A Macdonald-Laurier Institute Publication

True North in
Canadian public policy

GLOBAL SECURITY
LOOK AHEAD

February 2017

Building a Cyber-Safe Society in a New World Economy

Ray Boisvert

It can be justifiably said that in the Western world, 2016 was the year national governments awoke to the consequential, long-term effects of cyber crimes committed upon national security interests, privacy, and economic prosperity. And yet, current government cyber strategies – Canada's included – creep forward with unevenly applied approaches and ill-coordinated tactical responses. In this country there is a growing awareness of cyber threats, both nationally and provincially, but disjointed responses. What is sorely lacking is deep situational awareness, along with an ability to address three critical elements of cyber strategy: deter, defend, and deploy.

Canada's national cyber security strategy was written in 2010. In a networked or digital context, it is sorely outdated: back then, Blackberry was still the market-leading smartphone, the iPad had only just launched, cloud computing was emerging, and Uber had its first beta software release. Things have evolved since then – dramatically.

Thus far, governments in Canada have only delivered a disparate, almost non-sequitur, set of strategies to counter what is clearly a highly complex environment, involving a mix of actors with varying degrees of capability and competing motivations.

Although on-line criminals continue to pose a risk to personal identifiable information, the West faces an emerging reality in which the most sophisticated hacking methods and technologies primarily support illicit state interests. In this new era, malicious state-supported actors now operate in collusion with state authorities. These groups operate to make a profit, but they also serve nationalistic causes as plausibly deniable proxies.

Those causes include hybrid warfare in a conflict zone, eroding an opposing society's confidence in their institutions and government, or by targeting the critical infrastructure that simply supports the "enemy."

In Russia, the intelligence clique surrounding President Vladimir Putin values a 21st century version of the "Kompromat" that combines calculated political smear campaigns with old KGB finesse. Central to this strategy is an effort to compromise the economies and reputations of Western governments, institutions, and individuals. One case in point is the 2016 hack of the US Democratic National Committee and the strategic release of emails from Presidential candidate, former Secretary of State Hillary Clinton and other DNC leaders. The result, it seems, has been the successful influence of a US election by a foreign power. Through hacks of supposedly secure networks, and while working with supposedly credible organizations like Wikileaks, hostile intelligence agencies, such as those in Russia, successfully compromising messages intended to disrupt legitimate political processes. Given their success to date, from the US election to possibly Brexit results, the KGB successor state will be further emboldened to commit future acts of social and electoral sabotage, which are likely to include the next federal Italian, German and French elections in Europe.

The stakes are high. The explosive growth of internet-based commerce (US$1 trillion by 2020 according to *Forbes*), and government plans to deliver seamless connectivity to their citizens, are at risk. Moreover, talk of US retaliation against Russia risks leading to serious and unintended consequences. Rapid military escalation is possible, given that Russian cyber incursions are taking place against a backdrop of cascading Western and Russian tensions.

In this context, Canada lacks a well-considered and clearly articulated framework for addressing immediate security needs and planning for longer term requirements. At issue is a cyber security gap that insidiously and routinely undermines Canadian safety, security, and prosperity. Canada needs a coherent vision and comprehensive policy for cyber security that actively and aggressively deters aggression and defends our interests.

Canada needs a coherent vision and comprehensive policy for cyber security that...deters aggression and defends our interests.

Deter

Cyber deterrence can mean many things. First, engagement and diplomacy are critical. US and British dialogue with China on limiting state-sponsored targeting of private sector interests and critical infrastructure seem to have provided some relief. Given this measurable success, Canada must follow suit. In line with this approach, our government needs to refurbish the Mutual Legal Assistance Treaties with cyber security in mind; the recent arrest in the Czech Republic of a suspected Russian hacker allegedly involved in the 2012 LinkedIn hack may soon represent the norm.

