UNIVERSITY OF CALGARY

THE SCHOOL OF PUBLIC POLICY
SPP Communiqué

Volume 5 • Issue 3
March 2013

SPP Communiqués are brief articles that deal with a singular public policy issue and are intended to provide the reader with a focused, concise critical analysis of a specific policy issue.

Copyright © 2013 by The School of Public Policy.

All rights reserved. No part of this publication may be reproduced in any manner whatsoever without written permission except in the case of brief passages quoted in critical articles and reviews.

The University of Calgary is home to scholars in 16 faculties (offering more than 80 academic programs) and 36 Research Institutes and Centres including *The School of Public Policy*. Under the direction of Jack Mintz, Palmer Chair in Public Policy, and supported by more than 100 academics and researchers, the work of The School of Public Policy and its students contributes to a more meaningful and informed public debate on fiscal, social, energy, environmental and international issues to improve Canada's and Alberta's economic and social performance.

CANADA AND THE CHALLENGES OF CYBERSPACE GOVERNANCE AND SECURITY*

Ron Deibert

SUMMARY

When Canada stood with the United States and Britain in refusing to sign on to a new, state-controlled future for the Internet, at December's World Conference on Information Technology, it certainly made the federal government appear to be a stalwart champion of Internet freedom. But in reality, Canada's approach to cyberspace governance and security has, at best, sent mixed signals about our commitment to Internet freedom. At worst, it has actually contributed to increasing on-line censorship and surveillance by the very undemocratic and illiberal regimes that Canada voted against at the conference.

Unfortunately this is a dangerous time for Canada to wallow in aimlessness: when it comes to cyberspace governance and security, the momentum is headed in the direction of greater state control. As demographic realities indicate, Internet usage will increasingly belong to the global South and East, where freedom is an unsettled and elusive concept. If Canada truly seeks to guard against the Internet falling captive to the controls sought by repressive regimes, such as those in China and Russia, it will have to offer the world a compelling, competing vision that demonstrates integrity and dedication to genuine Internet freedom.

Among other things, that means moving beyond traditional top-down, state-centred models of security, which are a poor fit for a decentralized, global, publicly shared, but largely privately developed, communications network. Imposing conventional, state led policing frameworks on cyberspace — for instance, in the name of fighting cyber crime — only provides legitimacy to regimes abroad when they bring their own state powers to censor Internet communications. It also means thinking more carefully about how much we should tolerate our Canadian technology developers continuing to supply tools of repression to the foreign regimes who seek to dominate their own people.

Canada has the potential to take on a leadership role in showing the world what it means to truly stand for freedom in cyberspace. But providing global leadership will require that our own government commits to reducing state controls and surveillance here at home, encouraging greater transparency and checks on state power over the Internet, while enhancing privacy protections. Ultimately, the only way the Canadian government can truly help preserve and promote a decentralized and unfettered Internet for the world's future is to demonstrate that it is genuinely committed to promoting the same thing here at home.

* This research was financially supported by the Government of Canada via a partnership with Western Economic Diversification.

UNIVERSITY OF CALGARY

THE SCHOOL OF PUBLIC POLICY
SPP Communiqué

Volume 5 • Numéro 3
Mars 2013

Les communiqués de l'École de politique publique sont de courts articles portant sur une question particulière de politique publique et visent à fournir au lecteur une analyse concise, critique et ciblée.

Copyright © 2013 par l'École de politique publique.

Tous droits réservés. Il est interdit de reproduire cette publication en tout ou en partie de quelque façon que ce soit sans autorisation écrite, sauf sous forme de courtes citations dans des articles et des recensions.

L'Université de Calgary regroupe des chercheurs dans 16 facultés (et proposent plus de 80 programmes d'études) et 36 instituts et centres de recherche, notamment l'École de politique publique. Sous la direction de Jack Mintz, titulaire de la chaire Palmer d'études des politiques publiques, et avec la collaboration de plus de 100 enseignants et chercheurs, les travaux de l'École de politique publique et de ses étudiants contribuent à un débat public étayé sur les questions financières, sociales, énergétiques, environnementales et internationales, pour améliorer le rendement économique et social du Canada et de l'Alberta.

