooperates with the US and Five Eyes. Surveillance capacity, like capacity for cybersecurity, is on the increase. Managing the information that results from this capacity remains a key value that both the US and Canadian publics demand.

Given the sensitive and intrusive nature of cyberactivities and the vital principles of liberty and privacy, the national security activities of government in cybersecurity should include a representative oversight function in Canada in the form of a parliamentary committee composed of members from all parties with sufficient security clearance and responsibility to review and safeguard policy and operations. In both countries, the relationship between cybersurveillance data and cybersecurity should be governed by strict criteria of necessary security and limited use.

1. For a larger discussion on the implications of such measurement, see page 17, "Costs to Business" and following section.

The Nature and Logic of Cyber(in)security

It is a cliché now but the Internet was not designed for security—it was built to provide access to information and transmit it around an intranet of government-based computers inside the US Department of Defense. But, that network evolved into the Internet as we know it today, which spans the globe. From the early 1990s onward, virtually everything governments, companies, and individuals produced, used, and depended on began migrating to cyberspace. In 2010, it was estimated that some 90 trillion emails were transmitted (Alexander, 2012). The global connected nature of the Internet has brought unprecedented levels of information exchange and commercial exchange to "netizens" of the world and has contributed enormous gains in individual prosperity. Only in recent years are governments, militaries, industries, firms, and individuals coming to grips with the importance of protecting this critical element of information on which so much property and security depends. How to protect cyberspace without compromising its open character remains a debate. If most countries were to build their own restricted national Internet realms, the Internet would "balkanize"—that is, splinter—and many of its gains of open exchange would be lost.

The complexity of the task—of attaining a certain level of cybersecurity—requires technology, logic, and strategies that go beyond traditional notions of security and beyond traditional espionage.

The term "cyber" can refer to both the electronic and physical infrastructure of cyberspace and the line of alphanumeric data—the code—that tells a computer how to act (Deibert, 2013). Such code is based on human ingenuity and is thus also subject to human error. When people write code (the lines of instruction), they unintentionally create vulnerabilities (Frei, 2013). Millions of lines of code and growing networks of interconnected programs make such vulnerabilities a near certainty. For example, Windows XP has some 45 million lines of code. It is one thing not to like the program, but the people building it were among the best in the field. Yet, during 2012 and 2013 more than 40 vulnerabilities were discovered in this program alone

(Metz, 2013; Timberg and Nakashima, 2014; Rains, 2013). The point is that cybersecurity is about how to minimize vulnerability. It cannot be about attaining perfect security.

Cyberattacks range in severity from nuisance attacks to those having the potential to threaten the command and control operations of a national military apparatus. A cyberattack can occur when someone discovers and exploits a vulnerability hitherto unknown. Such a vulnerability is called a zero-day exploit ("zero day"). From the time a zero day is discovered, the clock starts ticking as to what the actor will do with it. If the potential recipient of such an intrusion discovers the vulnerability, he must engineer a patch to close the gap (*PC Tools*, 2011). The two actors may not know of each other's manoeuvers. If a state actor finds a vulnerability in another government's system and only uses the unprotected spot to snoop inside the information of that government, it is mainly understood as a form of espionage that is accepted by most players as fair game (Nye, 2011; Riley, 2013). But if the hostile actor gains access and uses it to manipulate another state's internal affairs or causes something to malfunction or block access to a service, we call it a cyberattack or, in the field's jargon, a "cyber effects operation".

Who can carry out such attacks? In one sense, more and more people are gaining expertise to do so. But, in a spectrum of potential cyberattackers and their impact on cybersecurity, the experts distinguish between script kiddies (inexperienced hackers) on the lowest end of risk and advanced persistent threats (APT), which are states or state-sponsored actors on the highest end (Winterfeld and Andress, 2012). Currently, the United States, United Kingdom, China, Russia, France, and Israel are considered the most capable of the APTs (Clarke and Knake, 2010; Lewis, 2013). Other states are emerging as up-and-coming APTs. Still others, such as Canada, are working hard to bolster their expertise (Carr, 2012). In the middle of the spectrum, we find so-called "hacktivists" and hired gangs and other semi-autonomous groups that may have close working arrangements with state actors, as is probably the case in Russia and China (Winterfeld and Andress, 2012; Clayton, 2012).

A zero day is both a vulnerability and an opportunity: Do you patch it or use it to probe another's capability (Kemp, 2012)? Finding a zero day is difficult. Being able to use those discovered to engineer a sophisticated cyberattack is even more challenging. It may take months and many experts and financial resources to execute a high-level cyberassault (Singer, 2012). Certain governments, such as the United States, may use the grey vulnerabilities market to buy a zero day from hackers, realizing the government alone cannot find all of them and that "commercial" expertise exists out there that the government can use. Ironically, legitimate governments buy cyberexploits from semi-legitimate operators in order to save money and to learn what expertise is out there (Gjelten, 2013; Fung, 2013).

This marketplace for cyberexploits, however, is not the only one. While governments buy from the hidden but not necessarily illegal grey market, criminals simultaneously take advantage of a black market. In the black market, "hired guns" look to buy expertise with which to attack Western commercial or governmental institutions and criminals buy the proceeds or contents of recent cyberattacks, such as credit card numbers and personal identities (Fung, 2013, Aug. 31; Ablon, Libicki, and Golay, 2014). Both Target and Home Depot are recent commercial victims of such cyberattacks, with customer information being sold in the black market.

Cybersecurity is, of course, not a governmental monopoly in the sense that nuclear weapons, for example, have remained thus far. Industry and individuals can be both suppliers and consumers of cyberinformation and, thus, cybersecurity. As we will discuss further below, firms are constantly bombarded by break-in attempts for information. In this regard, China has made itself notorious as a source country from which many such attacks arise. The relationship between information-rich firms such as Google, Microsoft, and Apple, mobile-phone providers such as Verizon, and government is even more complicated (Savage, Wyatt, and Baker, 2013; Greenwald, 2014). Industry often relies on government to help it stave off foreign cyberattacks but there are also times when firms have gained expertise or access that a government would like to tap into. Sometimes the government uses commercial platforms to advance its surveillance or information-gathering methods without the full knowledge and cooperation of the firm, as was disclosed from material revealed by Edward Snowden, the former subcontractor for the US National Security Agency (NSA) who sought diplomatic asylum in Russia after he revealed NSA secrets and became a US fugitive (Ball, Borger, and Greenwald, 2013; *New York Times*, 2013).

Understanding the nature of cyberattacks sheds light on why the spheres of defence and offence are not clear cut. When a country or actor launches a cyberattack, it reveals something of its own capability, even of its own vulnerability (Harris, 2009). The attack shows some of the know-how, engineering, and expertise needed to launch it—all offering clues about the attacker's capabilities. It is like a missile with a blueprint. The missile may explode but the blueprint stays fully intact for the receiving party to study at length (Kemp, 2012). It is important to realize that APTs are generally able to trace quite precisely where a cyberattack came from. It may take time but few (if any) remain a mystery (Brenner, 2012; Clarke and Knake, 2010; Lindsay, 2013). And there is more that is given away by the country or group launching a cyberattack. When the United States or Canada discover a cyberattack, they may learn something about the level of sophistication of their opponent and also about the information their opponent is seeking, though some APTs such as Russia are improving the stealth level of their attacks to make such information less clear (Singer and Friedman, 2013).

An important ingredient of the logic of cybersecurity is that a country should engage in some offence in order to strengthen its defence. Trying to detect and prevent intrusions, such as is done in the civilian US government systems called EINSTEIN (US, Executive Office of the President of the United States, 2009a) or the NSA's purported MonsterMind capability (Bamford, 2014; Zetter, 2014), is not yet regarded as highly effective. In the balance of weaknesses among competing countries, you do not want to be the state that is most vulnerable because you have not honed your skills in finding zero-day exploits or in using them. If attacked, the ability to reverse-engineer a counterattack may be crucial in preventing a future attack. So you must train and practice and let the attacker know that you know what it is doing and that you can still respond.

For states to launch a successful cyberattack against politically- or militarily-important targets, such as defence agencies or nuclear-weapons programs—targets that are generally more "hardened" than commercial targets—prolonged access into the target's systems or networks is required. Thus, an APT may want to have multiple zero days so that it can increase its probability of success (Weinberger, 2011; Collins and McCombie, 2012). At the same time, offensive action means giving away some of your own expertise (Kallberg and Bhavani Thuraisingham, 2013) and most certainly invites retaliation. *Stuxnet*, the Israeli-American cyberattack on Iran's nuclear enrichment process (see below), for example, was quite effective in its immediate objective of slowing down that process. But once Iranian scientists realized something was amiss inside their systems, they sought outside technical assistance, at which time *Stuxnet* was discovered. Moreover, in apparent retaliation, Iran launched data-wiping attacks on Aramco's operations in Saudi Arabia (Perlroth, 2012).

The dynamic of cybersecurity is thus not that Canada and the United States are the "poor" victims being attacked by all the "bad guys" in cyberspace. Rather, everyone who can is probing and learning in cyberspace. Every APT is engaged in various forms of defensive and offensive activities. It is the new Wild West, in some sense, where the arm of international law has not yet arrived. To be sure, there have been calls for "norms and standards regarding the use of cyberspace and cyber security," including at the United Nations level (Meyer, 2010). Committees in the UN's General Assembly have called for norms of responsible state behaviour and transparency. However, only one international agreement in the area of cybercrime is now in effect. Both Canada and the United States are signatories to the Convention on Cybercrime drawn up by the Council of Europe, which became effective in 2004. Both Russia and China are openly critical of this international convention. The international agreement seeks "to combat computer-related crimes worldwide through harmonizing national legislation, enhancing law enforcement and judicial capabilities, and improving international cooperation"

(Archik, 2006: 2). Verifiable arms control, non-proliferation, and disarmament as developed in the conventional, nuclear, and chemical realms are not easily transferred to the domain of cybersecurity.

The absence of formal international agreements on cybersecurity does not mean there are no rules or boundaries in practice. The rule of consequences and of self-interest is in play, as is the logic of cost-benefit in escalation. For example, using cyberspace to inflict fatalities on foreign citizens or physical damage to key economic assets is not something APTs would consider lightly. Experts debate whether such extensive attacks are even possible given current capabilities (Rid, 2013; Libicki, 2009; Samaan, 2010; Clarke and Knake, 2010). To illustrate: it may be possible to interfere with the operation of a large dam via cyberspace from abroad, but destroying the concrete structure and drowning a city down river is quite another matter. To be sure, President Barack Obama is on record warning hostile players that cyberattacks are not isolated from the rest of defence policy and national security. In 2011, he used the loaded term "all necessary means" to describe the possible American reaction should the nature of the attack so warrant (U.S. White House, 2011: 14). Interestingly, Russian military officials have argued that "the use of information warfare against Russia or its armed forces will categorically not be considered a non-military phase of a conflict, whether there were casualties or not" (Hildreth, 2001: 11).

