CDFAI

CANADIAN DEFENCE & FOREIGN AFFAIRS INSTITUTE

Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace

by Ron Deibert

August, 2012

Research Paper

Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace

by Ron Deibert

Director, the Citizen Lab and Canada Centre for Global Security Studies,
Munk School of Global Affairs, University of Toronto
August, 2012

Prepared for the Canadian Defence & Foreign Affairs Institute
1600, 530 – 8th Avenue S.W., Calgary, AB T2P 3S8
www.cdfai.org

ISBN: 978-0-9737870-9-2

Executive Summary

Cyberspace has matured to become the information and communication ecosystem for the entire planet. Security of cyberspace has now become an urgent priority. Security is inherently political; not all actors share the same perspectives in terms of what is, or should be, the object of security and/or what constitutes a "threat." These perspectives vary not only within countries, but also across the world. These different outlooks reflect deep divisions in the world today between democratic and authoritarian regimes. Cyberspace has become an object of intense contestation, not only between these different systems of rule, but between a multitude of private sector and civil society actors who all depend on and use the domain, and have an interest in shaping it to their strategic advantage. Canada recently issued a strategy for cyber security, but it was thin on both commitments and specifics and left many issues unaddressed. This paper begins by exploring the landscape of cyber security on a global level to give a "bird's eye" view of the scope of the issues in global cyberspace security and governance. The second part of the paper lays out some recommendations for a comprehensive approach to Canadian cyber security following a "distributed security" model that is inspired and derived from liberal-democratic and traditional republican security traditions and thought.

Cyberspace[1] has matured to become the information and communication ecosystem for the entire planet. As cyberspace has matured, the security of cyberspace has now become an urgent priority. Security is inherently political; not all actors share the same perspectives in terms of what is or should be the object of security and/or what constitutes a "threat." These perspectives vary not only within countries, but across the world. While liberal democratic countries tend to focus their concerns on the authentication and proper functioning of the networks that support global trade, finance, and communications as their primary focus of cyber security, other countries may place more emphasis on regime or cultural stability. These different outlooks reflect deep divisions in the world today between democratic and authoritarian regimes. Cyberspace has become an object of intense contestation, not only between these different systems of rule, but among a multitude of private sector and civil society actors who all depend on and use the domain, and have an interest in shaping it to their strategic advantage.

Cyberspace policy matters for all countries, no less so for Canada for a number of reasons. Canada is a country that has a long historical relationship with communications. The Canadian political, social, and cultural landscape has been shaped by the interrelationship between the environment, technology, and communications going back to its very origins. Some of the first innovations in telecommunications have taken place in, or are associated with, Canada, such as those of Alexander Graham Bell. Canada is home to some of the leading theorists of communication technologies, including Harold Innis, Marshall Mcluhan, and the "father" of cyberspace, the science fiction author William Gibson. The Canadian Charter of Rights and Freedoms has explicit guarantees of "freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication."[2] Canada has traditionally devoted considerable resources to institutions furthering communications in the public sphere, including the Canadian Broadcasting Corporation, the National Film Board, and others.

Canada is a market economy, and Canadian economic prosperity is fundamentally reliant on a secure and open network of global communications. Canadian Internet usage is nearly double the world average.[3] Canada is a country that is highly dependent on global markets, especially in energy, trade and financial relations with the United States and Asia. Cyberspace is the sinew through which these relations take place. Canada recorded the sharpest growth in e-commerce of all of the OECD countries, with the Internet contributing $49 billion dollars to Canada's economy in 2011 (an amount larger than the contributions from agriculture or utilities).[4]

---

[1] 'Cyberspace' here refers to the global domain of digital electronic telecommunications.The US Department of Defense presently defines cyberspace as 'a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers'. US Department of Defense (2010) Department of Defense Dictionary of Military and Associated Terms. Joint Publication (JP) 1-02. Washington, DC: US Joint Chiefs of Staff.

[2] Canadian Charter of Rights and Freedoms, s 2, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11.

[3] comScore; "2012 Canada digital future in focus," March 1, 2012; http://www.comscore.com/Press_Events/Presentations_Whitepapers/2012/2012_Canada_Digital_Future_in_Focus

[4] Tavia Grant; "Canada urged to pull up its socks in Internet economy," Globe and Mail, March 19, 2012; http://www.theglobeandmail.com/news/technology/tech-news/canada-urged-to-pull-up-its-socks-in-internet-economy/article2373042/

However, there are also major challenges around cyberspace policy and security for Canada. A report by the International Telecommunications Union ranked Canada 26th among countries worldwide based on 11 different indicators, including fixed telephone line subscriptions, mobile subscriptions, internet bandwidth, internet access, and mobile broadband.[5] Commenting on the report, the University of Ottawa's Michael Geist observes that "every neutral survey or study over the past several years has had other countries leapfrogging ahead of Canada as we reap the results of a missing national digital strategy, restrictions on foreign investment, and ongoing competitive concerns."[6]

Cyber security issues have plagued Canada and Canadian companies. A recent student ranked Canada as the sixth most likely country to host servers running malicious programs.[7] Canadian public and private sector institutions have experienced a spate of major data breaches. Recently, it came to light that the computing networks of the Canadian telecommunications company, Nortel, had been breached – potentially for many years.[8] The breach reportedly reached into the higher echelons of the company and was tracked back to IP addresses originating in China. Some speculate that the company's eventual bankruptcy might be connected to the theft of intellectual property and other information that occurred during the breach, although this would be difficult to verify. Another set of breaches, also connected back to China, hit several government agencies, including the Treasury and Finance Departments and the DRDC.[9] Federal employees were forced offline for several months as a consequence of the breach.[10] Meanwhile, another Canadian company, Research in Motion (RIM), has faced cyber security challenges of a different sort: dozens of governments have sought access to its encrypted communications networks for security reasons, calling into question the very basis of RIM's signature product offering.

Like many countries, Canada recently issued a strategy for cyber security.[11] While a cyber security strategy is a welcome development, this particular one was thin on both commitments and specifics and left many issues unaddressed. In this paper, I begin by exploring the landscape of cyber security on a global level. This "bird's eye" view of the issue is important to take in order to understand the full scope of the issues at play, and to begin formulating a comprehensive strategy for cyber security. In the second part of the paper, I lay out several areas for consideration that I believe will help supplement the existing strategy and develop a more comprehensive approach in line with core Canadian interests and values – what I call a "distributed security" model for cyber strategy. In order to secure cyberspace, we need to think

---

[5] International Telecommunications Union; "Measuring the information society," 2011; http://www.itu.int/net/pressoffice/backgrounders/general/pdf/5.pdf
[6] Geist, Michael; "ITU report says Canada slipped to 26th worldwide in ICT development," September 16, 2011; http://www.michaelgeist.ca/content/view/6007/125/
[7] Glenny, Misha; "Canada's weakling web defenses," May 18, 2011; http://www.theglobeandmail.com/news/opinions/opinion/canadas-weakling-web-defences/article2025517/
[8] Gorman, Siobhan; "Chinese hackers suspected in long-term Nortel breach," February 14, 2012; http://online.wsj.com/article/SB10001424052970203363504577187502201577054.html
[9] Weston, Greg; "Foreign hackers attack Canadian government," CBC News, February 16, 2011; http://www.cbc.ca/news/politics/story/2011/02/16/pol-weston-hacking.html
[10] Freeze, Colin; "All cursors point to China in global hack attack that threatens nations," Globe and Mail, August 3; 2011, http://www.theglobeandmail.com/news/technology/all-cursors-point-to-china-in-global-hack-attack-that-threatens-nations/article2119046/
[11] Government of Canada; "Canada's cyber security strategy," 2010; http://www.publicsafety.gc.ca/prg/ns/cbr/_fl/ccss-scc-eng.pdf

through what type of cyberspace we want, both here and abroad, and synchronize both domestic and foreign policy to accomplish that vision.

CANADA'S 2010 CYBER SECURITY STRATEGY

Canada released its long awaited Cyber Security strategy on October 3, 2010. In doing so, it joined a growing list of other countries who have done likewise. The strategy put forward $90 million over five years, and $18 million on an ongoing basis in the 2010 budget. Emphasis was placed on three pillars: securing government systems; partnering with the private sector; and helping Canadians to be secure online through awareness raising. The strategy also laid out the roles and responsibilities of the various agencies involved in cyber security, including Public Safety Canada, the Communications Security Establishment Canada, the Canadian Security Intelligence Service, Treasury Board Secretariat, Foreign Affairs and International Trade, and the Department of National Defence and the Canadian Forces.

Overall, the strategy conforms to the spirit of like-minded strategies put forward by Canada's allies, such as the United States, the United Kingdom and Australia. But it seems thin on a number of more fundamental levels. Although there are rudimentary statistics on Canadians' dependence on cyberspace, there is no clear articulation of what, exactly, it is that we should be securing and why. Absent is any first-order discussion of how cyberspace itself, as a global medium of open and distributed communications, is in Canada's interests, i.e., how the latter is critical to Canada as a liberal-democratic and market economy country. It is almost as if this justification is assumed to be non-controversial and thus not worthy of articulating in the first place. However, at a time in history when cyberspace is being contested, and is arguably up for grabs, one would think that an articulation of first order principles about what, ideally, needs securing would be anything but self-evident. More about why first principles are important to emphasize will be laid out below.