GOUVERNANCE ET SÉCURITÉ DANS LE CYBERESPACE AU CANADA : LES DÉFIS*

Ron Deibert

RÉSUMÉ

Le Canada a certainement fait figure de champion inconditionnel de la liberté sur le Web en refusant, à l'instar des États-Unis et de la Grande-Bretagne, d'avaliser un nouvel avenir sous contrôle gouvernemental pour Internet, à la conférence internationale sur les technologies de l'information, en décembre dernier. Mais en réalité, le moins qu'on puisse dire est que la position du Canada en matière de gouvernance et de sécurité dans le cyberespace est ambiguë. On peut même craindre qu'elle ait contribué à renforcer les mesures de censure et de surveillance en ligne de régimes autoritaires et antidémocratiques contre lesquels le Canada a voté à cette conférence.

Malheureusement, le moment est malvenu pour que le Canada se permette autant d'indolence et d'indécision : la tendance en ce qui a trait à la gouvernance et à la sécurité dans le cyberspace va dans le sens d'un plus grand contrôle gouvernemental. Comme l'indique la réalité démographique, c'est dans l'ensemble des pays du Sud et de l'Est qu'on fera bientôt le plus grand usage d'Internet, là où le concept de liberté est insaisissable. Si le Canada veut réellement empêcher Internet de devenir l'otage de régimes répressifs tels la Chine ou la Russie, il devra proposer au monde entier une vision différente et convaincante, qui soit garante de son intégrité et de sa détermination à maintenir la liberté sur Internet.

Entre autres choses, cela signifie qu'on doit délaisser les modèles de sécurité traditionnels fondés sur une pyramide hiérarchique et gouvernementale, qui peuvent difficilement convenir à un réseau de communications décentralisé, international, public et largement développé par le secteur privé. En imposant des cadres conventionnels de surveillance étatique au cyberespace — au nom, par exemple, de la lutte contre la cybercriminalité — on ne fait que légitimer la censure de certains régimes étrangers à l'égard des communications sur Internet. Il convient aussi de réfléchir plus à fond pour déterminer dans quelle mesure nous devrions tolérer que les développeurs canadiens de la technologie continuent de fournir des outils de répression à des régimes étrangers qui cherchent à opprimer leurs propres citoyens.

Le Canada a les moyens d'assumer un rôle de leadership pour montrer au monde qu'il entend réellement défendre la liberté dans le cyberespace. Mais pour ce faire, notre gouvernement devra s'engager à réduire les contrôles gouvernementaux et la surveillance ici même, au pays, et encourager la transparence et l'adoption de balises pour encadrer le pouvoir du gouvernement sur Internet, tout en améliorant les mesures de protection de la confidentialité et des renseignements personnels. En fin de compte, le Canada ne pourra réellement contribuer à préserver et promouvoir un réseau Internet décentralisé et libre à l'avenir et dans le monde qu'en s'engageant à cet égard ici même, au pays.

* Cette recherche a été soutenue financièrement en partie par le gouvernement du Canada via Diversification de l'économie de l'Ouest Canada.

Rarely does the meeting of an international organization warrant any popular attention, let alone an organization as obscure as the International Telecommunications Union (ITU). Yet, this meeting was an exception. The buildup to the ITU's December 2012 World Conference on Information Technology (WCIT), held in the United Arab Emirates, was immense. For months in advance, apprehension grew over what a new ITU agreement could mean for the future of Internet governance.[1] Two competing visions were pitted against each other: one favouring multi-stakeholder participation and an unfettered Internet; the other, a more state-based system of nationally based controls, supported by China, Russia and a growing number of like-minded allies.