If deterrence is what kept the peace during the Cold War and the Nuclear Age, resilience may be the governing principle of the Digital Age. Deterrence, after all, works best when your adversaries have a clear idea of what you can and will do if attacked (Betts, 2013). Yet, in cyberwarfare, secrecy is paramount in maintaining a competitive edge. Defining what weapons you will retaliate with when attacked invariably reveals part of your capabilities. Having an effective deterrent in cyberspace is thus problematic. The apparent attack by the North Korean government under the name of "Guardians of Peace" against the Sony Corporation in late 2014 seems to have set off a US reaction. The wiper malware used against Sony wreaked havoc on the company and brought to a halt its imminent release of the satirical movie about Kim Jong-un called "The Interview". A few days later, North Korea's admittedly small Internet went dark for a period of time. Possibly, Obama made good on his threat that North Korea's "cyber vandalism" would be met with "a proportional response" (Perlroth and Sanger, 2014, December 22).

In short, the operational concept best suited for cybersecurity per se is resilience. Resilience is quite different from deterrence, since resilience presupposes weathering an attack, while the aim of deterrence is to prevent an attack through the avowal of overwhelming retaliation. Moreover, given that the nature of cyberattacks is still evolving and that attackers increasingly use third and fourth parties to channel their attacks, and thus create false leads for those trying to find the attacker (Geers, 2010), traditional notions

of deterrence may not apply in cyberspace. A better defence is the ability to sustain one or more cyberattacks and to be able to counter and restore defensive capacity (Lindsay, 2013). How you recover and how you function when compromised becomes of utmost importance.

This appears to be the path NATO has chosen. The alliance regularly conducts defensive war games, such as Baltic Cyber Shield and Locked Shields, in cyberspace. In 2013, NATO defence ministers agreed to establish Rapid Reaction Teams to provide better protection for NATO's networks (NATO, 2014a). In 2014, the alliance declared cyberdefence "part of NATO's core task of collective defence" and noted that cyberattacks could lead to invocation of Article 5 of the North Atlantic Treaty, NATO's all-for-one collective defence commitment, which has been the foundation of Western deterrence since 1949 (NATO, 2014b: §72). Still, NATO's 2011 policy on cybersecurity focuses on "prevention, resilience and defence of critical cyber assets to NATO and Allies" (NATO, 2011: 1).

Three Case Studies of Cyberoperations

We offer three brief case studies to illustrate the nature of cyberoperations conducted by three of the largest APTs. None of these are exhaustive examinations of the activities undertaken by these states, but they do illustrate how a lack of cybersecurity is exploited. In the case of Russia, we note the development of hybrid warfare. This is a type of state-led organized violence in which cyberoperations are launched alongside asymmetric warfare and conventional military operations, as we have seen in Georgia and Ukraine. In the case of US-Israeli action against Iran, we note two things: the sophisticated technical nature of the cyberoperation and, at the same time, the limited or targeted political nature of the attack, namely to support the overarching diplomatic goal of stopping Iran from developing nuclear weapons. In the case of China, we note the predominant theme of industrial espionage and, increasingly, industrial blackmailing.

Russia's hybrid warfare

Estonia's brush with cyberwar started after the Estonian government decided to relocate a Soviet-era war memorial. The decision incensed Russia. What followed has been called "Web War I" and "a cyber-riot" (Davis, 2007; NATO Review, 2013). Cyber-savvy Russian nationalists—likely a group contracted by the government in Moscow—unleashed a volley of "distributed denial of service" (DDoS) attacks that crashed Estonian websites with countless computer-generated "zombie" hits, flooded servers in Estonia with junk data, and overwhelmed Estonian networks. The attacks, which lasted about three weeks in the spring of 2007, disrupted Estonia's communications infrastructure, targeting newspapers, the mobile-phone network, the country's largest bank, and key government web sites, including those of the president, prime minister, parliament, and foreign ministry. The impact of the attacks "harmed the state's ability to carry out its administrative functions in accordance with applicable law" (Tikk, Kaska, Rünnimeri, Kert, Talihärm, and Vihul, 2008: 11).

Unlike the cyberattacks against Estonia, the 2008 cyberattack against Georgia was conducted in combination with conventional military operations, "making it among the first cases in which an international political and military conflict was accompanied … by a coordinated cyber-offensive" (Tikk, Kaska, Rünnimeri, Kert, Talihärm, and Vihul, 2008: 4–5). It thus "demonstrated that cyber-attacks have the potential to become a major component of conventional warfare" (NATO, 2014a). According to a study conducted by NATO's Cooperative Cyber Defence Centre of Excellence, "[t]he methods of cyber-attacks against Georgia primarily included defacement of public websites and launch of distributed denial of service attacks against numerous targets", including the parliament, foreign affairs ministry, office of the president, foreign embassies, TV stations, newspapers, and the nation's largest commercial bank. The attacks "severed communication from the Georgian government" to its citizens and its allies (Tikk, Kaska, Rünnimeri, Kert, Talihärm, and Vihul, 2008: 5, 15).

Before and during Russia's annexation of Ukraine's Crimean peninsula in 2014, Ukrainian computer networks, including networks run by the government in Kiev, were hit by a virus "comparable in its complexity with *Stuxnet*", the computer worm that crippled Iran's nuclear program (Jones, 2014, March 7). The origins of the "Snake" virus that targeted Ukraine are reportedly unclear, but "its programmers appear to have developed it in a GMT+4 time zone—which encompasses Moscow" (Jones, 2014, March 7).

Finally, a recently unearthed piece of malware known as *Havex* began targeting US and European firms in 2011. Due to its target (companies involved in energy acquisition and production) and its apparent source (Russia), *Havex* has been dubbed "Energetic Bear" in the West. Like *Stuxnet* (see below), the goal of Energetic Bear was to "compromise" networks and then "control" them (Clayton, 2014, July 1).

American-Israeli "coercive" diplomacy

In 2006, press accounts reported that the George W. Bush administration authorized the "Olympic Games" cyberoperation against computer systems that ran Iran's nuclear program. The operation began with US and Israeli agencies identifying vulnerabilities in the computer systems themselves, which were provided to Iran by Siemens. Those vulnerabilities were then used as pathways for cyberattacks against Iran's nuclear program (Broad, Markoff, Sanger, 2011).

The Obama administration continued and expanded the effort, which included the now-famous *Stuxnet* computer worm. *Stuxnet* had two major components: one was designed to destroy Iran's nuclear centrifuges; another "secretly recorded what normal operations at the nuclear plant looked like, then played those readings back to plant operators … so that it would appear

that everything was operating normally while the centrifuges were actually tearing themselves apart" (Broad, Markoff, and Sanger, 2011). *Stuxnet* quietly ripped through Iran's nuclear program for 17 months, targeting the operating systems running the program; tricking centrifuges into running faster than normal, then abruptly slowing them down; and confounding Iran's nuclear scientists. Along the way, another cyberweapon was developed known as "Flame"—a piece of malware that targeted computers belonging to Iranian officials to gather intelligence used in *Stuxnet*'s sabotage.

Hundreds of system-critical computers and approximately 1,000 centrifuges (out of 5,000) were knocked out, and Iran's drive to develop a nuclear weapon was set back several months (Sanger, 2012a). *Stuxnet* became the first major cyberattack "used to effect physical destruction," according to Gen. Michael Hayden, who served as Bush's CIA director and NSA director (Sanger, 2012b).

In 2012, Iran launched *Shamoon*, a sophisticated computer virus that targeted the Saudi oil company, Aramco, and Qatari natural-gas giant, RasGas. It is quite possible that some of the expertise to do this was gained from the attacks Iran itself suffered. *Shamoon* "rendered inoperable—and effectively destroyed the data on—more than 30,000 computers" (Alexander, 2013) and, in the case of Aramco, "replace[d] the data on the hard drives with an image of a burning American flag" (Perlroth, 2012). *Shamoon*, according to former US Defense Secretary Leon Panetta, "was probably the most destructive attack that the private sector has seen to date" (Panetta, 2012). Although the attacks did not target the United States and Israel directly (perhaps they were unable), they nevertheless signaled that Iran is not a weak state incapable of threatening valuable interests in cyberspace (Perlroth, 2012). At present, Iran has second-tier capabilities for cyberoperations. Nevertheless, its growing capabilities suggest that one day (perhaps much sooner rather than later) it could narrow the gap between its capabilities and America's (Mandiant, 2014; Lewis, 2014; Perlroth, 2012).

China's economic cyberexploits

China's cyberoperations at first focused on espionage, gathering "political, military, corporate-strategic and scientific information in order to bridge technological gaps as quickly as possible" (US Defense Department, 2008: 4). A study conducted for the US-China Economic and Security Review Commission adds that China's use of "computer network exploitation activities to support espionage has opened rich veins of previously inaccessible information that can be mined both in support of national security concerns and, more significantly, for national economic development" (Krekel, Adams, Bakos, 2012: 107). However, the attacks are becoming more diversified and range beyond normal espionage activity.

In 2013, information-security firm Mandiant pointed to "an army unit in China" as the source of these attacks (US Senate Subcommittee on Emerging Threats and Capabilities, 2103). This supported the Pentagon's conclusion in 2007 that the People's Liberation Army (PLA) had "established information warfare units to develop viruses to attack enemy computer systems and networks" (US Defense Department, 2007: 22). The Mandiant report details a cybercampaign that has "penetrated the networks of at least 141 organizations" (US-China Economic and Security Review Commission, 2013: 15). The report claims that a PLA cyberforce known as "Unit 61398" is conducting "extensive" computer network operations (US Senate Subcommittee on Emerging Threats and Capabilities, 2013: 4–5). The following list highlights how Chinese actors are exploiting cyberspace:

- Planting computer components with codes that can be activated to destroy data or take control of critical infrastructure or financial networks in numerous countries, including the United States and Canada, and various US federal government offices. In a 2007 case, some 1,500 computers in the Pentagon were affected (Krekel, 2009; Gorman, 2012).

- Infiltrating subcontracting firms and systems related to the development of the Joint Strike Fighter (Gorman, Cole, Dreazen, 2009). The warplane represents the future backbone of air forces in the United States, Canada, Britain, Italy, Netherlands, Turkey, Australia, Denmark, and Norway (US Defense Department JSF Program, 2014).

- Conducting "cyber-warfare against civilian and military networks—especially against communications and logistics nodes" (US Defense Department, 2008: 21). The US Transportation Command (TRANSCOM) mission includes air-refueling and logistics and depends on many civilian subcontractors (Krekel, Adams, Bakos, 2012: 34–37).

- Conducting cyberattacks against Defence Research and Development Canada, the Finance Department, and Treasury Board. The 2011 attacks forced Canada's chief economic agencies to unplug from the Internet (NATO Review, 2013). A similar Chinese intrusion occurred in 2014 against the National Research Council (NRC), the Canadian government's principal R&D organization, which works closely with the private sector. The NRC was forced to shut down and quarantine its networks to prevent the attack from spreading (Boutilier, 2014).

- Stealing "user credentials" for more than 150 NASA employees and gaining "full functional control over networks at the Jet Propulsion Laboratory" (US-China Economic and Security Review Commission, 2012: 9).

- Orchestrating successful computer breaches within the foreign ministries of the Czech Republic, Portugal, Bulgaria, Latvia, and Hungary (Perlroth, 2013).