The most glaring omission concerns the lack of a sophisticated understanding of the inherently *international* dimensions of cyberspace security. Although there is acknowledgement in the strategy that cyberspace is global, and that there is a role for foreign policy in Canada's cyber security strategy, there is a lack of depth about the full scope of the issues involved. There is also under-appreciation of the extent to which the risks Canada faces on the home-front cannot be solved in isolation, or in a traditional statist manner, and likewise how what we do here in Canada can have important repercussions abroad that can come home to bite us if we are not careful. The vast majority of the strategy focuses on domestic policy, with only a few scattered references to international affairs. The strategy portrays threats to Canadian systems as being "out there" and separate from Canada – "state-sponsored cyber espionage and military activities, terrorist use of the internet, and cybercrime" – with the solutions oriented almost entirely around protecting Canadian networks as if they existed in isolation. For example:

> Every year, we detect more attackers than the year before. And every year, those seeking to infiltrate, exploit or attack our cyber systems are more sophisticated and better resourced than the year before. They are investing in their capabilities. We must respond by investing more in ours.

> The Government is continuing its efforts to help secure Canada's cyber systems and protect Canadians online.[12]

There are very meagre explanations in the strategy of how or why these threats have emerged, and what can be done about them in the first place, other than a passing note about the importance of building the cyber security capacities of less developed states and foreign partners to help "forestall adversaries from exploiting weak links in global cyber defences." Who those "less developed" countries are and what cyber security should look like for them is never actually defined. Nor are the complexities of accomplishing this actually addressed. It would be great if less developed countries (China? India?) borrowed models of cyber security from Canada (assuming ours are faithful to our values and traditions in the first place), but how do we get them to do that?

Cyber security is critical to Canada, not just because an occasional network is breached or Canadians' computers are infected with malicious software, but because of more fundamental reasons: Canada is a liberal democratic country built upon respect for human rights, the rule of law, and democracy. Our continued existence as a country depends on the security of these values here at home and abroad. A global communications network that is open and distributed, through which citizens around the world can communicate and share ideas freely, is a critical and inseparable component of those ideals. However, today that open and distributed communications network is very much under threat – not only because of "state-sponsored espionage, terrorism, and cybercrime," but more fundamentally because of major tectonic social forces and (perhaps ironically) because of the securitization of cyberspace itself. Cyberspace has become an object of geo-political contestation that threatens to subvert its core characteristics. Addressing these larger phenomena from the ground up is essential for Canadian security writ large.

CYBERSPACE SECURITIZATION[13]

The *securitization* of cyberspace – a transformation of the domain into a matter of national security – is perhaps the most important force shaping global communications today.[14] Policymakers around the world are rushing to develop cybersecurity strategies to deal with what they perceive as a growing range of cyber-related threats. The reasons for this rush to securitize cyberspace relate to the sudden and dramatic shift in communications that has occurred worldwide over the last decade.

It may seem obvious, but it makes it no less important a fact, that cyberspace is deeply embedded in all aspects of life, growing continuously and dynamically in all directions. It has moved in a very short period of time from a research tool exclusive to University professors, students and hobbyists, to an encompassing and all engrossing domain. We now depend on it for all of our daily activities, in the home, the workplace, in culture, politics, health and in every

---

[12] Toews, Minister Vic; "Message from the Minister," 2011; http://www.publicsafety.gc.ca/prg/ns/cbr/ccss-scc-eng.aspx

[13] Parts of the following section draws from:
Deibert, R.; "Cybersecurity," Great Decisions 2012 (Foreign Policy Association: Washington DC, 2012)
Deibert, R. & Rohozinski, R.; "Contesting Cyberspace and the Coming Crisis of Authority," Access Contested: Security, Identity, and Resistance in Asian Cyberspace, (MIT Press: Cambridge, 2011).

[14] Deibert, R., & Rohozinski, R.; "Risking Security: Policies and Paradoxes of Cyberspace Security," International Political Sociology (2010)

other sector of life. We store business and personal information on "clouds." We connect 24 hours a day through a continuously evolving range of devices. Naturally, any such infrastructure will be seen as critical, ranked as one of the top security priorities for governments of the world.

Such an enormous shift from something separate to something so deeply immersive is going to raise the stakes for not only the rules of the game, but the nature of the game itself, particularly around norms, rules, and principles that have previously been taken for granted or assumed away as non-controversial. As more individuals, groups, and organizations become dependent on cyberspace, the clashes of interests, values, and ideologies become increasingly acute. There are more players with more at stake, and thus a more active interest in how regulatory and other shifts affect their strategic interests. Whereas once the Internet was governed by a community of like-minded engineers, today cyberspace governance has been thrown up to a multitude of actors and communities the world over.

Since cyberspace is primarily owned and operated by the private sector, a considerable portion of the contest around cyberspace concerns the conditions by which these companies mediate our experiences with it, an issue that has become more complex as the range of devices connecting to each other through common protocols expands. Consider, for example, debates over intermediary liability: whether private actors that control cyberspace services should be held responsible for the content that passes through their networks. In the past, such debates centered mostly on one type of actor: ISPs, or telecommunications carriers. Today, questions of intermediary liability are relevant to a wide range of companies and services, from cloud computing platforms, to online hosting companies, mobile phone devices, and online forums and video sharing sites. As these market-based actors create, constitute, and control the spaces of cyberpsace, their activities come under increasing scrutiny, regulatory and other pressures, and legal oversight from a growing number of political jurisdictions. Naturally, expectations on how and under what authority private sector actors police cyberspace can vary widely from political jurisdiction to jurisdiction. Compliance with "local laws" can bring with it tough choices and compromises of larger principles, such as those relating to human rights. Companies like Google, Microsoft, Yahoo!, Twitter, Facebook and others have all faced these growing pressures as their operations expand worldwide, struggling to balance the desire to penetrate growing and potentially lucrative markets, the need to comply with local law in order to do so, and respect for freedom of speech and access to information.[15]

Technological developments, particularly in cloud computing, have made even more acute long-standing cross-border data issues as they relate to security and state sovereignty. As more and more data is entrusted to third parties, where that data is stored, and through which jurisdictions it transits, matters politically. The University of Toronto's IXMAPs project underscores these issues in an experimental project that aims to map the routes packets take as they traverse the Internet.[16] An email sent from one computer in Toronto destined for another across town may, in fact, transit through networks in the neighboring United States, and potentially through a National Security Agency eavesdropping facility. Any data stored on Google servers, no matter their physical location, are subject to US Patriot Act provisions on data sharing because Google is a company domiciled in the United States and thus subject to US law. In response to these concerns, some European legislators have proposed regulations that

[15] European Digital Rights; "Twitter censors unfavourable Sarkozy Accounts," February 29, 2012; http://www.edri.org/edrigram/number10.4/twitter-censors-anti-sarkozy-accounts
[16] See http://www.ixmaps.ca

would restrict the use of Google products and services by public officials.[17] With whom we share our data and where it ultimately transits and resides in cyberspace is an inherently international concern.

These extraordinary changes in communications are occurring simultaneously with a major demographic shift in cyberspace as the number of users expands in the developing world, which in turn will have an impact on cyberspace security on a global level. Although cyberspace has its roots in the United States and other western industrialized countries, and thus embodies many of the values of users from those regions, Internet users in places like China, India, Latin America, and Southeast Asia will soon dwarf these early adopting constituencies. At present, the Asian region comprises 45% of the world's Internet population (the most by region), but it ranks only sixth in terms of penetration rates at 26%, meaning that there is an enormous population yet to be connected, most of them young. In China, for example, 60% of Internet users are under the age of 30. According to the ITU, among the roughly 5.3 billion mobile subscriptions by the end of 2010, 3.8 billion are in the developing world.[18] These new users are bringing with them new values and different social and political norms. Already, the desire to encourage linguistic communities to express themselves online has triggered serious questions about how the systems that support them are managed and resources allocated, particularly around management of country top-level domains. For example, the 2010 introduction of a Cyrillic top-level domain controlled by Russian authorities and a Chinese language domain controlled by Chinese authorities has been enormously popular in both worlds, but has furthered the division of the Internet along national-linguistic lines. While interoperability is technically unaffected in the short term, the prospects for politically-motivated government control is greater since the registration process moves into the hands of government-delegated bodies.

In these regions, many states have a well-established tradition of government intervention and state control, particularly of the mass media and the economy. Already having such a tradition in place, they are also coming into cyberspace at a much different historical juncture than the "early adopters" in places like Canada, the United States, and parts of Europe. For the latter, cyberspace was either something to be cordoned from government intervention altogether, or a mystery best left untouched. For the former, they are coming at cyberspace from the perspective of a much different security context surrounding cyberspace, a different culture of state-society relations, and a much greater understanding of its contested terrain. They are doing so building upon the knowledge and practices of prior experiments and are adopting and sharing best practices of information control and denial.