Once thought to be dinosaurs of the information age, autocratic and democratically challenged countries, such as China and Russia, have proven to be adept at navigating cyberspace, showing a resilience that belies the conventional wisdom. They've adapted, excelled, and even fashioned a new strategy of Internet governance that may just succeed. Part of that strategy includes an international dimension: helping to set global technical standards, pushing for exports of national products and services, and working through regional and international organizations to propagate norms of state control.[2] Their active participation in the ITU-WCIT meeting was a case in point. Had they been able to push through their interests successfully, the Russians, Chinese, and their allies, would have passed new International Telecommunication Regulations (ITRs) that would have brought the Internet under a more state-based system of international controls.

In the end, their opponents' worst fears never materialized. The death knell came as the U.S. ambassador to the ITU, Terry Kramer, took to the podium and announced that the U.S. could not sign on to the final declaration. He was joined by several other countries, among them Canada.[3] For the moment, the ITU's Internet land grab was forestalled. But the future remains unclear. The ITU is but one forum, and the momentum is clearly moving in the direction of greater state controls. Here it is important to remember a demographic fact: today, and increasingly in the future, the vast majority of the world's Internet population will come from the global South and East, many of them living in authoritarian or democratically challenged states. A battle at the WCIT may have been won; but the war remains far from over.

The ITU-WCIT process also raised several questions worth contemplating in some depth. While the U.S., Canada, and their allies showed at the ITU what they are against, it is not entirely clear what, exactly, they're *for*. Certainly the phrases "Internet freedom" and "multi-stakeholder" are trumpeted loudly and repeatedly, but it is not entirely clear what they mean or whether they have any depth. They are a bit like "floating signifiers," in the words of Claude Lévi-Strauss — that is, they "represent an undetermined quantity of signification, in itself void of meaning and thus apt to receive any meaning."

---

1 Milton Mueller examines the potential dangers emerging from the WCIT negotiations in "Internet Revolution in Crisis," Index on Censorship, December 3, 2012, http://www.indexoncensorship.org/2012/12/internet-global-itu-wcit/.

2 Masashi Crete-Nishihata and Ronald J. Deibert, "Global Governance and the Spread of Cyberspace Controls," *Global Governance* 18 (2012): 339-361.

3 For an in-depth explanation of why the U.S. government decided not to sign the new Internet telecommunications regulations, see: Remarks of Terry Kramer at the World Conference on Internet Telecommunications, Dubai, United Arab Emirates, December 13, 2012, http://www.state.gov/e/eb/rls/rm/2012/202040.htm.

The reason is that the countries that promote these principles and are ostensibly their most vociferous advocates regularly contradict them in practice. Across the U.S., U.K., Canada, and among many European countries, the state is being privileged in Internet governance, stifling new copyright laws are being enacted,[4] Internet service providers (ISPs) are being compelled to police the Internet often without judicial oversight,[5] extensive new powers are being delegated to the most secretive intelligence agencies,[6] and state-backed content filtering and takedown regimes are now becoming routine.[7] With the Stuxnet virus, the U.S. and its allies are now on record as the first to employ offensive computer network attacks to take down and sabotage another state's critical infrastructure.[8] There is now a *digital arms race* in cyberspace.

As with traditional arms races, the private sector sees a market opportunity and a cyber-security military-industrial complex has mushroomed in response.[9] New products and services are being developed that put in the hands of policy makers, law enforcement, military leadership, and intelligence officers, capabilities never before imagined: big data analytics, deep-packet inspection, cell-phone tracking, geo-locational monitoring, targeted network intrusion and offensive computer network attack capabilities. Many of these products and services are developed by western firms, but are finding their way into the very regimes that are held up as the biggest threats to "Internet freedom." U.S., Canadian, British, and European

---

4 For example, the Anti-Counterfeiting Trade Agreement (ACTA), signed by the U.S., EU, Mexico, South Korea, Singapore, New Zealand, Australia, and Canada (and ratified by Japan), is controversial because of (among other reasons) its broad definition of criminal liability, which would hold the private sector legally responsible for what users do or share through their services. A larger discussion of the concerns associated with the Anti-Counterfeiting Trade Agreement is available in Michael Geist, "The Trouble with the Anti-Counterfeiting Trade Agreement (ACTA)," *SAIS Review* 30.2 (2010).