- Hacking into Boeing's C-17 Globemaster project in 2013. (The Globemaster is a military cargo plane used by both Canada and the United States.) A three-person team led by Chinese citizen Su Ben has been accused of this crime. Su was arrested in Canada. As of this writing, his extradition to the US is pending (Minnick, 2014).

- Launching "spearphishing" attacks—a tactic using email that appears to be from a trusted source to gain access to a target's computer—against Westinghouse Electric, Alcoa, Allegheny Technologies Incorporated, US Steel, the United Steelworkers Union, and SolarWorld. The five men indicted by the US government on account of this crime all serve in the PLA's Unit 61398 (US Department of Justice, 2014; US District Court Western District of Pennsylvania, 2014).

A more exhaustive tally of cyberincidents attributed to China has been produced by Laura Saporito and James A. Lewis of the Center for Strategic and International Studies (2013).

Another concern with Chinese cyberattacks stems from the close relationship between the central government and the many state-owned enterprises. A case in point is the telecommunications giant Huawei. US officials have tried to dissuade American firms in the defence and telecommunications arenas from contracting with Huawei (Harris and Fish, 2013). In 2011, for instance, Washington blocked Huawei from building a wireless network for emergency responders and, in 2013, Washington urged South Korea to exclude Huawei from participating in a wireless-network project (Entous, 2013). Some US officials suspect firms like Huawei of placing a "bug, beacon, or backdoor" into critical systems that could allow for "a catastrophic and devastating domino effect … throughout our networks" (Harris and Fish, 2013). The atmosphere of mistrust forced Huawei CEO Ren Zhengfei to announce in late 2013: "We have decided to exit the US market" (Harris and Fish, 2013).

The fact that Huawei has been involved "either directly as a vendor or indirectly as a research collaborator with various PLA-affiliated organizations or universities weakens claims by Huawei's leadership that it maintains no ties with the Chinese government or the military" (Krekel, Adams, Bakos, 2012: 75). The US-China Economic and Security Review Commission concludes that subsidies as well as collaborations with the PLA and other government entities suggest that "an ongoing relationship between Huawei and the Chinese military and Chinese political leadership may exist" (Krekel, Adams, Bakos, 2012: 75).

Huawei's alleged success in quietly and pervasively compromising systems has also heightened concerns in the British government that utilities-network upgrades carried out by Huawei may have given Beijing the ability to shut down essential services (Smith, 2009). The vulnerability of these systems already has been shown by natural disasters, human error, and software failures, as Canadians and Americans learned first hand during the August 2003 power outage (Alexander, 2010).

A senior systems-security official with the now-bankrupt Canadian telecommunications firm Nortel blames Huawei for hacking into Nortel, stealing vast amounts of intellectual property, and effectively killing the corporation in the process (Payton, 2012). Nortel's secrets were systematically stolen for almost 10 years, but the company did not become aware of China's extensive access until years after the initial attack (Gorman, 2012).

Canadian officials openly blamed the 2014 intrusions into the NRC's systems on a "highly sophisticated Chinese state-sponsored actor" (Boutilier 2014, July 29). Moreover, in 2011, the Canadian government reported cyber-attacks against Defence Research and Development Canada, the Finance Department, and the Treasury Board that caused Canada's key economic agencies "to disconnect from the Internet" (NATO Review, 2013). Emanating from China, the attacks targeted computers of senior government officials in an effort to gain access to government data and systems (Vieira, 2011). The attacks exposed a lack of preparedness and comprehension of the magnitude of the threat. Consider that the contingency plan for continuity of operations was, apparently, directing thousands of government employees to use home Internet connections or "wireless Internet connections at nearby cafes," as the *New York Times* reported at the time (Austen, 2011, February 17).

Risks and Costs of North American Cybersecurity

Both the American and Canadian governments (the latter more slowly) have developed strategies to limit, if not prevent, the damage cyberattacks by nation-states and non-state actors can inflict on the economic vitality, trade position, critical infrastructure, and security of the two North American neighbours. The Canadian and American strategies generally focus on three categories of threats: other states attempting to steal Canadian and American secrets; organized crime using cyberspace to make illegal profits; and terrorists using the Internet to recruit members and raise funds (Public Safety Canada, 2010; US, Executive Office of the President of the United States, 2009b; Cilluffo and Cardash, 2013). In addition, as nation-states and non-state actors progress from merely disruptive to destructive attacks, Canada, the United States, and their allies are devoting increasing attention to threats not only against national or economic security but also against the integrity of the systems and networks that support these functions.

Of the three threats, states with a well-developed capability for cyberattacks—the "Advanced Persistent Threats," or APTs, mentioned above—pose the greatest danger to national and economic security. These adversarial states possess the ability to execute sophisticated and unrelenting cyberattacks (Winterfeld and Andress, 2012: 4, 8–10). The most important distinguishing feature is the high level of expertise an APT possesses. The APT category is further divided between states such as the United States, United Kingdom, Russia, China, Israel, and France that possess superior capabilities and other states—like Canada—that possess some capability but have not reached the same level of sophistication (Brenner, 2011; Clarke and Knake, 2010; Carr, 2012; Lewis, 2013). Of the states with superior capabilities, China is the top intruder into government and private-sector networks in Canada and the United States.

Adding a complicating layer to cybersecurity are "insider" vulnerabilities. At the time the Canadian and American cyberstrategies were published (in 2010 and 2009, respectively), the scandals surrounding Jeffrey

Delisle, a Navy sub-lieutenant who stole and sold information from classified Canadian systems to Russian intelligence (Freeze and Taber, 2012), and Edward Snowden, who stole and leaked over 200,000 documents classified "top secret" or "special intelligence" (Hosenball, 2013, Nov. 14), had not yet come to light. "Insider threats" is the name given to these types of actors: individuals who possess legitimate system access and knowingly or unknowingly compromise government systems or critical infrastructure (Winterfeld and Andress, 2012: 83–84).

Cyberattacks include gaining unauthorized access to privileged or proprietary information and causing disruption to IT and other infrastructure that may result in physical disruption or damage. By gaining control of critical switches and the networks that control key infrastructure, a cyberattack could derail passenger trains, contaminate drinking-water supplies, and shut down power grids (Panetta, 2012). When asked in early 2014 what threshold a cyberattack would have to reach to trigger a US military response, Gen. Keith Alexander, first commander of the US military's Cyber Command, replied: "If it destroys government or other networks, I think it would cross that line" (Clark, 2014). Alexander predicted in 2012 that the "transition from disruptive to destructive attacks" is coming (Alexander, 2012). A Chinese general recently warned that the consequences of cyberattack "may be as serious as a nuclear bomb" (Perlez, 2013, April 22). Panetta, warned in 2012 that cyberattacks could "disable or degrade critical military systems and communication networks," leading to "a cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life" (Panetta, 2012). While some experts have challenged the parallel to Pearl Harbor as rhetorical exaggeration, the fact that senior defence officials within major military powers are saying these things says something at the very least about the worries generated by cyberspace.

Publicly available data about cyberattacks and cyberevents is still fragmented and incomplete. However, a trend is visible: both the associated costs and risks of cyberattacks are increasing. The number of cyberattacks on the United States rose 44% between 2010 and 2011 (Alexander, 2012). There are cascading economic costs—and rising national security and public safety risks—associated with these forms of cyberattack.

The research on quantifying the cost of failures in cybersecurity has only just begun. The two cost categories discussed here (cost to business and cost to government) have only a few studies, and these offer estimates rather than measurement (Public Safety Canada, 2011).

Cost to business

A 2013 study by the Center for Strategic and International Studies (CSIS) in Washington, DC, separates "malicious cyber-activity" into six parts:

1. loss of intellectual property and confidential information;
2. cybercrime;
3. loss of sensitive business information:
4. opportunity costs, including "service and employment disruptions, and reduced trust for online activities";
5. costs of securing networks, insuring IT systems and recovering from cyberattacks;
6. reputational damage to the victim. (CSIS, 2013: 3)

This broad definition of malicious cyberactivity helps explain why estimates of the economic costs are imprecise. As CSIS notes: "The wide range of existing estimates of the annual loss—from a few billion dollars to hundreds of billions—reflects several difficulties". First, many companies hide their losses and/or fail to report cyberevents. Some are not even aware they have been victims of a cyberattack (CSIS, 2013: 3). Indeed, Alexander noted in 2012 that 162 of 168 Fortune 500 companies surveyed report being victimized by cyberattacks of some sort. But the scope and scale of the danger is much worse: "They're the ones that know they're being hacked … there are more than a hundred companies for every one that knows they've been hacked that don't know they've been hacked" (Alexander, 2012). In 2013, the US government notified more than 3,000 companies—many of them defence contractors—that their computer networks and systems had been compromised by hackers (Nakashima, 2014).

The costs range beyond patching security gaps and lost revenue. Pointing to figures produced by the US Commerce Department's International Trade Administration that extrapolate export values into US jobs, CSIS concludes that the high-end estimate of $100 billion in US losses from cyberespionage "would translate into 508,000 lost jobs … roughly a third of a percent decrease in employment" (CSIS, 2013: 17).

A 2014 study on the economic costs of cyberespionage and other forms of cyber-attack conducted by CSIS on behalf of McAfee estimates the global costs of what it calls "malicious activity" at between $375 billion and $575 billion (CSIS, 2014: 6). Other studies on the economic global costs of cybercrime have estimated the figure as high as $1 trillion (Greenberg, 2012). Some 431 million people are victimized in cyberspace per year, and cybercrime represents an economy "larger than the global black market for marijuana, cocaine, and heroin combined … and approaching the value of all global drug trafficking" (Deibert, 2012: 11). According to a global survey of IT decision-makers conducted by McAfee, "[i]t costs an average of almost $600,000 per firm to respond to each security breach concerning the loss of vital information such as intellectual property" (McAfee, 2009: 7).

The upper-end figure of $1 trillion has drawn questions and criticism (Greenberg, 2012). In defending its 13-figure estimate, McAfee noted: "The

number was intended to provide a sense of scope around the very real problem of data and intellectual property loss" due to cyberattack, adding that "the issue is truly gigantic in scope and growing" (Greenberg, 2012, August 3). That point appears beyond debate.

The CSIS estimate of "malicious" cyberactivity costing between $375 billion and $575 billion is imprecise. However, it does give us a starting point—a sense of how important and significant cyberspace is to the global economy, how reliant the world is on this domain, and how this zone of commerce, communications, and collaboration is being exploited by many actors to pursue nefarious ends. CSIS noted that Canada's proportional cost of cybercrime was significantly lower than in the United States (0.17% versus 0.64% of GDP) but the main reason for this gap may be underreporting, including by business firms, and lack of systematic data of the economic costs of cyberattacks in Canada (Ligaya, 2014).

Cost to government

The cost to government is significant but underestimated. Individual departments report various expense categories that appear incomplete in part because IT and cyberprotection programs are widespread and integrated into how agencies operate and it is difficult to extract the exact cost devoted to security.