---

[17] A July 2011 "early warning assessment" produced by the RCMP's criminal intelligence branch, obtained by the Financial Post under an access to information request, listed some of these concerns. See: Tromp, Stanley; "Business crime thrives in the Cloud," Financial Post, February 13, 2012; http://business.financialpost.com/2012/02/13/business-crime-thrives-in-the-cloud/.
The Alberta Privacy Commissioner issued a report on this back in 2006 that raised issues about the Patriot Act at the time. See: Alberta Office of the Privacy Commissioner; "Public-sector outsourcing and risks to privacy," February 2006; http://www.oipc.ab.ca/Content_Files/Files/Publications/Outsource_Feb_2006_corr.pdf.
Australian Signals Intelligence agency issued a similar report last year: Australian Government Department of Defence - Defence Signal Directorate; "Cloud computing security considerations," April 2011; http://www.dsd.gov.au/infosec/cloud/cloud01.htm

[18] International Telecommunication Union; "ITU estimates two billion people online by end 2010," October 2010; http://www.itu.int/net/pressoffice/press_releases/2010/39.aspx

The regimes representing these new populations are also asserting themselves more forcefully in international cyberspace governance forums in order to broaden legitimacy for what they do at home – a phenomenon with significant implications for how cyberspace is constituted as a medium and as a whole. Notwithstanding internal contradictions, the United States and other liberal democracies tend to favour open communication networks, the projection of ideas, and see cyberspace (with some exceptions) primarily as a global common pool resource; China, Russia, and other authoritarian or democratically challenged countries, on the other hand, speak more often about "information security," which is largely equated with regime and cultural security, and are more comfortable asserting territorialized controls and sovereign rights. These countries also tend to see an imbalance toward the US and its allies' interests in existing cyberspace governance and ownership arrangements, and hope to have the United Nations take a more prominent role in cyberspace governance in a partial effort to redraw the balance.

These interventions in international governance of cyberspace are reflections of the sea-change in the way that governments the world over are asserting themselves in cyberspace. Whereas once the dominant metaphor of Internet regulation was "hands off", today the dominant metaphor is one of intervention, control, and, increasingly, contestation. The types of assertions of state power vary, depending on the nature of the regime, but all states are approaching cyberspace in a much different way than they did a decade ago. They are driven by the need to control dissent and opposition, protect and promote national identity and territorial control, or simply respond to the growing pressures to regulate cyberspace for copyright control, child protection, or to combat menaces of terrorism and cybercrime.

The worldwide growth of Internet filtering is one illustration of this sea change. Early in the Internet's history, it was widely assumed that the Internet was difficult for governments to manage and would bring about major changes to authoritarian forms of rule. Over time, however, these assumptions have been called into question as governments, often operating in coordination with the private sector, have erected a variety of information controls not only on the Internet, but on other platforms as well. It is now fair to say that there is a growing norm worldwide for national Internet filtering, although the rationale for implementing filtering varies widely from country to country. For example, since 2003 the OpenNet Initiative[19] project (a collaboration among the Citizen Lab at University of Toronto, Harvard University's Berkman Center, and the SecDev Group) has documented the growth of cyberspace controls through testing and research conducted in more than 70 countries worldwide. Its research shows that more than 40 countries engage in Internet content filtering in some manner. A recent ONI study calculated the number of citizens who live in censored countries as over 960 million, or 47% of all Internet users.[20]

Liberal democratic countries justify their Internet filtering to control access to content that violates copyright, concerns the sexual exploitation of children, or promotes hatred. In many liberal democratic countries, such as the United States, Canada, and the European Union, policymakers have argued that such filtering should be extended to cover content that promotes radical militancy, Islamic fundamentalism, and terrorism. Already, a number of liberal democratic countries, like the Netherlands, France, the United Kingdom, the United States, and

[19] http://opennet.net/
[20] OpenNet Initiatve; "Global Internet filtering at a glance," April 3, 2012; http://opennet.net/blog/2012/04/global-internet-filtering-2012-glance

others require Internet Services Providers to block access to websites and services known to be associated with illegal file-sharing.[21] Each day more proposals along those lines are debated in parliaments. Other countries filter access to content related to minority rights, religious movements, political opposition, and human rights groups. For example, Pakistan recently required 13 ISPs in the country to block access to the website of Rolling Stone magazine because of an article that referenced Pakistan's military spending.[22] Countries vary widely in terms of their transparency and accountability around such processes, and in terms of the methods by which they carry out filtering. But filtering of access to information within national borders for whatever reason and by whatever means is now a global norm.

The trajectory of greater government intervention into cyberspace has developed beyond Internet filtering. Governments have shown a greater willingness to employ a broader range of means, including covert and offensive-minded tactics, to shape cyberspace in their strategic interests. These tactics have developed largely as a consequence of the way cyberspace has grown in significance as an organizing and communicating platform for dissidents and activists. The tug-of-war between autocratic states seeking to limit communications and dissidents and activists armed with new technology has led to often dramatic episodes of disruption and counter-disruptions. For example, there have been a growing number of incidents where states have disrupted or tampered with communication networks for political purposes, including around elections and public demonstrations. Both Egypt[23] and Libya[24] severed all Internet access for brief periods of time during the so-called Arab Spring, a tactic that was also employed in Nepal,[25] China,[26] and Burma[27] at various times. Such a drastic move shows that some governments may be willing to sacrifice a lot to prevent the Internet from being used as a tool for mobilization. Even though Egypt has a relatively low Internet penetration rate of around 27%, the Organization for Economic Cooperation and Development estimated that the five-day shuttering of the Internet in early 2011 (discussed in more detail below) contributed to a loss of USD 90 million in direct revenues and a substantially higher amount in secondary economic impacts for which it did not account.[28] It is noteworthy in this respect that the shuttering of the

---

[21] Dutch ISP forced to block Pirate Bay website: European Digital Rights; "Dutch Internet providers forced to block the Pirate Bay," January 18, 2012; http://www.edri.org/edrigram/number10.1/dutch-isps-block-piratebay;
US pressures Spain to adopt Internet blocking of file-sharing sites: European Digital Rights; "The US pressure on Spain to censor the Internet has paid off," January 18, 2012; http://www.edri.org/edrigram/number10.1/spain-adopts-sinde-law;
Digital Civil Rights in Europe; "European countries' ISPs blocking file-sharing sites,";
http://www.edri.org/edrigram/number10.1/spain-adopts-sinde-law;
Italy blocking fraudulent websites: European Digital Rights; "Italy: Problematic Internet blocking decision against fraudulent website," March 28, 2012; http://www.edri.org/edrigram/number10.6/italy-internet-blocking-case
[22] York, Jillian; "Pakistan escalates its Internet censorship," Al Jazeera, July 26, 2011;
http://www.aljazeera.com/indepth/opinion/2011/07/201172511310589912.html
[23] OpenNet Initiative; "Egypt's Internet blackout: Extreme example of just-in-time blocking," January 28, 2011;
http://opennet.net/blog/2011/01/egypt%E2%80%99s-internet-blackout-extreme-example-just-time-blocking
[24] [24] OpenNet Initiative; "Libya's Internet restored briefly after months of silence," September 3, 2011;
http://opennet.net/blog/2011/09/libyas-internet-restored-briefly-after-months-silence
[25] [25] OpenNet Initiative; "Nepal: Internet down, media censorship imposed," February 4, 2005;
http://opennet.net/blog/2005/02/nepal-internet-down-media-censorship-imposed
[26] OpenNet Initiative; "China shuts down Internet in Xinjiang region after riots," July 6, 2009;
http://opennet.net/blog/2009/07/china-shuts-down-internet-xinjiang-region-after-riots
[27] OpenNet Initiative; "Pulling the plug: A technical review of the Internet shutdown in Burma,";
http://opennet.net/research/bulletins/013
[28] Organization for Economic Cooperation and Development; "The economic impact of shutting down Internet and mobile phone services in Egypt," February 4, 2011;
http://www.oecd.org/document/19/0,3746,en_2649_201185_47056659_1_1_1_1,00.html

Internet did not initially include the Internet service provider (ISP) Noor, whose clients include the Egyptian stock exchange, five-star hotels, and corporate clients ranging from Coca-Cola to Pfizer.[29]

During the so-called Green Revolution in Iran, the government was suspected of ordering Internet ISPs to tamper or "throttle" bandwidth and the use of certain protocols associated with censorship circumvention and anonymity tools, as a means to control opposition movements. As an illustration of the cat and mouse game that can go on between governments in cyberspace, it is noteworthy that the United States government lobbied the microblogging platform Twitter to postpone scheduled maintenance of its service in order to avoid disruptions for Iranian activists who were using the service during the Green Revolution.[30] Cambodia ordered a ban on all SMS messaging two days prior to national elections.[31] These "just-in-time" methods of blocking access to services or websites are not exclusive to non-democratic regimes. During riots in the United Kingdom in 2011, some British parliamentarians discussed implementing similar controls on mobile devices and social networking platforms,[32] and the Bay Area Rapid Transit (BART) authority in San Francisco, United States disabled cellular networks on its transit system in 2011 to prevent its use by protesters.[33]

Regimes aiming to control popular uprisings fueled by cyberspace technologies are turning to the private sector to identify, isolate, and contain organizers and participants. These actions, in turn, have generated fear, intense scrutiny, widespread condemnation and often very vocal criticism of the companies compelled, or encouraged in some manner, to collude with the regimes. For example, in Egypt in 2008, one of the country's largest cell phone carriers, Vodafone, turned over information on users who employed the service to organize food protests. Later, in 2011, the company admitted that it had sent messages on behalf of state security services, encouraging Egyptians to take to the streets to counter the mass uprising in that country.[34] Both cases caused public outrage and calls for boycotts against the company from human rights and privacy advocates. Similarly, in a much-publicized set of squabbles, RIM, the maker of the popular Blackberry device, has found itself facing demands from governments ranging from the United Arab Emirates to India and Indonesia for access to its encrypted data streams. In 2011, RIM agreed to implement content filtering on its Web browser in response to requests made by the Indonesian government to block pornography.[35] The controversy has brought about scrutiny into RIM's mobile architecture that otherwise would have likely never existed, pitted governments against each other and generated criticism of RIM itself by human rights advocates suspicious that the company has made secret deals that violate due process and public accountability. Should RIM comply with such requests for user data, its security would be