5 For example, Canada's proposed Bill C-30, now effectively shelved, would have authorized the Canadian government to install surveillance equipment in Internet and telecom service providers and mandated the disclosure of subscriber information as well as the warrantless disclosure of e-mails and online surfing habits. While the government killed Bill C-30, warrantless surveillance is far from dead. As Michael Geist explains, "On the same day the government put the bill out its misery, it introduced Bill C-55 on warrantless wiretapping. Although the bill is ostensibly a response to last year's R v. Tse decision from the Supreme Court of Canada, much of the bill is lifted directly from Bill C-30." See Laura Payton, "Government Killing Online Surveillance Bill," CBC News, February 11, 2013, http://www.cbc.ca/news/politics/story/2013/02/11/pol-rob-nicholson-criminal-code-changes.html; and Michael Geist, "Lawful Access id Dead (For Now): Government Kills Bill C-30," Michael Geist, February 12, 2013, http://www.michaelgeist.ca/content/view/6782/125/; and Christopher Parsons, "Lawful Access is Dead; Long Live Lawful Intercept!," Technology, Thoughts, and Trinkets, February 11, 2013, http://www.christopher-parsons.com/blog/technology/lawful-access-is-dead-long-live-lawful-intercept/.

6 For example, the United States Congress recently approved a five-year extension of the Foreign Intelligence Surveillance Act (FISA) Amendments Act, a domestic spying bill that authorizes the warrantless surveillance of Americans' overseas communications. Also see: Timothy B. Lee, "The New FISA Compromise: It's Worse Than You Think," Ars Technica, July 8, 2008. http://arstechnica.com/tech-policy/news/2008/07/fisa-compromise.ars.

7 In many Western countries, ISPs are required to filter websites and services that are associated with illegal file sharing. See: "Dutch Internet Providers Forced to Block the Pirate Bay," Digital Civil Rights in Europe, January 18, 2012, http://www.edri.org/edrigram/number10.1/dutch-isps-block-piratebay; "The US Pressure On Spain to Censor the Internet Has Paid Off," Digital Civil Rights in Europe, January 18, 2012, http://www.edri.org/edrigram/number10.1/spain-adopts-sinde-law; and "Italy: Problematic Internet Blocking Decision Against Fraudulent Website," Digital Civil Rights in Europe, March 28, 2012, http://www.edri.org/edrigram/number10.6/italy-internet-blocking-case.

8 David Sanger, "Obama Ordered Wave of Cyberattacks Against Iran," *New York Times*, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

9 Ronald Deibert and Rafal Rohozinski, "The New Cyber Military-Industrial Complex," *Globe and Mail*, March 28, 2011, http://www.theglobeandmail.com/news/opinions/opinion/the-new-cyber-military-industrialcomplex/article1957159.

technology and equipment are now used throughout the former Soviet Union, the Middle East, and Asia to restrict freedom of speech, limit access to information, and infiltrate the computers of meddlesome dissidents and activists.[10]

Paradoxically, the worst outcomes many people feared would materialize at the ITU at the behest of the Russians and Chinese, are indeed materializing, but not because of any decision taken by the ITU. They are being driven by western democracies.

****

Where does Canada stand? Where should it stand? The Canadian government is late to the cyber-security and governance arena. Its 2010 Cyber Security Strategy was thin on details, and even thinner on commitments and resources.[11] We do not yet have a clearly defined foreign policy for cyberspace, and Canada is not generally seen as a vocal advocate for any particular set of policies in the area.

Yet, like many other countries, much is at stake. Our critical infrastructure is as susceptible to attack as much as any other advanced knowledge economy, and there have been several high-profile breaches of Canadian government agencies and private businesses, which should give everyone pause. The now bankrupt Nortel was reportedly breached for up to 10 years by a cyber-espionage network emanating from China that reached right up to the executive level.[12] How many other corporations are presently suffering the same fate is anyone's guess. Like many other countries, we do need to secure cyberspace, but the question is how, especially in the context of complicated 21st century political and economics relationships, and geopolitical challenges.