The US Office of Management and Budget reported that in 2012, "federal agencies spent more than $15 billion on cybersecurity-related projects and activities" (CSIS, 2013: 12). The US Defense Department alone is investing more than $3 billion annually in cybersecurity (Panetta, 2012). In 2010, the United Kingdom announced it would "set £650 million aside over four years" toward a new "National Cyber Security Programme". Half of these resources are earmarked for detecting and countering cyberattacks (UK Cabinet Office, 2011: 27). Canada, in comparison, spends much less: only "$90 million over five years, and $18 million in ongoing funding" was initially allocated for cybersecurity (Press, 2012, October 17). Amid criticism of Canada's comparatively modest spending on cyberdefence, Canada increased its investment to $155 million over five years to 2016 to "reinforce the Government's cyber security capabilities" (Public Safety Canada, 2013: 6; MacDonald and Vieira, 2012).

North American Cybersecurity Cooperation: Canada, the United States, and the Five Eyes

Both the Canadian and American cyberstrategies recognize the shift in threats over the past five years. In 2004, cyberattacks were considered a low-risk threat by the government of Canada. Today, cyberattacks are "about as high as terrorism in terms of national security threats" (Canada, SSCNSD, 2012a). Canada's *Cyber Security Strategy* notes that the Canadian federal government is increasing the resilience of government systems, pursuing public-private partnerships to secure critical infrastructure, sharing information about cybersecurity with the public, and enhancing police powers (Public Safety Canada, 2010: 1). The American *Cyberspace Policy Review* calls on the US to "improve [its] … resilience to cyber incidence" through infrastructure hardening, and defence and recovery tactics (US, White House, 2013). Cyberthreats will be confronted through international partnerships, deterrence strategies, and "appropriate responses for … state and non-state actors" (US, Executive Office of the President of the United States, 2009a: 5). In 2011, the United States released its *International Strategy for Cyberspace*, which formalized the *Policy Review* into an actionable agenda for international collaboration (US, Executive Office of the President of the United States, 2011).

On a state-to-state level, Canada and the United States have an extensive history of working together through the Five Eyes alliance (Gendron, 2013). The 1946 UKUSA Agreement formalized an intelligence-sharing arrangement between the United States, the United Kingdom, Canada, Australia, and New Zealand that began in World War II and remains in force today (National Security Agency, Central Security Service, 2010). The Five Eyes—a shorthand that refers to the alliance members (Cox, 2012)—predominantly targeted states of the Soviet bloc during the Cold War (Rudner, 2001). After the Cold War, the alliance shifted its focus to tackle competing threats from multiple states and actors.

To ensure adequate coverage, the Five Eyes divided the world up into five regional clusters, one for each alliance member (Richelson, 1990). Unofficial accounts suggest that Canada covers the Arctic, Latin America,

and the North Pacific and North Atlantic Oceans. The United States surveys "the Caribbean, China, Russia, the Middle East and Africa". The United Kingdom is responsible for Europe and Western Russia, while Australia and New Zealand cover South and East Asia, and the South Pacific and Southeast Asia, respectively (Cox, 2012: 6; Rudner, 2001: 103).

The United States possesses cyberintelligence capabilities that are significantly more advanced than most states (Nye, 2011), yet alone it is unable to gather the volume of information it needs. Cooperation with the Five Eyes is necessary to reduce this intelligence deficit. Without the Five Eyes, America could only "collect [information] … against a part of the target" (Lander, 2004: 492). Cooperation provides more information so the US government can prepare more effectively for the threats it faces directly, and the threats its allies face that could spill over to the United States (Cilluffo and Cardash, 2013). Cooperation between Canada and the United States in the cyberrealm is largely embedded in, and a by-product of, the Five Eyes regime. As with much of the Canada-US partnership on security-related matters, Canada-US cooperation for cybersecurity goes even further than the Five Eyes. Close cooperation occurs between the NSA and the Communications Security Establishment (CSE)[2] to target "approximately 20 high-priority countries" in the collection of signals intelligence (SIGINT) (US, National Security Agency, Central Security Service, 2013).

A capabilities gap exists between the United States—the primary, technologically advanced, well-resourced partner—and the secondary Five Eyes partners (Lefebvre, 2003). Since Canada has a more limited ability to develop sophisticated technology, Canada acquires and uses NSA capabilities (US, National Security Agency, Central Security Service, 2013) to help manage its portion of the partnership's mission. Inevitably, the United States influences some of the intelligence gathering done by Canada.

US-Canada resource-sharing in the cybersphere—including hardware, software, and personnel—means that the NSA and CSE are relatively well integrated (US, National Security Agency, Central Security Service, 2013; Rudner, 2001). While integration increases efficiency, it also increases the prospect of a cyberattack against one partner spreading to another. *Titan Rain*, for example, was a series of coordinated cyberattacks from 2003 to 2005 that originated from China (Markoff, Sanger, and Shanker, 2010). Although *Titan Rain* initially stole information from the systems of the US Department of Defense, it later spread to other "sensitive government and private-sector systems" (Porteous, 2011: 1). By 2005, *Titan Rain* had infiltrated the systems of the Five Eyes governments, amongst other American allies (Porteous, 2011; Thornburgh et al., 2005). Likewise, an attack against a Five Eyes ally could

2. Formerly, Communications Security Establishment Canada (CSEC). See <https://www.cse-cst.gc.ca/en>; MacCharles, 2014, October 31.

spread into the United States via the allies' integrated cyberintelligence assets. An adversary in cyberspace may only need to penetrate one Five Eyes system to find and retrieve American secrets through the linked networks (Cox, 2012). Interoperability, while efficient, is perhaps more of a double-edged sword in cybersecurity than in conventional military defence.

Canadians should not underestimate the benefits they gain from America's willingness to share advanced capabilities. The NSA's US$10.8 billion budget (Gellman and Miller, 2013) easily dwarfs CSE's 2013 budget of CA$460 million and 2014 budget of CA$829 million (Freeze, 2013; Treasury Board of Canada Secretariat, 2014). To upgrade CSE's capabilities to roughly equivalent NSA levels would require a very large increase in its budget, a costly and most unlikely investment. Instead, Canada has "access to a $15 billion global [information-sharing] partnership" that imparts vital intelligence on key "threats and … technological challenges" through the Five Eyes (Canada, SSCNSD, 2012b). Participating in the alliance provides Canada with access to a multi-billion dollar intelligence apparatus without needing to make equivalent investments in its own SIGINT capabilities. Cooperation is decidedly cheaper than independently developing competitive intelligence capabilities (Sims, 2006).

Access to American capabilities and the dynamic of an alliance relationship, such as the Five Eyes, includes US requests on Canada's intelligence collection. Several Canadian embassies, for example, have been set up as listening posts at the request of the NSA (LeBlanc and Freeze, 2013; Weston, Greenwald, and Gallagher, 2013b). More recently, Canada allowed the NSA to carry out surveillance during the 2010 G20 Summit in Toronto. The specifics of Canada's involvement are unknown, but a leaked memo points to close operational cooperation between the NSA and "the Canadian partner" during the G20 (US, National Security Agency, 2010: 3; Weston, Greenwald, and Gallagher, 2013a).[3]

To carry out its Five Eyes mission—defending government systems in cyberspace and providing intelligence to support governmental decision-making (Cox, 2012)—Canada relies in part on American capabilities and, specifically, US intelligence. This means that the United States, in turn, can influence Canadian intelligence priorities (Richelson, 1990). In this relationship, Canada is, of course, in a more dependent position. The government of Canada must thus keep its eye continually on both the effectiveness of its cooperative cybersecurity network with the United States and the sovereign Canadian parameters for security and privacy. Despite some of the embarrassing leaks emanating from the Snowden incident, the relationship's disadvantages are outweighed by Canada's continued access to high-level American

3. The Canadian Government has denied spying on the G20 but did not explicitly deny cooperation with its SIGINT allies. See Weston, Greenwald, and Gallagher, 2013a.

intelligence and the advanced technologies Canada and the United States use together to confront the ever-evolving threat of cyberattacks (Richelson, 1990). At the same time, on a balance of vulnerabilities, cooperating with the Five Eyes and Canada in particular provides an important means for the United States to expand its global surveillance reach (Bauman et al., 2014) and to enhance North American cybersecurity.

Canada draws a clear net benefit from close cooperation with the United States in cybersecurity because the nature of the evolving threat and the nature and cost of countering this capacity is increasingly more difficult for a state to address on its own. At the same time, the Canadian government faces a balance between security and the Canadian definition of freedom as it cooperates with the United States and Five Eyes. Surveillance capacity, like capacity for cybersecurity, is on the increase. Managing the information that results from this capacity remains a key value that both the American and Canadian public demand.

Governing Cybersecurity and Freedoms

The focus of this report is on cybersecurity because, without a robust level of security, the benefits of the extended liberty provided by the Internet would dry up. High vulnerability of all in society, the lack of international governance in cyberspace, and the need for high levels of expertise point to a continuing role for national governments. The benefits of an open web can only continue if we have both an open and secure web.

As in other domains of political and commercial activity, there is a trade-off: as government intervention increases, there is a promise of greater security, but that security comes with economic costs and potential limits on liberty and privacy. This trade-off, it seems, is inescapable, but requires continuing management. If there is a see-saw between the two, we do not want all security and no liberty nor all liberty and no security. The call for keeping cyberspace open and non-balkanized is vital. We see authoritarian societies such as Russia, China, and Iran limiting the freedom of their national Internet, effectively turning them into giant but controlled intranets. The loss of information, education, and commerce, not to mention the loss of political ideas, are all at stake.

Long before there was such a thing as cyberspace, Adam Smith noted that "the first duty of the sovereign" is to protect society from "violence and invasion" (Smith, 1776/1991: 689). What serves as the launching pad for violence or invasion—land, sea, sky, space, or cyberspace—diminishes neither the danger nor the sovereign's duty to confront it. The problem is that in protecting against insecurity in cyberspace, the sovereign has relatively less power than we may assume and the sovereign's activities to protect include various potential activities that might infringe on commercial or individual freedoms.

In short, finding an acceptable balance between liberty and security in cyberspace is difficult. Overemphasizing security can "severely restrict one's freedom of choice," as how individuals gain access to cyberspace, with whom they interact, and how they behave becomes inhibited (Greenwald, 2014: 173). Excessive legislation or regulation on cybersecurity can also stifle entrepreneurial potential. Conversely, liberty without an appreciation of cybersecurity presents rising commercial and governmental costs and unacceptable threats

to national security. An individual unaware of how "a single wrong click today" can have larger consequences upon his livelihood, property, and liberty—as well as the livelihood, property, and liberty of his neighbours or coworkers or employer—presents a significant vulnerability in cyberspace (Singer and Friedman, 2013: 234). Similarly, companies such as Canada's Nortel and the US arm of Japan's Sony Corporation were destroyed or severely disrupted in large part by failures in cybersecurity. We cannot choose only liberty or only security: liberal democracies must aim for both (Alexander, 2009).

In liberal constitutional democracies such as in North America, we expect the freedom to access, use, and conduct legal inquiry and business online as part of our inalienable individual freedoms. Cybersecurity, then, inevitably is composed of two challenges: gaining security against threats in cyberspace and maintaining security as the servant of liberty. The test is to build in sufficient and effective checks and balances on that governmental role so that, on the one hand, security can be enhanced and, on the other, intrusions into individual liberties can be minimized.