Canada's diplomatic team has yet to properly engage the cyber file; the profile and size of the team managing the issue on the global stage is small. Given the potential severity and impact of cyber sabotage on Canadian society, governance, and commerce, we must treat the cyber file with the same force and importance as trade, migration, climate change, and development. It is necessary to build an international consensus, if only with like-minded states, to establish guidelines for acceptable cyber behavior.

Would "naming and shaming" help stop cyber sabotage? The private sector, with behind-the-scenes assistance from Western security intelligence agencies, has sought to attribute blame for the recent hacks and attacks. However, interference with the US Presidential election, along with the theft of US Office of Personnel Management files, illustrates that Western governments themselves must unequivocally point the finger at

malicious state actors. They must do so with transparency and authenticity, which includes releasing as much verifiable "proof" as can possibly be disclosed publicly – and they must then be prepared to act demonstrably, be it via criminal indictment or simple "name and shame."

The charges of "economic espionage" and "aggravated identity theft" such as those made by the US against five Chinese People's Liberation Army officers, are needed to deter cyber aggression. In 2014, John Carlin, the US Assistant Attorney General for National Security, warned that "cyber theft is real theft and we will hold state sponsored cyber thieves accountable as we would any other transnational criminal organization that steals our goods and breaks our laws."[1] Whereas some of the statements and charges may have been political theatre, lessons derived from the indictment of CIA and Italian intelligence officers following a 2003 case of rendition against Egyptian Abu Omar[2] suggests that criminal processes can shift state behaviour.

Defend

The Internet of Things (IoT) – a world of connected devices ranging from cars to appliances – is expected to grow to 38.5 billion "things" in 2020. Equally important, production of data continues to grow daily at an exponential rate (2.5 quintillion bytes per day). Although all that data provides an unprecedented opportunity for personal development and enrichment, it also greatly multiplies the types of possible attacks and the number of items and devices that must be defended.

Defensive responsibility is a key part of the challenge. What role does each level of government have in providing cyber defence? What about the private sector: Should it not cover the costs of protecting publicly accessible networks, business systems, and financial assets? How do we return to an environment where products and services come with a guarantee of performance, rather than a digital disclaimer absolving vendors and service providers of any liability should their product fail to protect the consumer from cyber harm?

What role does each level of government have in providing cyber defence?

Given constitutional realities that include financial clout, access to cyber and other technical expertise via law enforcement, and security intelligence actions and prosecutorial power, the federal government must lead. But given the proximity and aspirations of local governments, from securing health care data to fostering "smart cities," all levels of government have a role to play.

Canadian consumers also need a bill of digital rights to establish standards for data-driven products and services. A version of the Canadian Standards Association (CSA) could regulate, test, and certify digital products, from smart phones to smart cars. Canada needs national standards, perhaps modelled on the US National Institute of Standards and Technology, to guide and encourage small- and medium-sized businesses to participate in cyber security.

In addition, and through regulating market access, both federal and provincial governments must motivate the private sector to fully adopt a national standard. In other words, where private firms seek federal or provincial contracts, they must first meet a new norm for cyber resilience. This, in turn, will encourage the entire supply chain to become more cyber vigilant.

Conversely, governments must forge an entirely new relationship with private sector cyber security firms which, through more persistent innovation, have the most advanced technologies and skills to thwart cyber attacks at a fraction of the cost governments would have to pay.

In other areas, we must be quicker at modelling best practices from other jurisdictions. A recent report co-authored by three US agencies involved in regulating the financial sector call for the imposition of cyber security standards in that area to ensure an ability to "demonstrate effective cyber security governance" and a robust business continuity capability.

Canada has thus far failed to develop a fully coordinated and effective plan to defend against cyber attacks.

Elsewhere, the UK government has been the most aggressive at developing policy and allocating funding (reaching almost $3 billion CAN). The UK has stated that it will not accept significant risk being posed to the public and the country as a whole as a result of businesses and organizations failing to take the steps needed to manage cyber threats.