---

[29] Noor; "Clients,";
http://www.noor.net/Clients.aspx
[30] Pleming, Sue; "U.S. State Department speaks to Twitter over Iran," June 16, 2009;
http://www.reuters.com/article/2009/06/16/us-iran-election-twitter-usa-idUSWBT01137420090616
[31] Telecom Asia; "Cambodia shuts off SMS ahead of elections," April 2, 2007;
http://www.telecomasia.net/content/cambodia-shuts-sms-ahead-elections
[32] OpenNet Initiative; "Amidst riots in the UK, calls to censor social media," August 12, 2011;
http://opennet.net/blog/2011/08/amidst-riots-uk-calls-censor-social-media
[33] Cabanatuan, Michael; "BART admits halting cell service to stop protests, "San Francisco Chronicle, August 13, 2011;
http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2011/08/12/BAEU1KMS8U.DTL
[34] Associated Press; "Vodafone says Egyptian authorities forced it to send pro-Mubarak texts," February 3, 2011;
http://www.guardian.co.uk/world/2011/feb/03/vodafone-mubarak-text-messages
[35] Reuters; "RIM to abide by Indonesia porn access ban," January 17, 2011;
http://in.reuters.com/article/2011/01/17/idINIndia-54206220110117

called into question and users (which include large businesses) may lose confidence in the integrity of RIM's service offerings. Not complying, on the other hand, could force RIM out of potentially lucrative markets. As cyberspace grows exponentially, embedding itself deeper into everyday life through a greater range of connected devices and services, the contests over the rules and protocols by which such a complex domain is organized naturally intensify as well. Issues such as these bring to the forefront questions concerning the challenges private sector actors have in providing public communications services. How should companies whose operations may span multiple jurisdictions balance public rights with obligations to follow local laws in jurisdictions that may have widely differing due process standards and protections for civil liberties? How should they reconcile the imperatives of profit seeking, national security, and human rights when they conflict?

The new generation of cyberspace control techniques appear to include targeted computer network exploitation and other attacks on human rights and political opposition groups, some of which are highly sophisticated. The Information Warfare Monitor[36] (a research project running from 2003-2012 of which I was a co-founder and PI) discovered major cyber espionage networks in 2009 and 2010 that traced back to mainland China, both of which emerged from their investigations of the security of Tibetan-related organizations, including the Office of the Dalai Lama, whose systems were thoroughly infiltrated along with other victims of the espionage network.[37] These cases show that governments who lack resources or advanced capabilities of their own may instead be turning to the underworld of cybercrime for asymmetrical strategic advantage. The latter offers the benefits of accruing intelligence and other ends while allowing for plausible deniability. More recently, the Information Warfare Monitor project has documented computer network exploitation and website defacements conducted by what appear to be pro-patriotic hacker groups based in Iran, Syria, and Burma. In these cases, the governments appear to be offering tacit support and sometimes vocal encouragement of their attacks while keeping at arm's length the perpetrators of the attacks. The tolerance of these computer network operations by autocratic regimes traditionally averse to new technologies, demonstrates an evolution in cyberspace control strategies and a willingness to turn a blind eye to illegal activities when it suits national interests.

Governments with more "territorialized" visions of cyberspace controls are not just exercising their muscles in domestic contexts or through covert means; they are developing ambitious and increasingly internationalized strategies, sometimes coordinated through regional venues. One example of the former is the Shanghai Cooperation Organization (SCO), which is a regional organization made up of China, Kyrgyzstan, Kazakhstan, Russia, Tajikistan and Uzbekistan. India, Iran, Mongolia and Pakistan have observer status, and Belarus and Sri Lanka are considered dialogue partners. Iran is engaged in the SCO but prevented from formally joining because of UN sanctions. However, it is considered an active participant in the SCO summits, which have been held regularly throughout the region since the early 2000s. The SCO aims to share information and coordinate policies around a broad spectrum of cultural, economic, and security concerns, among them cyberspace policies. Generally speaking, experts see the SCO as a regional vehicle of "protective integration" against international norms of democracy and regime change with shared information policies being seen as critical to that end. Recently, the SCO issued a statement on "information terrorism", which drew attention to the way in which

[36] http:www.infowar-monitor.net
[37] Information Warfare Monitor; "Tracking GhostNet: Investigating a Cyber Espionage Network," 2009; http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network

these countries have a shared and distinct perspective on Internet security policy. The SCO has also engaged in joint military exercises and missions, described by some observers as simulations of how to reverse colour-style revolutions and popular uprisings. Unfortunately, the SCO's meetings tend to be highly secretive affairs and therefore not easily subject to outside scrutiny. But they are likely to become important vehicles of policy coordination, giving unity, normative coherence, and strength to the individual countries beyond the sum of their parts.

This greater assertion of state power is not going unchallenged. In fact, these growing controls are largely in direct response to the ways in which new information and technologies have enabled new forms of social mobilization and even regime change, as witnessed in the coloured revolutions of the countries of the former USSR and more recently in the Arab Spring. Networks of civil society actors, in some cases openly supported by countries like the United States and the European Union, and even by some private sector actors like Google, are developing a vast array of techniques and software tools to circumvent state controls. The stakes are becoming more acute as governments and civil society struggles in cyberspace spill into physical battles in the streets, as the contests in Tunisia, Egypt, Libya, Yemen, and Syria demonstrate (as well as Belarus, Burma, Thailand, Kyrgyzstan before them).

One area persistently highlighted in Canada's strategy is cybercrime. The underworld of cybercrime has exploded worldwide by any estimate. A recent crime report by Norton, a division of Symantec, suggests that the market for cybercrime is larger than the global black market for marijuana, cocaine, and heroin combined ($288 billion) and approaching the value of all global drug trafficking (at $411 billion).[38] Norton's report estimates that over 1 million people per day are considered victims of some kind of cybercrime, or approximately 431 million per year (14 adults every second). Meanwhile Verizon's 2011 Data Breach Investigations Report noted the growing *industrialization* of cybercrime that includes chains of specialized professionals ranging from coders to attackers to money launderers, all of whom managed themselves as professional businesses, independent contractors in what Verizon describes as a highly competitive arena.[39] Although it is difficult to assess the accuracy of these figures given the obscure nature of cybercrime and the interest's security companies may have in inflating threats, it is clear there is an enormous problem. There have been a series of high profile data breaches of major businesses, defence contractors, and government agencies worldwide, including victims in Canada mentioned above, that appear to be continuing unabated.

While Canada's Cyber Security strategy highlights cybercrime, it does not offer an explanation of why it is growing so fast – a necessary precondition for remediation. Cybercrime is growing at such an accelerated pace for several reasons. First, the number of users coming online, including individuals, businesses, organizations, and governments is growing rapidly, creating a growing baseline of potential targets. Second, the ways in which we communicate and share information online has changed fundamentally over the last several years, with the growth of social networking, cloud computing and mobile forms of connectivity. We share more data with each other, entrust it to third parties outside of our immediate control, and click on links and documents over social networking platforms and services with a greater degree of frequency. An

[38] Symantec; "Norton study calculates cost of global cybercrime: $114 billion annually," September 7, 2011; http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02
[39] Verizon; "2011 data breach investigations report,"; http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

epidemiologist studying this dynamic ecosystem of sharing would not be surprised by the cyber equivalent of disease.

But cybercrime also thrives because of the lack of deterrence. Law enforcement agencies tend to operate in national jurisdictions, and numerous constraints exist that prevent coordination across borders. Cyber criminals can act globally, but hide locally in jurisdictions where either such activities are tolerated or police lack resources and capabilities.

Third, companies rarely disclose security breaches to the public, which limits information about attacks and their methods. For example, the Sony corporation was the victim of several security breaches, but delayed disclosing them and then misrepresented the timeline of events pertaining to the attacks.[40] Similarly, Citigroup delayed disclosure of the breaches it suffered for nearly a month and then also mischaracterized their severity in contradictory public accounts.[41] Verisign computer systems were breached in 2010, but did not disclose them until two years later in its quarterly filings, almost as an aside.[42]

The worlds of cybercrime are not contained to economic-based theft; there is an increasing blurring of the techniques of cybercrime, cyber espionage, and cyber warfare. As mentioned above, in 2009, our Information Warfare Monitor research project discovered a major global cyber espionage network, called *Ghostnet*, that had infected 1295 computers in 103 locations, including government agencies, diplomatic missions, embassies, and ministries of foreign affairs.[43]

Ghostnet and other networks like it are notable for (among other reasons) the ways in which the techniques employed by attackers are largely indistinguishable from those of the cyber criminal underworld. In 2010, a German security researcher discovered that a sophisticated computer worm of unknown origin, called Stuxnet, had infiltrated and sabotaged air-gapped Iranian nuclear enrichment facilities. The code for Stuxnet is now widely available online, and in spite of its sophistication includes several techniques that are known in the cyber criminal underground. Stuxnet-style attacks present a higher order level of foreign policy and security threat than data breaches or other forms of exploitation since they target critical infrastructures that could cause significant loss of life. In light of the difficulties attributing the source of these type of attacks, Stuxnet-style acts of sabotage may prove to be tempting for governments and armed militant groups alike.[44]

---

[40] Phillips, Jack; "Sony knew hack was huge but delayed informing users," The Epoch Times, June 15, 2011; http://www.theepochtimes.com/n2/world/sony-knew-hack-was-huge-but-delayed-informing-users-57720.html
[41] Smith, Aaron; "Citigroup said to delay credit card hack report," CNN Money, June 13, 2011; http://money.cnn.com/2011/06/13/news/companies/citigroup_credit_card/?section=money_latest
[42] Mills, Elinor; "Hackers stole data from VeriSign in 2010, " CNet News, February 2, 2012; http://news.cnet.com/8301-27080_3-57370588-245/hackers-stole-data-from-verisign-in-2010
[43] Information Warfare Monitor; "Tracking GhostNet: Investigating a Cyber Espionage Network," 2009; http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network
[44] Also of concern are cyber criminal attacks that target the systems that secure cyberspace's core infrastructure. See: Fisher, Dennis; "RSA: SecurID attack was phishing via an excel spreadsheet," ThreatPost, April 1, 2011; http://threatpost.com/en_us/blogs/rsa-securid-attack-was-phishing-excel-spreadsheet-04011
In March 2011, the RSA admitted that it SecureID authentication system had been breached by attacks tracking back to China and of the advanced persistent threat variety. In September, 2011, a hacker claiming to be sympathetic to Iran hacked various certificate authorities: Mills, Elinor; "Second firm stops issuing digital certificates," CNet News, September 7, 2011; http://news.cnet.com/8301-27080_3-20102818-245/second-firm-stops-issuing-digital-certificates/.