Government interventions, including surveillance, can yield enormous information about the threats to a state's economic or national security. Cybersurveillance is also a key aspect of counter-terrorism and de-radicalization, including operations aimed at the recent phenomenon of lone-wolf political violence. Yet, individual liberty, and privacy in particular, can be compromised by the wrong use of data obtained by cybersurveillance (Greenwald, 2014). Gathering information on the bad actors often means that information on ordinary citizens is collected (Gellman, Tate, and Soltani, 2014). In cyberspace there is currently an unfortunate trade-off where, at times, a certain degree of anonymity and privacy—which certainly fall within the sphere of most conceptions of liberty—is violated to enhance security. That sacrifice does not have to lead to harmful results if managed and supervised correctly. We posit that surveillance should be open and largely unencumbered. Note that the nature of threats in cyberspace keeps changing. Therefore, curtailing the government's ability to gather data is too risky a measure. Instead, the key checks should be at the output level and not the input level: how the data is used, interpreted, and stored. The emphasis of checks should be on how surveillance data acquired through wide-net collection mechanisms can be used and stored, and for how long.

Cybersecurity and intelligence are increasingly connected. The 9/11 Commission in the United States pointed to the pitfall of "stove-piping" information as was seen in the lack of sharing and cooperation between the FBI and CIA. In Canada, the expansion of the powers wielded by the Canadian Security and Intelligence Service as well as the coordination of the CSE and NSA will likely mean more combined activity between domestic and foreign cybersecurity and intelligence. This task should not be left to the specialized agencies, such as the Canadian Security and Intelligence Service and CSE, without a layer of oversight by elected representatives. Canada's current

Security and Intelligence Review Committee is not well suited for the task because its officials are not elected and its powers are too limited. As Canada is updating its ability to deal with threats in cyberspace, it needs to enhance the ability of its representative government to oversee this important work. The idea of an all-party committee in Parliament, supported by former CSE Chief John Adams, is a good one (Chase, 2013; Adams, 2014). Members of this committee would have security clearance and the ability to call informed witnesses to ensure a careful review of Canada's cyberoperations (Livermore, 2014). Given the intense partisan climate in Canada, there should also be responsibilities adopted by these parliamentarians so that information would not be used for any other purpose than public safety and security.

In response to the public reaction to revelations made by Snowden about the US government's collection of metadata, President Obama announced plans in January 2014 "to provide greater transparency to our surveillance activities and fortify the safeguards that protect the privacy of US persons" (Obama, 2014). Obama's proposals include:

- reforms within the Justice Department and US national-intelligence apparatus to limit the federal government's ability "to retain, search, and use in criminal cases communications between Americans and foreign citizens incidentally collected";

- reforms in the way the FBI works with commercial entities, especially communications providers, to seek and obtain information used in government investigations; going forward, the Obama administration wants the secrecy surrounding these "national security letters" to be lifted sooner, and to allow communications providers "to make public more information … about the orders that they have received to provide data to the government"; and

- reforms aimed at phasing out certain elements of the metadata-collection program that began after the 9/11 attacks and establishing "a mechanism that preserves the capabilities we need without the government holding this bulk metadata". (Obama, 2014)

Because of the open nature of cyberspace and its predominant private ownership, protecting against, identifying, mitigating, deterring, and dealing with cyberattacks are responsibilities that transcend traditional state-centric security. In other words, cybersecurity cannot be provided by the federal government or by inter-governmental action alone. As detailed above, cybersecurity is a quest for relative advantage and low vulnerability. Cybersecurity has geographic, economic, and public-private boundaries and roles that differ from conventional security and defence. For example, the cyberdefence

exercises codenamed "Cyber Storm", in which Canada and the United States have partnered since 2006, have enfolded 12 allied governments, as many as 60 private-sector firms, and 115 national, state, and local agencies and organizations (US, Department of Homeland Security, 2014).

The Canadian and American cyberstrategies do not say much about "the how" of public-private partnerships in advancing cybersecurity, though both call for close cooperation. Each strategy, in principle, recognizes that the government and the private sector need to work together. It is not a top-down relationship. Actors that attack the private sector can also attack the government. Sharing information can thus support a secure private sector which, in turn, supports a secure government. Creating the necessary conditions to facilitate private-sector cooperation, however, requires a delicate balancing of interests.

Much remains unknown about the Canadian government's reach into the data held by private companies. Nevertheless, regular interactions appear to occur between private actors and the government to discuss threats in cyberspace and exchange information (Lukacs and Grovers, 2013).

The US government's relationship with private companies at times contains undertones of coercion. Some companies, for example, are legally required to hand over their data to the NSA through the PRISM program, as Snowden disclosed (Greenwald, 2014; *Washington Post*, 2013). Such disclosures invariably represent a significant government intrusion into corporate secrets and individual privacy (Nakashima and Warrick, 2013). As mentioned above, the Obama administration is reforming the rules governing these so-called "national security letters" that require companies to share information with the government.

"To be successful in cyberspace, it is going to require government and industry working together with the best of both," Alexander explains (US, Senate Committee on Armed Services, 2012). After all, Google, Amazon, Sun, Oracle, Microsoft, and the like are going to have skills and platforms crucial in advancing cybersecurity. Echoing such sentiments, John Forster, CSE chief, sees "cyber as a team sport; each of us [in government, the private sector, and as individuals] has responsibilities … this is not a Government of Canada issue; this is a Canada issue. [Policymakers] need to provide leadership and coordination in getting everyone on that" (Canada, SSCNSD, 2012b).

All true, but the relationship between government and private business in cybersecurity will not always align around national dimensions. Firms and government agencies make calculations about relative information advantage and low vulnerability. Some US firms after the Snowden leaks, for instance, have shown reluctance to cooperate with the NSA, fearing that their profile in cyberspace is being manipulated by government priorities. This is a difficult public-policy debate that has just begun in the United States and will likely also become increasingly important in Canada.

References

Ablon, Lillian, Martin C. Libicki, and Andrea A. Golay (2014). *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*. RAND Corporation.

Adams, John (2014, February). Terrorism, the Internet, and the Security/Privacy Conundrum. Strategic Studies Working Group Paper. Canadian Defence and Foreign Affairs Institute. <https://d3n8a8pro7vhmx.cloudfront.net/cdfai/pages/96/attachments/original/1414205316/Terrorism_Internet_Security_Privacy_Conundrum.pdf?1414205316>, as of January 18, 2015.

Alexander, Keith (2009, April). *Securing Our Government Networks*. RSA Security Conference in San Francisco, CA. <https://www.nsa.gov/public_info/speeches_testimonies/21apr09_dir.shtml>.

Alexander, Keith (2010, September 23). Statement to the House Committee on Armed Services. US Department of Defense. <http://www.defense.gov/home/features/2010/0410_cybersec/docs/USCC%20Command%20Posture%20Statement_HASC_22SEP10_FINAL%20_OMB%20Approved_.pdf>.

Alexander, Keith (2012, July 9). Remarks at the American Enterprise Institute. <http://www.aei.org/events/cybersecurity-and-american-power>, as of December 7, 2014.

Alexander, Keith (2013, March 13). Statement to the Subcommittee on Intelligence, Emerging Threats and Capabilities Subcommittee of the House Committee on Armed Services. US House of Representatives <http://docs.house.gov/meetings/AS/AS26/20130313/100444/HHRG-113-AS26-Wstate-AlexanderG-20130313.pdf>.

Anonymous (2013, July 10). NSA Slides Explain the PRISM Data-Collection Program. *Washington Post.* <http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/>.

Anonymous (2013, September 5). Secret Documents Reveal N.S.A. Campaign against Encryption. *New York Times*. <http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html?ref=us>.

Austen, Ian (2011, February 17). Canada Hit by Cyberattack. *New York Times*. <http://www.nytimes.com/2011/02/18/world/americas/18canada.html?_r=0>, as of December 12, 2014.

Ball, James, Julien Borger, and Glenn Greenwald (2012, September 6). Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security. *Guardian*. <http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>.

Bamford, James (2014, August). The Most Wanted Man in the World. *Wired Magazine*. <http://www.wired.com/2014/08/edward-snowden/>.

Barford, P., M. Dacier, T.G. Dietterich, M. Fredrikson, J. Giffin, S. Jajodia, S. Jha, J. Li, P. Liu, P. Ning, X. Ou, D. Song, L. Strater, V. Swarup, G. Tadda, C. Wang, and J. Yen (2010). Cyber SA: Situational Awareness for Cyber Defence. In Sushil Jajodia, Peng Liu, Vipin Swarup, and Cliff Wang, eds., *Cyber Situational Awareness: Issues and Research* (Springer): 3–14.

Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jarbi, David Lyon, and R.B.J. Walker (2014). After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology* 8, 2: 121–144. DOI: 10.1111/ips.12048.

Betts, Richard K. (2013). The Lost Logic of Deterrence: What the Strategy that Won the Cold War Can – and Can't – Do Now. *Foreign Affairs* 92, 2. <http://www.foreignaffairs.com/articles/138846/richard-k-betts/the-lost-logic-of-deterrence>.

Boutilier, Alex (2014, July 29). Canadian Spy Agency Says China Hacked into National Research Council Computers. *Toronto Star*. <http://www.thestar.com/news/canada/2014/07/29/ canadian_spy_agency_says_chinese_hacked_into_national_research_council_computers.html>, as of December 12, 2014.

Boutilier, Alex (2014, August 21). NRC Head Says Cyberattack Hasn't Spooked Partners. *Toronto Star*. <http://www.thestar.com/news/canada/2014/08/21/nrc_head_says_cyberattack_hasnt_spooked_partners.html>.

Brenner, Joel (2011). *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. Penguin Press.

Broad, William, and John Markoff and David Sanger (2011, January 15). Israeli Test on Worm Called Crucial in Iran Nuclear Delay. *New York Times*. <http://www.nytimes.com/ 2011/01/16/world/middleeast/16stuxnet.html?_r=1&pagewanted&>, as of January 13, 2014.

Canada, Parliament, Senate, Standing Senate Committee on National Security and Defence [SSCNSD] (2012a). Transcript of Proceedings. 41st Parl., 1st sess. Meeting No. 14. <http://www.parl.gc.ca/Content/SEN/Committee/411/secd/09ev-49764-e.htm?Language=E&Parl=41&Ses=1&comm_id=76>.

Canada, Parliament, Senate, Standing Senate Committee on National Security and Defence [SSCNSD] (2012b). Transcript of Proceedings. 41st Parl., 1st sess. Meeting No. 15. <http://www.parl.gc.ca/Content/SEN/Committee/411/secd/10ev-49784-e.htm?Language=E&Parl=41&Ses=1&comm_id=76>.

Canada, Parliament, Senate, Standing Senate Committee on National Security and Defence [SSCNSD] (2014). Transcript of Proceedings. 41st Parl., 2nd sess. Meeting No. 18. <http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=6511518&Language=E&Mode=1>.