In Australia, the government launched a revised cyber security strategy in April 2016, and linked it to Prime Minister Malcolm Turnbull's economic plan. In addition, Turnbull appointed a minister for the file and committed to an annual cyber security meeting with business leaders. As importantly, within that strategy is a revamped government structure wherein all key agencies, from defence to the intelligence services and federal police, operate the cyber file from within a single Australian cyber security centre.

In the United States, there have been some calls to reorganize the way law enforcement agencies interoperate, from the FBI to the almost 20,000 other local, state, and federal agencies. These agencies must become better coordinated in a world of globalized crime. In Canada, the number of agencies is much smaller, but they remain stuck in the 20th century. Moreover, they have yet to be fully and clearly empowered and funded to address this new challenge head-on.

Despite facing the same level of threat as our closest allies, Canada has thus far failed to develop a fully coordinated and effective plan to defend against cyber attacks. In this new century, it is imperative that we vigorously defend our digital assets and space, nationwide.

Deploy

In the first of the three 2016 US Presidential debates, former Secretary of State Hillary Clinton commented notably about Russian cyber attacks against fundamental US institutions, such as the attack on the Democratic National Party. "We're going to have to make it clear that we don't want to use the kinds of tools that we have. We don't want to engage in a different kind of warfare. But we will defend the citizens of this country," she said.[3]

Clearly, she was referring to the deployment of cyber warfare capabilities. In this context, "deploy" means building and applying weaponized digital tools to attack the networks and information operations of hostile states or non-state actors. However, the dialogue necessary in Western democracies to shape policies pertaining to the use of offensive cyber capability – known by experts as Advanced Cyber Defence (ACD) – remains absent.

Given that cyber and digital technology has created an era of asymmetric conflict, we now find that individuals, organizations, and corporations can build, access, or acquire certain weapons at will. What was not discussed in the US election, nor during the recently completed round of public consultation by the government of Canada on cyber security, is whether or not the state will attempt to retain the monopoly of power in this particular domain.

How then should Canada and other democracies regulate ACD? What about the "first strike" doctrine? Have we reached a conclusion that a cyber first strike would incur incalculable and catastrophic consequences? The answer is a very probable "no." As a result, policy gaps and mitigation strategies must be addressed post-haste.

The US defence and intelligence communities, as well as some US lawmakers, are prepared to react to the shifting realities of warfare by pre-emptively destroying an opponent's critical infrastructure. Important changes to the command and control of US cyber defence and offensive capabilities are being proposed by Congressional leaders. There is some discussion about making US Cyber Command a separate and distinct military entity dedicated to the degradation and possible destruction of an enemy's infrastructure, while retaining the National Security Agency as an intelligence-gathering entity. The key issue for Canada is to recognize the importance and magnitude of this strategic shift – a shift in which five dozen countries are retooling as the US is – and to set forth a new policy direction that will ensure adequate funding for a credible Canadian response.

Separately, Canada must also consider how to establish a governance model to address the growing interest of using ACD to "hack back." In hacking back, victims of cyber crime, even citizens themselves, retaliate in kind. We now recognize that passive cyber security has its limits, particularly given that attacks are increasingly state sponsored, so there must be some way to aggressively and proactively counter such attacks. How, then, do we use offence to improve our defensive strategy?

We now find that individuals, organizations, and corporations can build, access, or acquire certain weapons at will.

Many organizations are reeling from the impact of relentless cyber attacks. An AT&T study found that 62 percent of US firms had suffered a data breach between 2015 and 2016. As a result, those with sufficient financial resources are reportedly considering ACD because there is a perception that governments are not sufficiently protecting privately held assets. Allowing for the unfettered application of ACD by private interests has important and very tangible consequences, however. Chief among them is that current international agreements can be undermined and the existing global security framework destabilized. Once an organization, firm, or citizen engages with an adversary outside of their own network, even if only to recover lost data, they enter a world devoid of traditional rules of engagement.