The combination of enabling conditions, including a lack of law enforcement capabilities and resources, a growing number of victims, more valuable data being placed online, and major incentives among state intelligence agencies and illicit actors to exploit the wares of the cyber criminal, means that we can expect the underworld of cybercrime to grow and expand into areas critical to global security worldwide. The attacks experienced by the Canadian Treasury and Finance Departments, Nortel, and the DRDC are but symptoms of this larger trend.

Of perhaps the most serious of all security issues in cyberspace, one that overarches and potentially exacerbates the others, is that cyberspace is emerging as a new domain of war fighting. Cyberspace is now explicitly recognized in United States strategic doctrine as equal in importance to land, air, sea, and space, and a dedicated strategic command has been established in the United States military around cyberspace.[45] Although estimates vary widely, numerous governments are actively developing military doctrines for cyberspace operations, while others may be employing unconventional cyberspace strategies. There is an arms race in cyberspace looming on the horizon that suggests a period of intense hostility operating within and through this domain. As Joseph Nye has explained, cyberspace has all of the system characteristics that lend themselves well to arms racing: offence dominates; barriers to entry are low; and attributing the source of attacks is difficult making deterrence signaling a challenge.[46] Questions of whether and how traditional concepts of strategic thought, such as deterrence, apply in the cyber domain are now very much alive in strategic studies literature (but oddly absent from Canada's Cyber Security strategy).

While the rhetoric of cyber war is often heated and exaggerated to serve policy ends, there are recent cases of international conflict in which cyberspace has played a prominent and important role. During the 2006 war in South Lebanon, for example, Hezbollah was able to dominate the information environment by exploiting the Internet and other technologies as part of its distributed communication infrastructure. Likewise, in Estonia (2007), the state's banking and public administration systems were brought to a standstill as millions of computers from around the world were hijacked and harnessed together as a botnet to flood the country's national backbone. During the Russia-Georgia 2008 war over the disputed territory of South Ossetia, Georgian government ministries came under a massive distributed denial of service attack.[47] These attacks greatly affected the ability of the Georgian government to disseminate information and struck key infrastructure, such as the financial sector. Ironically, the Georgian government's attempts to mitigate these attacks included filtering access to Russian news and information sources. When combined with the DDoS attacks, the filtering had the unfortunate consequence of sowing fear and panic in the Georgian capital as citizens were subject to a widespread information blackout of unknown origins. Given the way that information and communication technologies permeate all aspects of society, economics, and politics today, it is impossible to engage in armed conflict separate from cyberspace.

A recent *New York Times* report claimed that the governments of United States and Israel were responsible for Stuxnet. See: Sanger, David; "Obama Ordered Wave of Cyberattacks Against Iran," New York Times, June 1, 2012; www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

[45] US Department of Defense; "National Military Strategy for Cyberspace Operations," (Washington, DC: US Joint Chiefs of Staff, 2006)

[46] Nye, Joseph S.; "Cyber war and peace," Al Jazeera, April 21, 2012; http://www.aljazeera.com/indepth/opinion/2012/04/201241510242769575.html

[47] Deibert, R.; Rohozinski, R., & Crete-Nishihata, M.; "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 South Ossetia War," Security Dialogue (2012)

Cyberspace securitization includes a political economy dimension: there is a growing cyber industrial complex around security products and services that both responds to, but also shapes the policy marketplace.[48] Corporate giants of the Cold War, like Northrup Grunman, Boeing, and General Dynamics, are re-positioning themselves for lucrative cyber security defence contracts, alongside a growing array of niche companies that offer computer network exploitation products and services. The global cyber arms trade now includes malicious viruses, computer exploits, and massive botnets. Many of the firms that produce these products and services are based in Western countries, but have found a market among authoritarian and other democratically challenged governments looking to flex their muscles. For example, after the fall of President Hosni Mubarak, Egyptian protesters uncovered secret documents of the Egyptian security services, among which was a contract for services from a British firm selling offensive computer exploitation capabilities.[49] Likewise, when Libyan rebels permeated Muammar Qadhafi's intelligence facilities they uncovered contracts between the regime and Narus, a subsidiary of the American firm Boeing, providing electronic surveillance equipment.[50]

The market for surveillance and offensive computer attack products and services that has emerged in recent years was preceded, and is supplemented by, a market for Internet filtering technologies. The latter were developed initially to serve business environments but quickly spread to governments looking for solutions for Internet censorship demands. ONI research throughout the 2000s was able to document a growing number of authoritarian countries using US-based commercial filtering products, including Smartfilter in Iran and Tunisia, Websense in Yemen, and Fortinet in Burma.[51] More recent ONI reports document a Canadian company's products (Netsweeper) being used in Yemen, Qatar, and the United Arab Emirates.[52] Some of these products appear to have been tailored to meet the unique requirements of authoritarian regimes. A powerpoint presentation by the company Cisco (the maker of telecommunications routing equipment) surfaced in 2008 in which the argument was made that a market opportunity presented itself for the company working in collusion with China's security services.[53] Commercial solutions such as these can help structure the realm of the possible for governments. Whereas in the past it might have been difficult or even inconceivable to engage in "deep-packet inspection" or keyword based filtering on a national scale, commercial solutions open up opportunities for policymakers looking to deal with vexing political problems on a fine-grained scale. In doing so, long-standing principles of network governance – such as network neutrality – can be eroded.

---

[48] Deibert, R. & Rohozinski, R.; "The new cyber military-industrial complex," *Globe and Mail*, March 28, 2011; http://www.theglobeandmail.com/news/opinions/opinion/the-new-cyber-military-industrial-complex/article1957159/

[49] McVeigh, Karen; "British firm offered spying software to Egyptian regime," *Guardian*, April 28, 2011; http://www.guardian.co.uk/technology/2011/apr/28/egypt-spying-software-gamma-finfisher

[50] Sonne, Paul and Coker, Margaret; "Firms aided Libyan spies," *Wall Street Journal*, August 30, 2011; http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html

[51] Noman, H., & York, J.; "West censoring East: The use of Western technologies by Middle East censors," (2010-2011)

[52] OpenNet Initiative; "When a Canadian company decides what citizens in the Middle East can access online," May 16, 2011; http://opennet.net/blog/2011/05/when-a-canadian-company-decides-what-citizens-middle-east-can-access-online

[53] Kessler, Glenn; "Cisco file raises censorship concerns," Washington Post, May 20, 2008; http://www.washingtonpost.com/wp-dyn/content/article/2008/05/19/AR2008051902661.html

The next decade will be critical for the future of cyberspace. There are several trajectories of possible development, depending on how the domain is secured and in whose interests. Cyberspace is entering into a period of potential chaos and instability, as cybercrime grows, an arms race in cyberspace escalates and new, potentially lethal, weapons are developed to target critical infrastructures. There is no consensus as to whether cyberspace governance should be primarily driven by governments, led by the private sector who owns, operates, and leads the development of the technology, or some combination of governments and private sector actors that also includes the vast multitude of users. How the norms, rules and principles of cyberspace are developed and made applicable across borders is presently an open question. Canada's cyber security strategy must include recognition of these trends and open-ended debates, and a strategy for how to influence them in Canada's national interests and according to its political values.

RECOMMENDATIONS FOR A COMPREHENSIVE CANADIAN STRATEGY FOR CYBER SECURITY

As outlined earlier, Canada's 2010 cyber security strategy had several shortcomings and unaddressed gaps. While it is unrealistic to expect Canada to solve all of the issues outlined above, especially in a context of limited resources, more can, and should, be done. The following section lays out six recommendations that can form the basis for a more comprehensive Canadian strategy for cyber security.

1. **Start with fundamentals and first principles, and work outward.** What is the political philosophy that underpins Canada's approach to securing cyberspace? Thinking about politics in relation to the security of a technological ecosystem may seem incongruous. In engineering and computer science communities, security is most often thought of in objective and functionalist terms. A fix, or a patch, is required to solve a specific vulnerability. But cyber security is more than just a technical issue. It pertains to the security of an entire communications ecosystem, which is the forum for the exchange of public and private information, communications and social relations. Security is always for someone, and some purpose, to paraphrase the Canadian political economist Robert Cox.[54] There are many different ways to secure cyberspace, depending on political preferences and values as to what needs to be protected in the first place. Cyber security is, therefore, inherently a discussion of political philosophy.