Carr, Jeffrey (2012). *Inside Cyber Warfare: Mapping the Cyber Underworld*. O'Reilly Media.

Center for Strategic and International Studies [CSIS] (2013, July). *The Impact of Cybercrime and Cyber Espionage*. McAfee. <http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf>, as of January 16, 2014.

Center for Strategic and International Studies [CSIS] (2014, June). *Net Losses: Estimating the Global Cost of Cybercrime*. McAfee. <http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf>, as of June 11, 2014.

Chase, Steven (2013, October 8). Former CSEC Boss Calls for More Scrutiny of Agency amid Brazil Spying Claims. *Globe and Mail*. <http://www.theglobeandmail.com/news/politics/former-csec-boss-calls-for-more-scrutiny-of-agency-amid-brazil-spying-claims/article14758480/>, as of January 1, 2015.

Cilluffo, Frank J., and Sharon L. Cardash (2013). Cyber Domain Conflict in the 21st Century. *Journal of Diplomacy & International Relations* 14, 1: 41–47. EBSCOhost (87977324).

Clark, Colin (2014, February 27). CyberCom Chief Alexander Lays Down Cyber Red Line: Destroy A Network, Risk War. *Breaking Defense*. <http://breakingdefense.com/2014/02/cybercom-chief-alexander-lays-down-cyber-red-line-destroy-a-network-risk-war/>, as of March 6, 2014.

Clarke, Richard, and Robert K. Knake (2010). *Cyber War: The Next Threat to National Security and What to Do about It*. Ecco.

Clayton, Mark (2012, September 14). Stealing US Business Secrets: Experts ID Two Huge Cyber "Gangs" in China. *Christian Science Monitor*. <http://www.csmonitor.com/USA/2012/0914/Stealing-US-business-secrets-Experts-ID-two-huge-cyber-gangs-in-China>, as of December 7, 2014.

Clayton, Mark (2014, July 1). An Anti-US Stuxnet? Startling Attack against Industrial Complex Revealed. *Christian Science Monitor*. <http://www.csmonitor.com/World/Passcode/2014/0701/An-anti-US-Stuxnet-Startling-attack-against-industrial-complex-revealed>, as of January 18, 2015.

Collins, Sean, and Stephen McCombie (2012). Stuxnet: The Emergence of a New Cyber Weapon and its Implications. *Journal of Policing, Intelligence, and Counter Terrorism* 7, 1: 80–91. DOI: 10.1080/18335330.2012.653198.

Cox, James (2012). *Canada and the Five Eyes Intelligence Community*. Canadian Defence & Foreign Affairs Institute.

Davis, Joshua (2007, August 21). Hackers Take Down the Most Wired Country in Europe. *Wired*. <http://www.wired.com/politics/security/magazine/15-09/ff_estonia>, as of August, 21, 2007.

Deibert, Ron (2012, August). *Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace*. CDFAI Policy Paper. Canadian Defence and Foreign Affairs Institute. <https://d3n8a8pro7vhmx.cloudfront.net/cdfai/pages/41/attachments/original/1413662138/Distributed_Security_as_Cyber_Strategy.pdf?1413662138>, as of January 18, 2015.

Deibert, Ronald J. (2013). *Black Code: Surveillance, Privacy, and the Dark Side of the Internet*. McClelland & Stewart.

Entous, Adam (2013, December 4). US Raises Concerns about South Korea Deal with China's Huawei. *Wall Street Journal*. <online.wsj.com/news/articles/SB10001424052702304355104579236372543293320#printMode>, as of January 14, 2014.

Freeze, Colin (2013, November 12). Spy Agency's Budget to Hit $460-Million after "Steady Path" of Growth. *Globe and Mail*. <http://www.theglobeandmail.com/news/politics/spy-agencys-budget-to-hit-460-million-after-steady-path-of-growth/article15385168/>.

Freeze, Colin, and Jane Taber (2012, October 22). Mole Had Access to Wealth of CSIS, RCMP, Privy Council Files. *Globe and Mail*. ProQuest (1113976368).

Frei, Stefan. 2013. *The Known Unknowns: Empirical Analysis of Publicly Unknown Security Vulnerabilities*. NSS Labs.

Fung, Brian (2013, August 31). The NSA Hacks Other Countries by Buying Millions of Dollars' Worth of Computer Vulnerabilities. *Washington Post*. <http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/31/the-nsa-hacks-other-countries-by-buying-millions-of-dollars-worth-of-computer-vulnerabilities/>.

Geers, Kenneth (2010). The Challenge of Cyber Attack Deterrence. *Computer Law & Security Review* 26, 3: 298–303. <http://dx.doi.org/10.1016/j.clsr.2010.03.003>.

Gellman, Barton, and Greg Miller (2013, August 29). U.S. Spy Network's Successes, Failures and Objectives Detailed in "Black Budget" Summary. *Washington Post*. <http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_print.html>, as of October 14, 2014.

Gellman, Barton, Julie Tate, and Ashkan Soltani (2014, July 5). In NSA-intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are. *Washington Post*. <http://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html>, as of October 14, 2014.

Gendron, Angela (2013). Cyber Threats and Multiplier Effects: Canada at Risk. *Canadian Foreign Policy Journal* 19, 2: 178–198. DOI: 10.1080/11926422.2013.808578.

Gjelten, Tom (2013). First Strike: US Cyber Warriors Seize the Offensive. *World Affairs* 75, 5: 33–43. EBSCOhost (92026925).

Gorman, Siobhan (2009, April 8). Electricity Grid in US Penetrated by Spies. *Wall Street Journal*. <http://www.wsj.com/articles/SB123914805204099085>, as of January 18, 2015.

Gorman, Siobhan (2012, February 14). Chinese Hackers Suspected In Long-Term Nortel Breach. *Wall Street Journal*. <http://www.wsj.com/articles/SB10001424052970203363504577187502201577054>, as of January 18, 2015.

Gorman, Siobhan, August Cole, and Yochi Dreazen (2009, April 21). Computer Spies Breach Fighter-Jet Project. *Wall Street Journal*. <http://www.wsj.com/articles/SB124027491029837401>, as of January 18, 2018.

Greenberg, Andy (2012, August 3). McAfee Explains the Dubious Math Behind Its "Unscientific" $1Trillion Data Loss Claim. *Forbes*. <http://www.forbes.com/sites/andygreenberg/2012/08/03/mcafee-explains-the-dubious-math-behind-its-unscientific-1-trillion-data-loss-claim/>, as of January 13, 2014.

Greenwald, Glenn (2014). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. Signal; McClelland & Stewart.

Harris, Shane (2009, November 14). The Cyberwar Plan. *National Journal*. EBSCOhost (45266379).

Harris, Shane, and Isaac Stone Fish (2013, December 2). Accused of Cyber-spying, Huawei Is "Exiting the US Market". *Foreign Policy*. <http://foreignpolicy.com/2013/12/02/accused-of-cyberspying-huawei-is-exiting-the-u-s-market/>, as of January 18, 2015.

Hildreth, Steven (2001). *CRS Report to Congress: Cyberwarfare*. Congressional Research Service.

Hosenball, Mark (2013, November 14). NSA Chief Says Snowden Leaked up to 200,000 Secret Documents. *Reuters*. <http://www.reuters.com/article/2013/11/14/us-usa-security-nsa-idUSBRE9AD19B20131114>.

Jones, Sam (2014, March 7). Cyber Snake Plagues Ukraine Networks. *Financial Times*. <http://www.ft.com/cms/s/0/615c29ba-a614-11e3-8a2a-00144feab7de.html>, as of March 7, 2014.

Kallberg, Jan, and Bhavani Thuraisingham (2013). Cyber Operations: Bridging from Concept to Cyber Superiority. *Joint Force Quarterly* 1, 68: 53–58. <http://www.dtic.mil/doctrine/jfq/jfq-68.pdf>.

Kemp, R. Scott (2012, June 7). Cyberweapons: Bold Steps in a Digital Darkness? *Bulletin of the Atomic Scientists*. <http://thebulletin.org/cyberweapons-bold-steps-digital-darkness>.

Krekel, Bryan (2009, October 9). *Capability of the People's Republic of China to Conduct CyberWarfare and Computer Network Exploitation*. Northrop Grumman on behalf of the US-China Economic and Security Review Commission. <http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-030.pdf>, as of January 16, 2014.

Krekel, Bryan, Patton Adams, and George Bakos (2012, March 8). *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*. Northrop Grumman on behalf of the US-China Economic and Security Review Commission. <http://www.uscc.gov/Research/occupying-information-high-ground-chinese-capabilities-computer-network-operations-and>, as of January 16, 2014.

Lander, Stephen (2004). International Intelligence Cooperation: An Inside Perspective. *Cambridge Review of International Affairs* 17, 3: 481–493. DOI: 10.1080/0955 757042000296964.

LeBlanc, Daniel, and Colin Freeze (2013, November 28). Ottawa Denies G20 Summit Spying, Stops Short of Clear Denial of Foreign Deals. *Globe and Mail*. <http://www.theglobeandmail.com/news/politics/minister-defends-spy-agencys-record-after-g20-espionage-revelations/article15657707/>.

Lefebvre, Stéphane (2003). The Difficulties and Dilemmas of International Intelligence Cooperation. *International Journal of Intelligence and CounterIntelligence* 16, 4: 527–542. DOI: 10.1080/716100467.

Lewis, James A. (2013). *Conflict and Negotiation in Cyberspace*. Centre for Strategic and International Studies.

Lewis, James A. (2014). *Cybersecurity and Stability in the Gulf*. Centre for Strategic and International Studies. <http://csis.org/files/publication/140106_Lewis_GulfCybersecurity_Web_0.pdf>, as of December 5, 2014.

Libicki, Martin C. (2009). *Cyberdeterrence and Cyberwar*. RAND Corporation.

Lindsay, Jon R. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies* 22, 3: 365–404. DOI: 10.1080/09636412.2013.816122.

Ligaya, Armyna (2014, June 9). Grasping in the Dark: How Canada's Undercounting of Cybercrime May Be Leaving Us Vulnerable. *Financial Post*. <http://business.financialpost.com/2014/06/09/grasping-in-the-dark-how-canadas-undercounting-of-cybercrime-costs-may-be-leaving-us-vulnerable/?__lsa=f15c-1d8c>, as of December 23, 2014.

Livermore, Daniel (2014, November 27). *Three Missing Pieces in the Canadian Security and Intelligence Debate*. Centre for International Policy Studies, University of Ottawa. <http://cips.uottawa.ca/three-missing-pieces-in-the-canadian-security-and-intelligence-debate/>, as of December 22, 2014.

Lukacs, Martin, and Tim Groves (2013, October 9). Canadian Spies Met with Energy Firms, Documents Reveal. *Guardian*. <http://www.theguardian.com/environment/2013/oct/09/canadian-spies-met-energy-firms-documents>.

MacCharles, Tonda (2014, October 31). Spy Agency CSEC Says Goodbye to Canada. <http://www.thestar.com/news/canada/2014/10/31/spy_agency_csec_says_goodbye_to_canada.html>.