There is an instinctive tendency in international security policy-making to default to the tradition of realism, with its accompanying characteristics of state-centrism, top-down hierarchical controls, and a defensive perimeter to the threats outside. As compelling as this tradition may be, it fits awkwardly in a world where divisions between inside and outside are blurred, threats can emerge as easily within as without, and that which requires securing — namely cyberspace — is a globally networked commons of information almost entirely in the hands of the private sector. Moreover, this model privileges state-based agencies as leads in securing cyberspace, which can create awkward privacy concerns in domestic settings while fueling reciprocal suspicions on an international scale. At their worst, they lend legitimacy to the very policies we ostensibly oppose abroad and give credence to Russian, Chinese, and

---

[10] Vernon Silver, "FinFisher Spyware Reach Found on Five Continents: Report," *Bloomberg*, August 8, 2012, http://www.bloomberg.com/news/2012-08-08/finfisher-spyware-reach-found-on-five-continents-report.html; Karen McVeigh, "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; and Margaret Coker and Paul Sonne, "Firms Aided Libyan Spies," *Wall Street Journal*, August 30, 2011, http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html.

[11] Government of Canada, "Canada's Cyber Security Strategy," 2010, http://www.publicsafety.gc.ca/prg/ns/cbr/_fl/ccss-scc-eng.pdf.

[12] Jameson Berkow, "Nortel Hacked to Pieces," *Financial Post*, February 25, 2012, http://business.financialpost.com/2012/02/25/nortel-hacked-to-pieces.

other similar states' efforts to territorialize Internet governance. We can see some of these tendencies materializing in Canada today: in the over-reaching lawful-access Bill C-30, now shelved because of widespread political backlash, which would have done away with basic protections for civil liberties while setting up a digital surveillance regime of substantial proportions; they are also evident in the ballooning size, growing importance, and yet persistent 'cold war style' secrecy around the Communications Security Establishment of Canada (CSEC),[13] and the Canadian intelligence service as a whole, now poised to take on leadership roles in securing cyberspace. But instinctive tendencies fostered by bureaucratic subcultures and old-school paradigms are not the only way to go.

In the following section, I lay out some principles that form the basis for an alternative approach to Canadian cyberspace and security policy, and draw from and encourage other tendencies than the classical Realist, state-based approach. Canada has much to offer in the area of cyberspace governance and security. Indeed, there is a major opportunity for Canada and Canadians not only to secure our cyberspace here at home, but to help build the foundation for a more open and connected world. In order to grasp that opportunity, we need to remind ourselves of some fundamental principles that should inform our strategy moving forward.

****

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. There are many different ways to secure cyberspace, depending on the values that underline that which requires protection in the first place. Cyber security is, therefore, inherently a discussion about political philosophy when debated in a policy or governance context. What political system do we want to secure?

Canada's cyber-security strategy should begin with an articulation of first national principles. 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. In the West, cyberspace has largely been constructed as an open and distributed ecosystem. The Internet, the communications backbone of networked cyberspace, is a mixed common pool resource, the vast majority of it in the hands of the private sector. In functional terms, as a network, the Internet functions on the basis of decentralized organization rather than hierarchical control as in the case of the public telephone network.

---

[13] The mandate of Communications Security Establishment Canada (CSEC) was updated under Canada's Anti-terrorism Act of December 2001. The act stipulates that CSEC collect information from "the global information infrastructure" about the "capabilities, intentions or activities of a foreign individual, state, organization or terrorist group, as they relate to international affairs, defence or security." A second part of its mandate focuses on security of information infrastructures in Canada, while a third specifies CSEC should assist federal law enforcement and security agencies "in performance of their lawful duties." See: Anti-terrorism Act, SC 2001, c.41, s.102, codified as National Defence Act, RSC 1985, c.N-5, s,273.61-273.7 [National Defence Act].