Canada's cyber security strategy should include an articulation of first principles, both about Canada as an ideal country and cyberspace as an ideal domain. Canada is a liberal democratic country with protections for individual rights and freedoms enshrined in its Charter. It is also a country that depends on an open and secure network of global information and communications for commercial, political and social relations. Cyberspace is an open and distributed ecosystem. It is a mixed, common pool resource, the vast majority of it in the hands of the private sector. In ideal terms, as a network, it functions on the basis of decentralized organization rather than hierarchical control.

At the heart of Canada's cyber security strategy, therefore, should be a strong affirmation of both of these principles around a vision of what is best described as *distributed security*. Distributed

[54] Cox, Robert; "Social forces, states and world orders: Beyond international relations theory," Neorealism and its Critics (New York: Columbia University Press, 1986)

security emphasizes checks and balances on power, oversight on authority, and protections for rights and freedoms. It is part of a tradition emphasizing the *negation* of violence and power that it is at the heart of liberal-republican theories of security going back to ancient Greece.[55] Distributed security offers a contrast and counter-narrative to traditional realist or statist versions of security, which are antithetical to the openness of cyberspace as a global commons. Distributed security emphasizes mixture, division and restraint.

Starting with these first principles can help guide the discussion and help frame the agenda from the ground all the way up to the global level. Ironically, to some extent, Canada's strategy for distributed cyber security should begin with a sharply limited role for the Canadian government itself (more on this below). Public authority does have an important contribution to make, but mostly in terms of laying out a vision, providing a conducive regulatory environment for the application of that vision, and ensuring basic rights and freedoms are protected as constitutive principles. Law enforcement, armed forces, and intelligence agencies all still have critical missions in protecting cyber security. However, securing cyberspace, while at the same time keeping it open, will require a multitude of cooperative behaviours by numerous actors at all points of the network and across public and private sectors – something that cannot be engineered or controlled by any one single authority.

Distributed security can help guide Canada's approach to foreign policy in cyberspace – a missing dimension to the present cyber security strategy (more on this below). Rather than centralize control of cyberspace in new institutions, as some governments are proposing to do, Canada should, instead, be forcefully advocating for re-investment in the grassroots and distributed forms of multi-stakeholder governance that keep the Internet and related technologies running today.

Ultimately, distributed security forcefully articulates a model of governance and security for cyberspace that affirms decentralized and mixed authority and a multitude of overlapping responsibilities as an ideal state towards which we should work. It offers a powerful counter-narrative, rich in republican theorizing, to realist or state-based visions that will place cyberspace under territorial rule. The political philosophy of distributed security should be the explicit point of departure for Canada's cyber security strategy.

2. **International implications of domestic policies**: Critical moving forward will be to find ways to secure cyberspace, and address all of the vexing threats that exist, without undermining the benefits of open networking and liberal democratic principles, such as access to information, freedom of speech, and privacy, and the enormous gains that have been made in advancing these principles over the last decade through open networking. In an urgency to address critical security issues as exemplified in radical plans to build a new Internet or outlaw anonymity online, there is a real risk that the "baby will be thrown out with the bathwater" thus undermining the positive social benefits of the Internet and its associated technologies. We must not lose sight that at the heart of what we aim to secure are systems of rule based upon the protection of democratic rights and liberties. Those rights and liberties need to be at the forefront of our security strategy, not accidentally trampled underneath its implementation.

---

[55] Deudney, Daniel H.; "Bounding power: Republican security theory from the polis to the global village" (Princeton, New Jersey: Princeton University Press, 2007)

Securing these principles matters not just in and of themselves but for the precedent they set as a model for norms, principles, and governance abroad. For example, ostensibly at the core of the Canadian government's approach to cyber security, Bill C-30[56] touches upon almost all of these issues – but in a negative way. While there may be some need to update lawful access legislation, Bill C-30 goes entirely in the opposite direction of the principles laid out above by, for example, mandating disclosure of subscriber information and the warrantless disclosure of emails and web surfing habits. Going further, the Bill authorizes the government to install surveillance equipment of its own choosing in ISPS and telecom service providers.[57] A similar negative dynamic can be seen in surveillance proposals in the United Kingdom, the SOPA, PIPA, and CISPA legislative proposals, or in amendments to the Foreign Intelligence Services Act (FISA) in the United States.[58] No credible evidence exists that in order to secure cyberspace the basic foundations of a liberal democratic system have to be eroded in the manner in which these proposals do. But evidence does exist that they help buttress illiberal policies abroad.

How the international implications of our domestic policies can come home to roost can be seen clearly in the case of RIM. That company's success has arguably rested on its proprietary and highly secure encrypted network for enterprise communications. However, as governments have joined the bandwagon to implement lawful access type provisions, RIM has been forced to make numerous compromises on its security – to the point where its value-added advantage is potentially undermined. As the company's fortunes suffer, one wonders to what extent the compromises of its security made a contribution?[59]

When liberal democratic countries download policing functions to the private sector without proper oversight and accountability, stand up within their armed forces capabilities to fight and win wars in cyberspace, allow companies based in their jurisdictions to profit from tools and services that enable widespread censorship and surveillance abroad, a precedent and justification is set for other less democratically inclined countries to follow. Unfortunately, in a rush to deal with pressing cyber security issues, liberal democratic countries may be cutting off their noses to spite their faces. A country cannot lament the loss of rights and freedoms internationally when those very rights and freedoms are being eroded at home. Liberal-democratic countries need to provide a strong model of governance and distributed security in order to shore up the future of cyberspace as its centre of gravity shifts to the South and to the East, where these traditions are much less strong. A consistent, comprehensive strategy to secure cyberspace in a way that deals with mutually perceived threats while at the same time ensuring that basic human rights, such as freedom of speech, access to information and privacy,

---

[56] Note: As of writing (July 2012) Bill C-30 has been temporarily withdrawn by the Government of Canada

[57] Geist, Michael; "Why Bill C-30 gives the govt the power to instlal its own surveillance equipment on ISP networks," February 22, 2012; http://www.michaelgeist.ca/content/view/6335/125/, and
Jeftovic, Mark; "Bill C-30...awful access (especially for ISPs)," February 16, 2012;
http://blog2.easydns.org/2012/02/16/bill-c-30-awful-access-especially-for-isps/

[58] Lee, Timothy B.; "Analysis: "Cybersecurity" bill endangers privacy rights," Ars Technica, April 18, 2012;
http://arstechnica.com/tech-policy/news/2012/04/analysis-cybersecurity-bill-endangers-privacy-rights.ars and
Lee, Timothy B.; "The new FISA compromise: It's worse than you think," Ars Technica, July 8th, 2008;
http://arstechnica.com/tech-policy/news/2008/07/fisa-compromise.ars

[59] Singh, Sanjay; "No secrets on Blackberry: Security services to intercept information after government gets its way on popular messenger service," Mail Online India, April 6, 2012;
http://www.dailymail.co.uk/indiahome/indianews/article-2126277/No-secrets-Blackberry-Security-services-intercept-data-government-gets-way-messenger-service.html and
Agence France Presse; "Privacy rights: BlackBerry maker vows privacy," January 4, 2012;
http://tribune.com.pk/story/316368/blackberry-maker-vows-privacy-safeguard-amid-memo-probe/

are bedrock pillars of global cyberspace will be the major challenge for the next decade – and they must begin "at home."

3. **Open up the "black box"**: "Secrecy," said Cardinal Richelieu in 1641, "is the first essential in affairs of the State" (1641).[60] Cyber security touches upon what is traditionally one of the most sensitive areas of national security: electronic surveillance, otherwise known as signals intelligence. The agencies that oversee signals intelligence have long been shrouded in secrecy and tend to lack rigorous and independent oversight, as do many of the agencies involved in national security matters in general. These agencies are now taking on a more expansive role as cyber security becomes a more vital issue to national security. Some, like the National Security Agency in the United States, are pushing to become the lead agency for both domestic and foreign cyber security. These agencies also have enormous path dependency through a built up reservoir of practices, expertise, and sunk costs, that make the implementation of constraints, let alone wider public debate, a difficult challenge. Indeed, the very agencies that should be re-examined in a new age of transparency are, somewhat perversely, being delegated the lead role in charting a course to cybersecurity.

However, there is a contradiction at the heart of having closed and highly secretive agencies leading the effort to secure what is in essence a highly decentralized and distributed mixed private-public network. National security agencies may have vital information that can be beneficial to cyber security, but they face challenges sharing that information outside of classified circles, with the private sector and with the public at large, which owns and operates much of cyberspace. These agencies' activities are shrouded in secrecy, with less robust public oversight of their operations than other government agencies. In an era when so much private information and communications circulate in vast clouds and networks – when data is abundant and plentiful – there is a very strong argument to be made that national security agencies should have more, rather than less, checks and balances.

Here again, the international implications of domestic policies matter as well. The more national security agencies are seen as leading cyber security efforts in liberal democratic countries, the more likely they will do so in non-democratic countries. The less oversight we provide on state surveillance domestically, the less likely it is to occur abroad.

A Canadian cyber security strategy should set an example by opening up the black box of intelligence and national security agencies, subjecting them to far greater scrutiny and oversight as a template for other countries to follow – or at least opening up their missions to public debate. Unfortunately, doing so clashes with the culture of secrecy that surrounds these institutions, and the tradition of national security in Canada as a whole that is still very much immersed in a Cold War mentality. The role of national security agencies, especially signals and other intelligence agencies, in the "big data" world of cyberspace should be a topic of wide public debate as a primary concern of Canada's cyber security strategy.