Given these realities, the government of Canada must address the ACD challenge both domestically and internationally. It must turn its attention to building a dedicated yet flexible public policy framework that will pre-empt a rapid growth in the adoption and use of ACD by private interests. To avoid inadvertently falling into broader state conflicts, governments must regulate Internet vigilantes who will be tempted to invoke their right to strike back. In addition, governments must set out what is to be achieved by a public agency working to protect Canadians via an ACD strategy. In order to achieve the desired outcome, governments must invest in and develop appropriate policies, and establish an effective review. Governments must also ensure that any offensive capability is built on a clear and appropriate legal footing, and be ethically and morally defensible.

Conclusion

The fusion of individuals, data, and devices – along with technological globalization and increasing levels of cynicism and distrust within and between societies – all but ensures that cyber security issues will continue to transform our nations in new and unexpected ways. Unless we secure our digital world today, we risk entering an era of incessant and uncertain cyber conflict. Even while we are mitigating the threats posed by cyber attacks, we must not let concerns over terrorist violence dictate Canada's priorities in national security planning. It is important that the currently applied strategies derived from dated policies and approaches not be our primary response to an increasingly complex, malicious, and threatening environment.

A 21st century approach to cyber security requires the prioritization of new efforts across three pillars of governance that combine deterrence, defence, and deployment. The urgent task ahead is to secure our increasingly digital world, protect our privacy, and most of all, ensure the future prosperity of our liberal democratic nation.

Endnotes

1 US Department of Justice, May 19, 2014, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," *Justice News*, Government of the United States, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor, accessed on November 30, 2016.

2 Stephanie Kirchgaessner, April 25, 2016, "Former CIA Officer Faces Extradition to Italy over Abu Omar Kidnapping," *The Guardian*, https://www.theguardian.com/us-news/2016/apr/25/former-cia-agent-sabrina-de-sousa-extradition-italy-abu-omar-kidnapping, accessed on November 30, 2016.

3 French Caldwell, October 9, 2016, "To the Next President: Get a National Cybersecurity Strategy," *Forbes*, http://www.forbes.com/sites/ciocentral/2016/10/09/to-the-next-president-get-a-aational-cybersecurity-strategy/#1376fd7b6a0f, accessed on November 30, 2016.

ABOUT THE AUTHOR

Ray Boisvert is the Provincial Security Advisor to the Government of Ontario, and is the former Assistant Director, Intelligence, at the Canadian Security Intelligence Service (CSIS).

Macdonald-Laurier Institute

True North in Canadian public policy

Critically Acclaimed, Award-Winning Institute

The Macdonald-Laurier Institute fills a gap in Canada's democratic infrastructure by focusing our work on the full range of issues that fall under Ottawa's jurisdiction.

- The Macdonald-Laurier Institute fills a gap in Canada's democratic infrastructure by focusing our work on the full range of issues that fall under Ottawa's jurisdiction.
- One of the top three new think tanks in the world according to the University of Pennsylvania.
- Cited by five present and former Canadian Prime Ministers, as well as by David Cameron, the British Prime Minister.
- First book, *The Canadian Century: Moving out of America's Shadow*, won the Sir Antony Fisher International Memorial Award in 2011.
- *Hill Times* says Brian Lee Crowley is one of the 100 most influential people in Ottawa.
- The *Wall Street Journal*, the *Economist*, the *Globe and Mail*, the *National Post* and many other leading national and international publications have quoted the Institute's work.

"The study by Brian Lee Crowley and Ken Coates is a 'home run'.The analysis by Douglas Bland will make many uncomfortable but it is a wake up call that must be read."
FORMER CANADIAN PRIME MINISTER PAUL MARTIN ON MLI'S PROJECT ON ABORIGINAL PEOPLE AND THE NATURAL RESOURCE ECONOMY.

Ideas Change the World

Independent and non-partisan, the Macdonald-Laurier Institute is increasingly recognized as the thought leader on national issues in Canada, prodding governments, opinion leaders and the general public to accept nothing but the very best public policy solutions for the challenges Canada faces.