At the heart of Canada's cyber-security strategy, therefore, should be a strong affirmation of both our liberal democratic national first principles along with the open architecture principles that undergird Western cyberspace. Together these two sets of social and technical principles could form a unified vision of what is best described as *distributed security*. Distributed 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 is at the heart of liberal-republican theories of security going back to ancient Greece.[14] Distributed security offers a contrast to both traditional Realist or statist versions of security — which are antithetical to the openness of cyberspace as a global commons — and to simplistic anti-authority views which would do away with security altogether. It describes a system of rule in between the extremes of hierarchy and anarchy. Distributed security emphasizes mixture, division and restraint.

Starting with these first principles can help frame a full spectrum cyber-security agenda from the local 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. 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 that basic rights and freedoms are protected as constitutive principles. Law enforcement, armed forces, and intelligence agencies all still have critical missions in contributing to cyber security, especially in the turbulent interdependent world in which we currently live. However, securing cyberspace, while at the same time keeping it open, will require a multitude of co-operative 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.

Second, and related, a comprehensive strategy to protect the cyber commons should begin by **linking the international consequences of domestic policies**. If liberal- democratic countries govern their own societies in ways that infringe on basic rights, then they have no moral basis with which to condemn those actions when they occur in places like Russia, China, Iran, or Belarus.

While it is certainly true that law enforcement is overwhelmed with the surge of cyber crime, it does not mean that its agencies should be given unrestricted access to private data. As many civil liberties groups have chronicled, the types of virtually unrestricted access that many law enforcement agencies seek in Canada and the West already constitute a major threat to the principles and norms that support a healthy liberal-democratic society. In fact the opposite may be more the case. The problem for law enforcement and intelligence today is not a lack of information; it is the deluge of it. We need to give law enforcement new resources, capabilities, proper training and equipment to sort through voluminous flows of existing data. But alongside those resources, Canada should be setting the highest standard of judicial oversight and public accountability. New resources, yes, but the same, if not more rigorous checks and constraints on powers.

---

[14] Daniel H. Deudney, *Bounding Power: Republican Security Theory From the Polis to the Global Village* (Princeton: Princeton University Press, 2007).

Open Up the Black Box. 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 as a whole. These agencies are now taking on a more expansive role as cyber security becomes a more vital issue to national security. They have enormous path dependency, through a built-up reservoir of practices, expertise, and sunk costs, that make the implementation of regulatory 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 cyber security.

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. 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 are abundant and plentiful — there is a very strong argument to be made that national security agencies should have more, rather than fewer, checks and balances.

Here again, the international implications of domestic policies matter as well. The more that 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 for state surveillance domestically, the less likely it is to occur abroad.

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. Unfortunately, doing so clashes with the culture of secrecy that surrounds these institutions, and the tradition of national security in Canada as a whole, a tradition still very much immersed in a Cold War military 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.

Privacy is a Security Issue Too. A comprehensive approach to cyber security should amplify 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 mobile phones, social networking, and cloud computing. As more data is shared internationally and with third parties, the security of Canadians' personal data is a critical public policy issue. Privacy commissioners are best poised to evaluate, monitor, and raise awareness about these concerns, and Canadian privacy commissioners have a proven track record of leadership in cyberspace policy matters here in Canada, and enjoy a strong reputation for it abroad. It is a strength we should build upon and use as a model to export to countries just now beginning to grapple with cyberspace governance and security.

Canadian policy towards cyberspace governance and security must address squarely the market for **"dual-use" technologies** and what many are calling **the "digital arms trade."** 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 disreputability of its clients, and how it operates in brazen openness.[15] Some Canadian companies are included in this market: Sandvine reportedly provides deep packet inspection products and services to countries in the former Soviet Union, where they may be applied to stifle dissent;[16] Netsweeper products are presently used to censor access to basic information in Qatar, the United Arab Emirates and Yemen;[17] Blackberry (formerly Research in Motion) is being pressured to collude with many governments who claim a need for greater surveillance,[18] and the company may have already set up facilities to do so in India.[19] It also reportedly censors access to information in Indonesia, and possibly elsewhere too.[20] As the pressures to control and secure cyberspace grow and the user base shifts to the global South and East, these market opportunities and pressures to comply with "local laws" and needs will grow, too. With them will come some important ethical and legal issues.