4. **What is the object of security? Underscoring privacy and other core rights as security issues**: Securing cyberspace should require attention to more than just servers and networks. A comprehensive strategy for cyber security should consider the importance of

[60] See Forcese, Craig; "Canada's national security "complex," IRPP Choices, June 2009; http://observgo.uquebec.ca/observgo/fichiers/53123_Choix.pdf

securing all values, including privacy, free speech, access to information and free association.[61] Looking at cyber security in this manner will highlight issues that tend to get overlooked in security debates – issues like access, affordability, and protection of personal information. For example, Canada might follow the lead of the Council of Europe, who recently issued recommendations for respect for human rights, and especially the processing of personal information, by search engines operating in Europe[62] The existing Cyber Security Strategy barely mentions privacy, and only does so in the context of the risks of cybercrime. As much as cybercrime is a real threat to privacy, an arguably much more potent risk to privacy revolves around the entrusting of personal data to third parties who operate in multiple national jurisdictions and are increasingly required to share information with law enforcement and intelligence agencies, some of whom are based in jurisdictions outside of Canada.

A comprehensive cyber security strategy might consider amplifying the role of the national and provincial privacy commissioners, whose oversight has been instrumental in raising awareness about a variety of issues related to the security of personal information in cyberspace – particularly around new technologies like mobile phones, social networking, and cloud computing. As more data is shared internationally, the security of Canadians privacy data is a critical public policy issue. Privacy commissioners may be best poised to evaluate, monitor, and raise awareness about these concerns. These issues pertain to a number of transnational relations, but are most acute with the United States, with whom we share deep economic, security, cultural, and policy linkages and with whom there is considerable pressure to normalize a common security protocol.

5. **Data Breach regulations**: As more and more data is entrusted to third parties, governments may have to consider passing laws that put more responsibilities on those third parties to properly secure and handle that data. As noted above, there is a tendency for companies to contain information about data breaches as opposed to making them public. Some have either sat on information for extended periods of time, or misled the public about the nature and scope of the breaches. Many companies do not dedicate appropriate resources to data security. The lack of frank and timely public disclosure about data breaches, and commitment of adequate resources to data security, are major security issues.

A strong data security breach disclosure law should be an essential component of a national cyber security strategy in Canada. As Jon Penney recently described, Canada's Bill C-29, which died in Parliament before the last federal election, was one such bill. However, it lacked teeth, and gave companies too much discretion in deciding what situations required security-breach reports. Some bills being proposed in the United States congress, such as the "Safe Data Act"[63] or the "Personal Data Privacy"[64] act may provide more suitable models for Canada to follow. As Penney summarizes:

---

[61] Some of the criticism of the CISPA in the United States focuses on these issues: Lee, Timothy, B.; "Analysis: "Cybersecurity bill endangers privacy rights" Ars Technica, April 18th, 2012; http://arstechnica.com/tech-policy/news/2012/04/analysis-cybersecurity-bill-endangers-privacy-rights.ars

[62] European Digital Rights; "New CoE recommendations for human rights in Internet services," April 11, 2012; http://www.edri.org/edrigram/number10.7/coe-recommandations-human-rights-search-engines-social-networks

[63] U.S. House. 112th Congress; "H.R. 2577, Secure and Fortify Electronic Data Act of 2011,"; http://republicans.energycommerce.house.gov/Media/file/Markups/CMT/072011/H2577_RSC_xml.pdf

[64] U.S. Senate. 112th Congress; "S.1151. Personal Data Privacy and Security Act of 2011,"; http://www.leahy.senate.gov/press/press_releases/release/?id=31e641c0-013e-4abc-8148-2c4f04ac3a86

> The last Canadian proposals, which died with Bill C-29, lacked teeth, and gave companies too much discretion in deciding what situations required security-breach reports, as well as the timing of those reports. Now, the Canadian government has a clean slate, and knowledge of these tougher alternatives, with which to forge a more robust disclosure regime. Cyber-security challenges, and the privacy, transparency, and data-retention issues they raise, are not going away, and the ideas offered here are far from comprehensive. But full disclosure, public scrutiny, and transparency are, without question, the foundation upon which more intelligent and comprehensive solutions will be built.[65]

6. **A Foreign Policy for Cyberspace** Just as what happens domestically can have repercussions around the world, what happens around the world can come back and bite us here in Canada. Of all of the missing components in Canada's cyber security strategy, the most glaring is the absence of a foreign policy for cyberspace. As part of the Cyber Security strategy, DFAIT was tasked with developing a cyber security foreign policy "that will help strengthen coherence in the Government's engagement abroad on cyber security."[66] To date, a foreign policy for cyberspace has not been articulated, although the Department is said to be exploring the area. Cyber security does not appear as one of DFAIT's "priority commitments for 2011-2012".[67] The problems that vex Canada's cyber security, from data breaches to cyber espionage, crime, and warfare, all have their roots in developments abroad. Until we deal with the roots of those problems, they will continue to vex us. Likewise, the nature of cyberspace itself will not be determined in Ottawa, or even Washington DC, as much of it will be in the burgeoning cities of India, China, and Brazil where the vast majority of users increasingly reside. As former DFAIT employee Paul Meyer recently argued, "The time has come for Canada to develop a dedicated cyber foreign policy with an associated diplomatic strategy to promote it, and a supporting policy and research capacity." Unless we actively engage cyberspace as a global issue, Meyer warns, we risk living in a cyberspace largely determined by others.[68]

As with domestic policy, a Canadian foreign policy for cyberspace should start with first principles. Here again, distributed security can provide a guiding philosophy. One promising development is that there is now a growing momentum around discussions of "norms of mutual restraint" and "rules of the road" in cyberspace, which plays very much into a debate about the constitutive principles of cyberspace and by extension the relevance of distributed security. Several major international conferences and meetings have been held on this topic, attended by Russia, China, the United States, Britain, as well as representatives from the private sector and civil society. To be sure, there are significant differences among major stakeholders concerning what should be the substance of those rules of the road, particularly between China, Russia and some other rising powers on the one hand, who are coalescing around a more top-down, territorialized vision of cyberspace governance, and the liberal democratic countries on the

---

[65] Penney, Jon; "Time to Get Transparent about Cyber Security," InfoWar Monitor, July 29, 2011; http://www.infowar-monitor.net/2011/07/time-to-get-transparent-about-cyber-security/

[66] Public Safety Canada; "Message from the Minister," October 3, 2011; http://www.publicsafety.gc.ca/prg/ns/cbr/ccss-scc-eng.aspx

[67] The issue of "cyber crime" is is identified as a threat to international security, and Canada's participation in the various international organizations dealing with the area are highlighted (G8, UN Office on Druges and Crime, and the OAS).

[68] Meyer, Paul; "A Cyber Foreign Policy - Time for Canada to Get One," Policy Options, December, 2010; http://www.irpp.org/po/issue.php?month=December&year=2010

other, led by the United States and its allies, who are favourable to an open commons. The Canadian government is, presently, not a major voice in these forums, but could easily translate its core foreign policy principles around respect for the rule of law, human rights, and promotion of democracy to articulate a counter-narrative around distributed security at the international level. As Milton Mueller notes with respect to US government policy, but in language that has broader appeal:

> The Internet's lightweight governance institutions have and continue to serve as points of coordination. But private actors own and operate the Internet's infrastructure and it is they who must repeatedly deal with the security challenges thrown at it. This is as it should be. Large-scale manmade Denial-of-Service attacks on the DNS root servers are an actual risk identified by the USG, but have been found to be of low likelihood because of the distributed and global nature of the DNS. These structural features allow a myriad of actors to respond to problems as necessary within the boundaries of the law. In many respects, the centralization and militarization sought by the security mavens will make us less secure.[69]

Encouraging norms of mutual restraint among states will be critical to furthering these principles. Canada's experience in arms control might help alleviate some of the growing tensions that are emerging in cyberspace as an arms race escalates. Cyberspace arms control is a controversial topic. While it is clear that there is a growing need for mutual restraints on growing hostilities and threats in cyberspace, not everyone agrees arms control is the best approach. Information – the central ingredient of warfare in cyberspace – is thought to be impossible to control in today's digitally networked and highly distributed environment. Moreover, attackers can hide their tracks and muddy attribution, making verification of any arms control agreement difficult. However, lessons can be derived from arms control regimes that do not restrict classes of weapons *per se* but rather actor behaviour or behaviour in entire domains instead (e.g., parts of the Outer Space Treaty and the Antarctic Treaty). Governments may look to some of the principles enshrined in these treaties as to how to conduct themselves in a common pooled resource like cyberspace that benefits all but is owned by no one in particular. Discussions around confidence and security building measures in cyberspace being undertaken under the auspices of the OSCE and the United Nations are encouraging in this regard.[70]

There is also a largely informal and quite influential cyber security "epistemic community" that cuts across public and private sectors that secures cyberspace in an ad hoc but occasionally very coordinated fashion that could be thought of as a form of cyber security "arms control." Indeed, the best examples of policing and control in this sector come in the form of distributed approaches. For example, in April 2011, the FBI and US Justice Department, working with the non-profit Internet Systems Consortium, dismantled the Coreflood botnet, a network of compromised computers which had been used to steal user credentials and an estimated $100 million from victims.[71] With a court order permitting them to set up what is known as a

---

[69] Mueller, Milton; "'Feeble' governance? The push to discredit multistakeholder institutions," April 18, 2012; http://www.internetgovernance.org/2012/04/18/feeble-governance-the-push-to-discredit-multistakeholder-institutions/

[70] See Camino Kavanagh; "Wither 'Rules of the Road' for Cyberspace?," Cyber Dialogue 2012; http://www.cyberdialogue.citizenlab.org/wp-content/uploads/2012/2012briefs/brief-1.pdf

[71] Zetter, Kim; "With court order, FBI hijacks 'Coreflood' botnet, sends kill signal," Wired, April 13, 2011; http://www.wired.com/threatlevel/2011/04/coreflood/

"sinkhole," officials replaced the botnet's command & control servers and sent code directly to compromised machines, stopping them from communicating and effectively disabling the botnet. Although not perfectly executed (users were not approached to give permission before the commands were sent to their machines in this case) the Coreflood takedown, and others like it, may be seen as part of a new form of distributed cyber security in which governments, the private sector, and civil society work to contain and mitigate unwanted behaviour in cyberspace around shared operating procedures and principles. A critical question will be whether such mitigation is done in a transparent and accountable way or not, and avoids the risks of cyber vigilantism. Canada's long-standing experiences with arms control policy and regimes, and especially its experiences in convening multiple stakeholders from civil society, the private sector, and government in the Landmines Ban, the Chemical Weapons convention, and other arms control regimes, could be positively marshalled and drawn upon in this sector.