CTV
corus ENTERTAINMENT
cpac
tvo
CBC news
WALL STREET JOURNAL
FP Foreign Policy
The Economist
THE HILL TIMES
THE GLOBE AND MAIL
CANADA'S NATIONAL NEWSPAPER • FOUNDED 1844
NATIONAL POST

About the Macdonald-Laurier Institute

What Do We Do?

When you change how people think, you change what they want and how they act. That is why thought leadership is essential in every field. At MLI, we strip away the complexity that makes policy issues unintelligible and present them in a way that leads to action, to better quality policy decisions, to more effective government, and to a more focused pursuit of the national interest of all Canadians. MLI is the only non-partisan, independent national public policy think tank based in Ottawa that focuses on the full range of issues that fall under the jurisdiction of the federal government.

What Is in a Name?

The Macdonald-Laurier Institute exists not merely to burnish the splendid legacy of two towering figures in Canadian history – Sir John A. Macdonald and Sir Wilfrid Laurier – but to renew that legacy. A Tory and a Grit, an English speaker and a French speaker – these two men represent the very best of Canada's fine political tradition. As prime minister, each championed the values that led to Canada assuming her place as one of the world's leading democracies.
We will continue to vigorously uphold these values, the cornerstones of our nation.


SIR JOHN A. MACDONALD


SIR WILFRID LAURIER

Working for a Better Canada

Good policy doesn't just happen; it requires good ideas, hard work, and being in the right place at the right time. In other words, it requires MLI. We pride ourselves on independence, and accept no funding from the government for our research. If you value our work and if you believe in the possibility of a better Canada, consider making a tax-deductible donation. The Macdonald-Laurier Institute is a registered charity.

Our Issues

The Institute undertakes an impressive programme of thought leadership on public policy. Some of the issues we have tackled recently include:

- Getting the most out of our petroleum resources;
- Ensuring students have the skills employers need;
- Aboriginal people and the management of our natural resources;
- Controlling government debt at all levels;
- The vulnerability of Canada's critical infrastructure;
- Ottawa's regulation of foreign investment; and
- How to fix Canadian health care.

True North in
Canadian public policy

CONTACT US: Macdonald-Laurier Institute
8 York Street, Suite 200
Ottawa, Ontario, Canada K1N 5S6

TELEPHONE: (613) 482-8327

WEBSITE: www.MacdonaldLaurier.ca

CONNECT WITH US:

Scan this QR code to get your copy of our iphone app or to visit our mobile website

@MLInstitute

www.facebook.com/MacdonaldLaurierInstitute

www.youtube.com/MLInstitute

What people are saying about the Macdonald-Laurier Institute

In five short years, the institute has established itself as a steady source of high-quality research and thoughtful policy analysis here in our nation's capital. Inspired by Canada's deep-rooted intellectual tradition of ordered liberty – as exemplified by Macdonald and Laurier – the institute is making unique contributions to federal public policy and discourse. Please accept my best wishes for a memorable anniversary celebration and continued success.

THE RIGHT HONOURABLE STEPHEN HARPER

The Macdonald-Laurier Institute is an important source of fact and opinion for so many, including me. Everything they tackle is accomplished in great depth and furthers the public policy debate in Canada. Happy Anniversary, this is but the beginning.

THE RIGHT HONOURABLE PAUL MARTIN

In its mere five years of existence, the Macdonald-Laurier Institute, under the erudite Brian Lee Crowley's vibrant leadership, has, through its various publications and public events, forged a reputation for brilliance and originality in areas of vital concern to Canadians: from all aspects of the economy to health care reform, aboriginal affairs, justice, and national security.

BARBARA KAY, NATIONAL POST COLUMNIST

Intelligent and informed debate contributes to a stronger, healthier and more competitive Canadian society. In five short years the Macdonald-Laurier Institute has emerged as a significant and respected voice in the shaping of public policy. On a wide range of issues important to our country's future, Brian Lee Crowley and his team are making a difference.

JOHN MANLEY, CEO COUNCIL