Although Canada cannot independently solve these issues on a global level, it can at least tackle them at home, and with respect to how Canadian companies should operate abroad. At the very least, it can join discussions in Europe[21] and in the United States[22] that attempt to set regulations and standards around the export of sensitive technologies to regimes that violate basic human rights. In the absence of such discussions, Canada may find itself to be a leader in cyber security of a sort: in a rogue market, about which most Canadians would be ashamed rather than proud.

---

[15] Ben Wagner, Exporting Censorship and Surveillance Technology (The Hague: Hivos, 2012), http://www.hivos.nl/content/download/72343/618288/file/Exporting%20Censorship%20And%20Surveillance%20Technology%20by%20Ben%20Wagner.pdf; and Rebecca MacKinnon, "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.

[16] See "The Kremlin's New Internet Surveillance Plan Goes Live Today," Wired.com (November 11, 2012), http://www.wired.com/dangerroom/2012/11/russia-surveillance/all/

[17] Helmi Noman and Jillian C. York, "West Censoring East: The Use of Western Technologies by Middle East Censors, 2010–2011," OpenNet Initiative, http://opennet.net/west-censoring-east-the-use-western-technologies-middle-east-censors-2010-2011; and "When a Canadian Company Decides What Citizens in the Middle East Can Access Online," OpenNet Initiative, May 16, 2011, http://opennet.net/blog/2011/05/when-a-canadian-company-decides-what-citizens-middle-east-canaccess-online.

[18] Ronald Deibert, "Cyberspace Confidential," *Globe and Mail*, August 6, 2010, http://www.theglobeandmail.com/commentary/cyberspace-confidential/article1241035/?page=all.

[19] "RIM Sets Up Facility to Help Indian Government with Lawful Surveillance," *Toronto Star*, October 28, 2011, http://www.thestar.com/business/article/1077575--rim-sets-up-facility-to-help-indian-government-with-lawful-surveillance?bn=1.

[20] Andreas Ismar, "RIM Starts Internet Filters in Indonesia," *Wall Street Journal*, January 21, 2011, http://online.wsj.com/article/SB10001424052748704881304576093174017705238.html.

[21] European member of Parliament Marietje Schaake proposed that the EU enact laws that regulate the export of technologies to countries that use them to violate human rights, saying that it is "unacceptable that regimes in Syria and Iran can use European technologies to violate human rights, let alone that European companies are actively involved in that." Schaake's proposal is detailed in "European Parliament Endorses Stricter European Export Control of Digital Arms," Marietje Schaake, October 23, 2012, http://www.marietjeschaake.eu/2012/10/ep-steunt-d66-initiatief-controle-europese-export-digitale-wapens.

[22] U.S. congressional lawmakers have debated to restrict such sales, for instance, through the Global Online Freedom Act. See: Cindy Cohn, Trevor Timm, and Jillian C. York, "Global Online Freedom Act 2012 Is An Important Step Forward," Electronic Frontier Foundation, April 18, 2012, https://www.eff.org/deeplinks/2012/04/global-online-freedom-act.