Another component of Canada's foreign policy for cyberspace might address the sale of censorship, surveillance, and information warfare technologies to regimes that violate human rights. This market has become an object of considerable scrutiny and controversy in recent years. Several major media and other reports have spotlighted this industry, emphasizing the clients, and how it operates in brazen openness.[72] The research of the ONI has highlighted some of these issues over the years, including recent reports about Netsweeper, a Canadian company that sells censorship technology to the regimes of Qatar, UAE, and Yemen.[73] The software blocks access to content that in Canada would be considered a Charter violation. In the United States, congressional lawmakers have debated formally restricting these sales, the latest variation being the Global Online Freedom Act. President Obama also recently weighed into this debate, announcing a targeted sanctions regime for sales of technologies to the governments of Iran, Syria, and others who use them to engage in surveillance against dissidents in the context of violence.[74] To date, Canadian policy has not squarely addressed the issue, but it would be wise to begin considering them as part of a comprehensive cyber security policy sooner rather than later. Although Canada cannot solve these issues on a global level, it can at least begin the process of sorting them through here in Canada, and with respect to norms around how Canadian companies operate abroad.

Whether and to what extent Canada will develop an explicit "Internet Freedom" support policy as part of its foreign policy strategy will be an important question to discuss. Several allies of Canada, including the United States, Sweden, the European Union, the Netherlands, and others have devoted resources to training, advocacy, and tool development around Internet openness and security. These programs have not always been well received, obviously by governments who stand to lose the most, but also by local actor networks, some of whom have viewed the resources as a thin cover for the exercise of state interests. However, a dedicated program to

---

[72] MacKinnon, Rebecca; "Containing weapons of mass surveillance," Foreign Policy, April 24, 2012; http://www.foreignpolicy.com/articles/2012/04/24/containing_weapons_of_mass_surveillance?page=full

[73] OpenNet Initiative; "When a Canadian company decides what citizens in the Middle East can access online," May 16, 2011; http://opennet.net/blog/2011/05/when-a-canadian-company-decides-what-citizens-middle-east-can-access-online

[74] The White House Office of the Press Secretary; "Fact sheet: A comprehensive strategy and new tools to prevent and respond to atrocities," April 23, 2012; http://www.whitehouse.gov/the-press-office/2012/04/23/fact-sheet-comprehensive-strategy-and-new-tools-prevent-and-respond-atro; and
Bloomberg; "Unplug companies that help Iran and Syria spy on citizens," April 24th, 2012; http://www.bloomberg.com/news/2012-04-24/unplug-companies-that-help-iran-and-syria-spy-on-citizens.html

research and development around key components of "distributed security", as opposed to "Internet freedom", would likely be seen as less ideological.

Lastly, Canada's foreign policy in cyberspace should include a dedicated outreach component with countries that will matter most for the future of cyberspace governance and policy going forward, and anticipate as much as possible the demographic shift that is occurring as the centre of gravity of cyberspace moves to the South and to the East. Here, Canada's foreign policy strategy might be linked to development and aid policy to encourage networks of engineers, policymakers, and researchers from North and South to share best practices around rights, security, and governance in cyberspace. Such engagement will have not only long-term benefit; as described above, many of these countries are going to be linchpins in the debates over the future of cyberspace governance.

This engagement should also include international and regional forums of cyberspace governance. In recent years, the traditional organs of cyberspace governance (ICANN, the IETF, the RIR and others) have been joined by a variety of others, including the G8, G20, OECD, OSCE, European Commission, the ITU, the UN General Assembly, and a lengthy list of regional organizations. Obviously scarce resources dictate to what extent Canada can engage in all of these forums, and no country can be "everywhere." But part of a foreign policy for cyberspace must include a strategic assessment of where best to weigh in as part of a collective effort of like-minded countries, private sector actors, and civil society who share the same values.

CONCLUDING REMARKS

Surveying the landscape of cyberspace on a global level, one cannot help but be struck that we are at a watershed moment. Major social forces are converging that threaten to subvert cyberspace's core characteristics as an open distributed network, including growing assertions of state power, interstate competition, espionage, crime and warfare. Governments with more territorialized visions of cyberspace controls are imposing those visions in international bodies and drawing growing networks of support for their vision. There is a large market for technologies, products, and services that facilitate censorship, surveillance and information warfare. None of these developments are in Canada's interests, and yet none are squarely addressed in its Cyber Security strategy.

There are countervailing forces, however, that might be marshaled to check and constrain some of the more dangerous possible outcomes while protecting and even furthering the gains in freedom and individual empowerment that have been made over the last decade. Major stakeholders across governments, the private sector and civil society recognize the value of constituting cyberspace as a "global commons" and are actively working on norms, rules, principles and technological infrastructure to support it as such. In some respects, we are entering a "constitutive" moment for cyberspace that may define the global communications environment for decades to come. A comprehensive cyber security framework that is articulated by Canada that takes advantage of these opportunities would be a major contribution to domestic and international security. The model of "distributed security" should be the basis for that strategy moving forward.

About the Author

Ron Deibert (PhD, University of British Columbia) is Professor of Political Science, and Director of the Canada Centre for Global Security Studies and the Citizen Lab at the Munk School of Global Affairs, University of Toronto. The Citizen Lab is an interdisciplinary research and development hothouse working at the intersection of the Internet, global security, and human rights. He is a co-founder and a principal investigator of the OpenNet Initiative and Information Warfare Monitor (2003-2012) projects.

Deibert was one of the founders and (former) VP of global policy and outreach for Psiphon Inc.

Deibert has published numerous articles, chapters, and books on issues related technology, media, and world politics. He was one of the authors of the Tracking Ghostnet report that documented an alleged cyber-espionage network affecting over 1200 computers in 103 countries, and the Shadows in the Cloud report, which analyzed a cloud-based espionage network. He is a co-editor of three major volumes with MIT Press: Access Denied: The practice and policy of Internet Filtering (2008), Access Controlled: The shaping of power, rights, and rule in cyberspace (2010), and Access Contested: Security, Identity, and Resistance in Asian Cyberspace (2011). He is the author of Parchment, Printing, and Hypermedia: Communications in World Order Transformation (New York: Columbia University Press, 1997), and the forthcoming book *Black Code: the battle for the future of cyberspace* (forthcoming: McClelland & Stewart, 2013).

He has been a consultant and advisor to governments, international organizations, and civil society/NGOs on issues relating to cyber security, cyber crime, online free expression, and access to information. He presently serves on the editorial board of the journals International Political Sociology, Security Dialogue, Explorations in Media Ecology, Review of Policy Research, and Astropolitics.

Deibert is on the advisory board of Access Now, Privacy International, and is a member of the board of directors of Lake Ontario Waterkeeper.

Deibert was awarded the University of Toronto Outstanding Teaching Award (2002), the Northrop Frye Distinguished Teaching and Research Award (2002), and the Carolyn Tuohy Award for Public Policy (2010). He was a Ford Foundation research scholar of Information and communication technologies (2002-2004).

Canadian Defence & Foreign Affairs Institute

CDFAI is the only think tank focused on Canada's international engagement in all its forms - diplomacy, the military, aid and trade security. Established in 2001, CDFAI's vision is for Canada to have a respected, influential voice in the international arena based on a comprehensive foreign policy, which expresses our national interests, political and social values, military capabilities, economic strength and willingness to be engaged with action that is timely and credible.

CDFAI was created to address the ongoing discrepancy between what Canadians need to know about Canadian international activities and what they do know. Historically, Canadians tend to think of foreign policy – if they think of it at all – as a matter of trade and markets. They are unaware of the importance of Canada engaging diplomatically, militarily, and with international aid in the ongoing struggle to maintain a world that is friendly to the free flow of goods, services, people and ideas across borders and the spread of human rights. They are largely unaware of the connection between a prosperous and free Canada and a world of globalization and liberal internationalism.

In all its activities CDFAI is a charitable, nonpartisan organization, supported financially by the contributions of foundations, corporations and individuals. Conclusions or opinions expressed in CDFAI publications and programs are those of the authors and speakers and do not necessarily reflect the views of the Institute staff, fellows, directors, advisors, or any individuals or organizations that provide financial support to CDFAI.