MacDonald, Alistair, and Paul Vieira (2012, October 17). Canada to Beef Up Its Cyber Defences. *Wall Street Journal*. <http://www.wsj.com/articles/SB10000872396390444592704578062744030325244>, as of January 18, 2015.

Markoff, John, David E. Sanger, and Thom Shanker (2010, January 25). In Digital Combat, US Finds No Easy Deterrent. *New York Times*. <http://www.nytimes.com/2010/01/26/world/26cyber.html>, as January 18, 2015.

Mandiant (2014). *M-Trends: Beyond the Breach.* 2014 Threat Report. <https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf>.

McAfee (2009). Unsecured Economies: Protecting Vital Information. Center for Education and Research in Information Assurance and Security. <https://www.cerias.purdue.edu/assets/pdf/mfe_unsec_econ_pr_rpt_fnl_online_012109.pdf>, as of January 15, 2015.

Metz, Cade (2013, April 30). Facebook Says It's Now as Big as Windows (Literally). *Wired Magazine*. <http://www.wired.com/wiredenterprise/2013/04/facebook-windows/>.

Meyer, Paul (2010, December). A Cyber Foreign Policy – Time for Canada to Get One. *Policy Options*. <http://policyoptions.irpp.org/issues/the-year-in-review-2/a-cyber-foreign-policy-time-for-canada-to-get-one/>, as of September 24, 2014.

Minnick, Wendell (2014, July 19). Chinese Businessman Charged with Hacking Boeing, Other Arms Companies. *Defense News*. <http://www.defensenews.com/article/20140719/DEFREG02/307190017/Chinese-Businessman-Charged-Hacking-Boeing-Other-Arms-Companies>, as of July 21, 2014.

Nakashima, Ellen (2013, May 27). Confidential Report Lists U.s. Weapons System Designs Compromised by Chinese Cyberspies. *Washington Post*. <http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html?hpid=z1>.

Nakashima, Ellen (2014, March 24). US Notified 3,000 Companies in 2013 about Cyberattacks. *Washington Post*. <http://www.washingtonpost.com/world/national-security/2014/03/24/74aff686-aed9-11e3-96dc-d6ea14c099f9_story.html>, as of January 18, 2015:.

Nakashima, Ellen, and Joby Warrick (2013, July 14). For NSA Chief, Terrorist Threat Drives Passion to "Collect It All". *Washington Post*. <http://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html>.

NATO Review (2013, June 17). The History of Cyberattacks: A Timeline. <http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm>, as of January 15, 2014.

North Atlantic Treaty Organization [NATO] (2011). *Defending the Networks*. <http://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf>, as of December 12, 2014.

North Atlantic Treaty Organization [NATO] (2014a). *NATO and Cyber Defence*. <www.nato.int/cps/en/natolive/topics_78170.htm>, as of January 13, 2014.

North Atlantic Treaty Organization [NATO] (2014b). *Wales Summit Declaration*. September 5, 2014. <http://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=en>, as of September 5, 2014.

Nye, Jr., Joseph S. (2011). *The Future of Power*. Public Affairs.

Obama, Barack (2014, January 17). Remarks by the President on Review of Signals Intelligence. <http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence>, as of September 5, 2014.

Panetta, Leon (2012, October 11). Remarks to Business Executives for National Security. <http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136>, as of January 16, 2014.

Payton, Laura (2012, October 11). Former Nortel Exec Warns against Working with Huawei. *CBC News*. <http://www.cbc.ca/news/politics/former-nortel-exec-warns-against-working-with-huawei-1.1137006>, as of January 14, 2014.

PC Tools (2011). What Is a Zero-Day Vulnerability? Symantec. <http://www.pctools.com/security-news/zero-day-vulnerability/>.

Perlez, Jane (2013, April 22). US and China Put Focus on Cybersecurity. *New York Times*. <http://www.nytimes.com/2013/04/23/world/asia/united-states-and-china-hold-military-talks-with-cybersecurity-a-focus.html?_r=3&>, as of January 15, 2014.

Perlroth, Nicole (2012, October 23). In Cyberattack on Saudi Firm, US Sees Iran Firing Back. *New York Times*. <http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all>, as of January 16, 2014.

Perlroth, Nicole (2013, December 10). China Is Tied to Spying on European Diplomats. *New York Times*. <http://www.nytimes.com/2013/12/10/world/asia/china-is-tied-to-spying-on-european-diplomats.html?_r=0>, as of January 16, 2014.

Perlroth, Nicole, and David E. Sanger (2014, December 22). Attack Is Suspected as North Korean Internet Collapses. *New York Times*. <http://www.nytimes.com/2014/12/23/world/asia/attack-is-suspected-as-north-korean-internet-collapses.html>, as of December 22, 2014.

Porteous, Holly (2011). *Cybersecurity and Intelligence: The US Approach*. Background Paper. Library of Parliament.

Press, Jordan (2012, October 17). Ottawa Doubles Investment in Cyber Security to $155 Million. *National Post*. <http://news.nationalpost.com/2012/10/17/ottawa-doubles-investment-in-cyber-security-to-155-million/>.

Public Safety Canada (2010). *Canada's Cyber Security Strategy for a Stronger and More Prosperous Canada*. <http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf>.

Public Safety Canada (2011, August). *Measuring the Extent of Cyber Fraud in Canada*. <http://publications.gc.ca/collections/collection_2011/sp-ps/PS14-4-2011-eng.pdf>, as of December 23, 2014.

Public Safety Canada (2013). *Action Plan 2010-2015 for Canada's Cyber Security Strategy*. <http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/ctn-pln-cbr-scrt-eng.pdf>.

Rains, Tim (2013, August 15). *The Risk of Running Windows XP after Support Ends April 2014*. Microsoft Security Blog. <http://blogs.technet.com/b/security/archive/2013/08/15/the-risk-of-running-windows-xp-after-support-ends.aspx>.

Richelson, Jeffrey T. (1990). The Calculus of Intelligence Cooperation. *International Journal of Intelligence and CounterIntelligence* 4, 3: 307–323. DOI: 10.1080/08850609008435147.

Rid, Thomas (2013). Cyberwar and Peace: Hacking Can Reduce Real-World Violence. *Foreign Affairs* 96, 6. <http://www.foreignaffairs.com/articles/140160/thomas-rid/cyberwar-and-peace>.

Riley, Michael (2013, May 23). How the U.S. Government Hacks the World. *Bloomberg BusinessWeek*. <http://www.businessweek.com/printer/articles/119394-how-the-u-dot-s-dot-government-hacks-the-world>.

Rudner, Martin (2001). Canada's Communications Security Establishment from Cold War to Globalization. *Intelligence and National Security* 16, 1: 97–128. DOI: 10.1080/714002836.

Samaan, Jean-Loup (2010). Cyber Command: The Rift in US Military Cyber-Strategy. *Rusi Journal* 155, 6: 16–21. DOI: 10.1080/03071847.2010.542664.

Sanger, David E. (2012a). *Confront and Conceal: Obama's Secret Wars and the Surprising Use of American Power*. Crown Publishers.

Sanger, David (2012b, June 1). Obama Order Sped Up Wave of Cyber-attacks. *New York Times*. <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all>, as of January 14, 2014.

Saporito, Laura, and James A. Lewis (2013, March 11). *Cyber Incidents Attributed to China*. Center for Strategic and International Studies. <http://csis.org/publication/cyber-incidents-attributed-china>, as of January 14, 2014.

Savage, Charlie, Edward Wyatt, and Peter Baker (2013, June 6). U.S. Confirms that It Gathers Online Data Overseas. *New York Times*. <http://www.nytimes.com/2013/06/07/us/nsa-verizon-calls.html?pagewanted=all&_r=0>.

Sherstobitoff, Ryan, Itai Liba, and James Walter (2013). *Dissecting Operation Troy: Cyber-Espionage in South Korea*. McAfee. <http://www.mcafee.com/us/resources/white-papers/wp-dissecting-operation-troy.pdf>, as of January 16, 2014.

Sims, Jennifer E. (2006). Foreign Intelligence Liaison: Devils, Deals, and Details. *International Journal of Intelligence and CounterIntelligence* 19, 2: 195–217. DOI: 10.1080/08850600500483657.

Singer, Peter W. (2012, May). *The "Oceans 11" of Cyber Strikes*. Brookings Institution. <http://www.brookings.edu/research/articles/2012/05/21-cyber-threat-singer>.

Singer, Peter W., and Allan Friedman (2013). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.

Smith, Adam (1776/1991). *The Wealth of Nations*. Liberty Fund.

Smith, Alexander (2009, March 29). Spy Chiefs Fear Chinese Cyberattack. *Sunday Times*. [London; subscription required.] <http://www.thesundaytimes.co.uk/sto/news/uk_news/article158319.ece>, as of January 16, 2014.

Symantec (2011). Norton Study Calculates Cost of Global Cybercrime: $114 Billion Annually. Press release. <http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02>, as of January 13, 2014.

Symantec (2012). 2012 Norton Study: Consumer Cybercrime Estimated at $110 Billion Annually. Press release. <http://www.symantec.com/about/news/release/article.jsp?prid=20120905_02>, as of January 13,2014.

Symantec (2013, June 26). *Four Years of Dark Seoul Cyber-Attacks against South Korea Continue on Anniversary of Korean War*. Security Response, Official Blog. <http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war>, as of January 14, 2014.

Thornburgh, Nathan, Matthew Forney, Brian Bennett, Timothy J. Burger, and Elaine Shannon (2005, Sept. 5). The Invasion of the Chinese Cyberspies (and the Man Who Tried to Stop Them). *Time Magazine*. EBSCOhost (18065208).

Tikk, Eneken, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm, and Liis Vihul (2008). Cyber Attacks against Georgia: Legal Lessons Identified. NATO Cooperative Cyber Defence Centre of Excellence. <https://web.archive.org/web/20121119120809/http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf>, as of January 21, 2015.

Timberg, Craig, and Ellen Nakashima (2014, March 16). Government Computers Running Windows XP Will Be Vulnerable to Hackers after April 8. *Washington Post*. <http://www.washingtonpost.com/business/technology/government-computers-running-windows-xp-will-be-vulnerable-to-hackers-after-april-8/2014/03/16/9a9c8c7c-a553-11e3-a5fa-55f0c77bf39c_story.html>.

Treasury Board of Canada Secretariat (2014). *2014–15 Estimates: Parts I and II, The Government Expenditure Plan and Main Estimates*. <http://www.tbs-sct.gc.ca/ems-sgd/me-bpd/20142015/me-bpd-eng.pdf>.

United Kingdom, Cabinet Office (2011, November). *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*. <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf>.

United Kingdom, Houses of Parliament (2011, September). *Cyber Security in the UK.* <http://www.parliament.uk/documents/post/postpn389_cyber-security-in-the-UK.pdf>.

U.S.-China Economic and Security Review Commission (2012). *2012 Report to Congress*. <http://www.uscc.gov/Annual_Reports/2012-annual-report-congress>, as of January 16, 2014.

U.S.-China Economic and Security Review Commission (2013). *2013 Report to Congress*. <http://www.uscc.gov/Annual_Reports/2013-annual-report-congress>, as of January 16, 2014.