We Need a Foreign Policy for Cyberspace. Just as domestic developments can have repercussions around the world, what happens around the world can come here to bite us 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 2010 Cyber Security Strategy, the Department of Foreign Affairs and International Trade (DFAIT) was tasked with developing a cyber-security foreign policy "that will help strengthen coherence in the Government's engagement abroad on cyber security." To date, a foreign policy for cyberspace has not been articulated, although the department is exploring the area and is beginning to participate more actively in international forums. Unfortunately, cyber security does not appear as one of DFAIT's "priority commitments for 2011-2012."[23]

However, 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. As with domestic policy, a Canadian foreign policy for cyberspace should start with first principles. Distributed security can help guide us here too. Rather than centralizing control of cyberspace in new institutions, as some governments are proposing to do, Canada should be forcefully advocating instead for re-investment in the grassroots and distributed forms of multi-stakeholder governance that keep the Internet and related technologies running today. Our efforts at the ITU-WCIT meeting, in which Canada joined other like-minded countries in resisting proposals to include Internet governance in ITU regulations, are a good basis from which to continue to work. Our government should aid in the promotion of civil society and private-sector participation in governance forums where such stakeholders are typically excluded. In those forums that are formally restricted to state participation, we should act as an information bridge. Outreach and consultation with multiple stakeholders should be our government's hallmark.

Diplomatically, we should work to build a broad community of like minded-states that share an interest in the promotion of norms of mutual restraint in cyberspace, protections for privacy and civil liberties, joint vigilance against cyber crime networks, and respect for the free flow of information. This engagement should also include international and regional forums of cyberspace governance. In recent years, the traditional organs of cyberspace governance (ICANN, the Internet Engineering Task Force, the Regional Internet Registry system and others) have been joined by a variety of others, including the G8, G20, OECD, Organization for Security and Co-operation in Europe (OSCE), European Commission, as well as the ITU, the UN General Assembly, and a lengthy list of regional organizations. Obviously the scarcity of 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.

---

[23] The issue of "cyber crime" 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 Drugs and Crime, and the Organization of American States).

Canada's foreign policy in cyberspace should include a dedicated outreach component with countries — including civil society in those countries — that will matter most for the future of cyberspace governance and policy going forward. Here, Canada's foreign-policy strategy might be linked to international development and aid policy to encourage networks of engineers, policy makers, and researchers from North and South to share best practices around rights, security, and governance in cyberspace. However, doing so will require a reversal of recent trends that have seen Canadian international development and aid scaled back and reoriented around a business-first rationale. Such thinking may look good on accountant's ledger, but it is the type of short-term thinking that could eventually hurt us at home.

Canadian foreign policy must also address military issues in cyberspace. Encouraging norms of mutual restraint among states in a situation of growing tensions in cyberspace will be critical to furthering all of the aforementioned principles. Canada's experience in arms-control regimes might help, but we need to understand the nuances around the issue area. Information — the central ingredient of warfare in cyberspace — is 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 (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 a guide for conducting 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. Canadian participation in these forums should be encouraged and broadened.

There is also a largely informal and quite influential cyber-security "epistemic community" that cuts across public and private sectors, that secures cyberspace in a largely ad hoc but occasionally very co-ordinated 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 in which governments, the private sector, and civil society work to contain and mitigate unwanted behaviour in cyberspace around shared operating procedures and principles. The critical questions will be whether such mitigation is done in a transparent and accountable way or not, and if it avoids the risks of cyber vigilantism. Canada's long-standing experience with arms-control policy and regimes, and especially its experience 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 marshaled and drawn upon in this sector.

****

As one of the world's largest economies and home to some of the greatest thinkers in the communications field, from Harold Innis and Marshall McLuhan to William Gibson, Canada should be forging a leading position in global cyberspace governance and security. We certainly stand among those with the most to lose should cyberspace continue its spiral into

censorship, securitization, militarization, and crime. Looking ahead, there are a great many challenges and opportunities for Canada, but tackling them will require imagination, dedication, and a willingness to think outside the box — something one hopes that a new generation of cyber savvy policy makers and Foreign Service officers will eventually encourage. As we grapple with the appropriate responses to the tough challenges presented by global cyberspace and the mounting pressures to bring cyberspace under state-based control, we need to ensure we do not lose sight of what makes our society so valuable, and why we were so opposed to the ITU land-grab in the first place.

About the Author

Ron Deibert (OOnt, 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 laboratory focusing on advanced research and development at the intersection of digital media, global security, and human rights.