United States, Defense Department (2007). *Annual Report to Congress on the Military Power of the People's Republic of China 2007*. United States Department of Defense. <http://www.defense.gov/pubs/pdfs/070523-china-military-power-final.pdf>, as of January 16, 2014.

United States, Defense Department (2008). *Annual Report to Congress on the Military Power of the People's Republic of China 2008.* United States Department of Defense. <http://www.au.af.mil/au/awc/awcgate/dod/china_report_2008.pdf>, as of January 16, 2014.

United States, Defense Department, Joint Strike Fighter Program (2014). Program. <http://www.jsf.mil/program/prog_intl.htm>, as of January 14, 2014.

United States, Department of Homeland Security (2014). *Cyber Storm: Securing Cyber Space*. <https://www.dhs.gov/cyber-storm-securing-cyber-space>, as of January 15, 2014.

United States, Department of Justice (2014, May 19). US Charges Five Chinese Military Hackers for Cyber Espionage against US Corporations and a Labor Organization for Commercial Advantage. <http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor>, as of January 18, 2015.

United States, District Court Western District of Pennsylvania (2014, May 1). *United States of America v. Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui*. US Department of Justice. <http://www.justice.gov/iso/opa/resources/512201451913235846194 9.pdf>, as of January 18,2015.

United States, Executive Office of the President of the United States (2009a). *The Comprehensive National Cybersecurity Initiative*. <http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf>.

United States, Executive Office of the President of the United States (2009b). *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. <http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>.

United States, Executive Office of the President of the United States (2010). *National Security Strategy*. <http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf>.

United States, Executive Office of the President of the United States (2011). *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. <http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>.

United States, National Security Agency (2010). *NSA Lends Support to Upcoming G8 and G20 Summits in Canada*. Dynamic Page (leaked by Edward Snowden). <http://www.cbc.ca/news2/pdf/summit-doc.pdf>.

United States, National Security Agency, Central Security Service (2010, June 24). *UKUSA Agreement Release, 1940–1956*. <https://www.nsa.gov/public_info/declass/ukusa.shtml>.

United States, National Security Agency, Central Security Service (2013). *NSA Intelligence Relationship with Canada's Communications Security Establishment Canada (CESC)*. Information Paper (leaked by Edward Snowden). <http://www.cbc.ca/news2/pdf/nsa-canada-april32013.pdf>.

United States, Senate Committee on Armed Services (2012, March 27). Hearing to Receive Testimony on US Strategic Command and US Cyber Command in Review of the Defense Authorization Request for Fiscal Year 2013 and the Future Years Defense Program.

United States, Senate Subcommittee on Emerging Threats and Capabilities of the Committee on Armed Services (2013, March 19). Hearing to Receive a Briefing on Cyber-security Threats in Review of the Defense Authorization Request for Fiscal year 2014 and the Future Years Defense Program.

United States, White House (2013). *Foreign Policy: Cyber Security*. <http://www.whitehouse.gov/issues/foreign-policy/cybersecurity> as of September 24, 2013.

Vieira, Paul (2011, February 17). Budget Safe after Cyberattack, Ottawa Says. *National Post*. <http://www.nationalpost.com/news/canada/Budget+safe+after+cyber+attack/4301368/story.html>.

Weinberger, Sharon (2011). Is This the Start of Cyberwarfare? *Nature* 474, 7350: 142–145. DOI: 10.1038/474142a.

Weston, Greg, Glenn Greenwald, and Ryan Gallagher (2013a). New Snowden Docs Show U.S. Spied during G20 in Toronto. *CBC News (*December 1). <http://www.cbc.ca/news/politics/new-snowden-docs-show-u-s-spied-during-g20-in-toronto-1.2442448>.

Weston, Greg, Glenn Greenwald, and Ryan Gallagher (2013b). Snowden Document Shows Canada Set Up Spy Posts for NSA. *CBC News (*December 10). <http://www.cbc.ca/news/politics/snowden-document-shows-canada-set-up-spy-posts-for-nsa-1.2456886>.

Winterfield, Steve, and Jason Andress (2012). *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice*. Syngress.

Zetter, Kim (2014, August 13). Meet MonsterMind, the NSA Bot that Could Wage Cyberwar Autonomously. *Wired Magazine*. <http://www.wired.com/2014/08/nsa-monstermind-cyberwarfare/>.

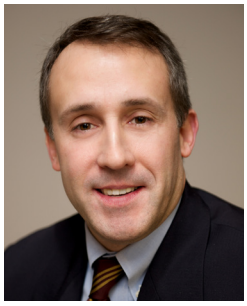
About the Authors

Alexander Moens

Alexander Moens is a professor of political science at Simon Fraser University and a Senior Fellow in Canadian-American Relations at the Fraser Institute. Dr Moens has published on American presidential decision-making, North American and European security issues, NATO policy, and regional and global trade issues. He is the author of *The Foreign Policy of George W. Bush: Values, Strategy, Loyalty* (Ashgate Publishing, 2004), as well as *Foreign Policy under Carter* (Westview Press, 1990). He has served in the Policy Planning Staff of Canada's Foreign Affairs Department and was a visiting fellow at the National Defense University in Washington, DC. In addition, he has conducted various research projects supported by NATO, the European Union, the departments of Foreign Affairs and National Defence of Canada, and the Social Sciences and Humanities Research Council of Canada.

Seychelle Cushing

Seychelle Cushing's research examines how the United States can leverage information in cyberspace to enhance national security. A parallel focus explores how the cyber domain and cyber threats have affected America's security relationship with Canada. Prior to her studies, she worked in the public sector as a writer and outreach organizer. She has organized and co-organized several events involving both national and international governments, and influential organizations across Canada. Most recently, she co-organized a roundtable sponsored by The Atlantic Council of Canada entitled *Perspectives on Canada's Role in International Cyber Security: An ACC Roundtable Discussion*. Ms Cushing obtained an M.A. with Distinction from the Department of Political Science at Simon Fraser University in 2014. She also holds a B.A. in Political Science from Simon Fraser University.



Alan W. Dowd

Alan W. Dowd is a Senior Fellow and Senior Editor with the Fraser Institute. He researches defence and security issues, writes on economic freedom, and has contributed to the Institute's report, *Economic Freedom of North America*. Mr Dowd's writing has appeared in *Policy Review*, *Parameters*, *Claremont Review of Books*, *Journal of Diplomacy & International Relations*, *Fraser Forum*, *American Legion Magazine*, *Military Officer*, *The American*, *World Politics Review*, *American Outlook*, *Diplomat & International Canada*, *National Post*, *Wall Street Journal Europe*, *Jerusalem Post*, *Financial Times Deutschland*, *Baltimore Sun*, *Washington Times*, *Washington Examiner*,

Sacramento Bee, *Indianapolis Star*, *Detroit News*, *Vancouver Sun*, and the online editions of *American Interest*, *National Review*, and *Weekly Standard*. Mr Dowd is an adjunct faculty at Butler University; holds senior-fellow posts with the Sagamore Institute and American Security Council Foundation; and served as director of Hudson Institute's corporate headquarters. He holds a B.A. from Butler University and an M.A. from Indiana University.

Acknowledgments

The authors acknowledge the helpful comments and insights of several anonymous reviewers. Any remaining errors or oversights are the sole responsibility of the authors. As the researchers have worked independently, the views and conclusions expressed in this paper do not necessarily reflect those of the Board of Directors of the Fraser Institute, the staff, or supporters.

Publishing Information

Distribution

These publications are available from <http://www.fraserinstitute.org> in Portable Document Format (PDF) and can be read with Adobe Acrobat® or Adobe Reader®, versions 7 or later. Adobe Reader® XI, the most recent version, is available free of charge from Adobe Systems Inc. at <http://get.adobe.com/reader/>. Readers having trouble viewing or printing our PDF files using applications from other manufacturers (e.g., Apple's Preview) should use Reader® or Acrobat®.

Ordering publications

To order printed publications from the Fraser Institute, please contact:

- e-mail: sales@fraserinstitute.org
- telephone: 604.688.0221 ext. 580 or, toll free, 1.800.665.3558 ext. 580
- fax: 604.688.8539.

Media

For media enquiries, please contact our Communications Department:

- 604.714.4582
- e-mail: communications@fraserinstitute.org.

Copyright

Date of issue

March 2015

ISBN

978-0-88975-342-6.

Citation

Alexander Moens, Seychelle Cushing, and Alan W. Dowd (2015). *Cybersecurity Challenges for Canada and the United States.* Fraser Institute. <http://www.fraserinstitute.org>.

Cover design

Bart Allan

Cover image

©Bigstock®

Supporting the Fraser Institute

To learn how to support the Fraser Institute, please contact

- Development Department, Fraser Institute
  Fourth Floor, 1770 Burrard Street
  Vancouver, British Columbia, V6J 3G7 Canada
- telephone, toll-free: 1.800.665.3558 ext. 586
- e-mail: development@fraserinstitute.org
- website: <http://www.fraserinstitute.org/support-us/overview.aspx>

Purpose, Funding, and Independence

The Fraser Institute provides a useful public service. We report objective information about the economic and social effects of current public policies, and we offer evidence-based research and education about policy options that can improve the quality of life.

The Institute is a non-profit organization. Our activities are funded by charitable donations, unrestricted grants, ticket sales, and sponsorships from events, the licensing of products for public distribution, and the sale of publications.

All research is subject to rigorous review by external experts, and is conducted and published separately from the Institute's Board of Directors and its donors.

The opinions expressed by authors are their own, and do not necessarily reflect those of the Institute, its Board of Directors, its donors and supporters, or its staff. This publication in no way implies that the Fraser Institute, its directors, or staff are in favour of, or oppose the passage of, any bill; or that they support or oppose any particular political party or candidate.

As a healthy part of public discussion among fellow citizens who desire to improve the lives of people through better public policy, the Institute welcomes evidence-focused scrutiny of the research we publish, including verification of data sources, replication of analytical methods, and intelligent debate about the practical effects of policy recommendations.

About the Fraser Institute

Our mission is to improve the quality of life for Canadians, their families and future generations by studying, measuring and broadly communicating the effects of government policies, entrepreneurship and choice on their well-being.

Notre mission consiste à améliorer la qualité de vie des Canadiens et des générations à venir en étudiant, en mesurant et en diffusant les effets des politiques gouvernementales, de l'entrepreneuriat et des choix sur leur bien-être.

Peer review—validating the accuracy of our research

The Fraser Institute maintains a rigorous peer review process for its research. New research, major research projects, and substantively modified research conducted by the Fraser Institute are reviewed by experts with a recognized expertise in the topic area being addressed. Whenever possible, external review is a blind process. Updates to previously reviewed research or new editions of previously reviewed research are not reviewed unless the update includes substantive or material changes in the methodology.

The review process is overseen by the directors of the Institute's research departments who are responsible for ensuring all research published by the Institute passes through the appropriate peer review. If a dispute about the recommendations of the reviewers should arise during the Institute's peer review process, the Institute has an Editorial Advisory Board, a panel of scholars from Canada, the United States, and Europe to whom it can turn for help in resolving the dispute.

Editorial Advisory Board