Centre for International
Governance Innovation

# Governing Cyber Security in Canada, Australia and the United States

SPECIAL REPORT

Centre for International
Governance Innovation

# Governing Cyber Security in Canada, Australia and the United States

SPECIAL REPORT

Edited by Christian Leuprecht and Stephanie MacLellan

## CIGI Masthead

### Executive

President Rohinton P. Medhora
Deputy Director, International Intellectual Property Law and Innovation Bassem Awad
Chief Financial Officer and Director of Operations Shelley Boettger
Director of the International Law Research Program Oonagh Fitzgerald
Director of the Global Security & Politics Program Fen Osler Hampson
Director of Human Resources Susan Hirst
Interim Director of the Global Economy Program Paul Jenkins
Deputy Director, International Environmental Law Silvia Maciunas
Deputy Director, International Economic Law Hugo Perezcano Díaz
Director, Evaluation and Partnerships Erica Shaw
Managing Director and General Counsel Aaron Shull
Director of Communications and Digital Media Spencer Tripp

### Publications

Publisher Carol Bonnett
Senior Publications Editor Jennifer Goyder
Publications Editor Susan Bubak
Publications Editor Patricia Holmes
Publications Editor Nicole Langlois
Publications Editor Lynn Schellenberg
Graphic Designer Melodie Wakefield

For publications enquiries, please contact publications@cigionline.org.

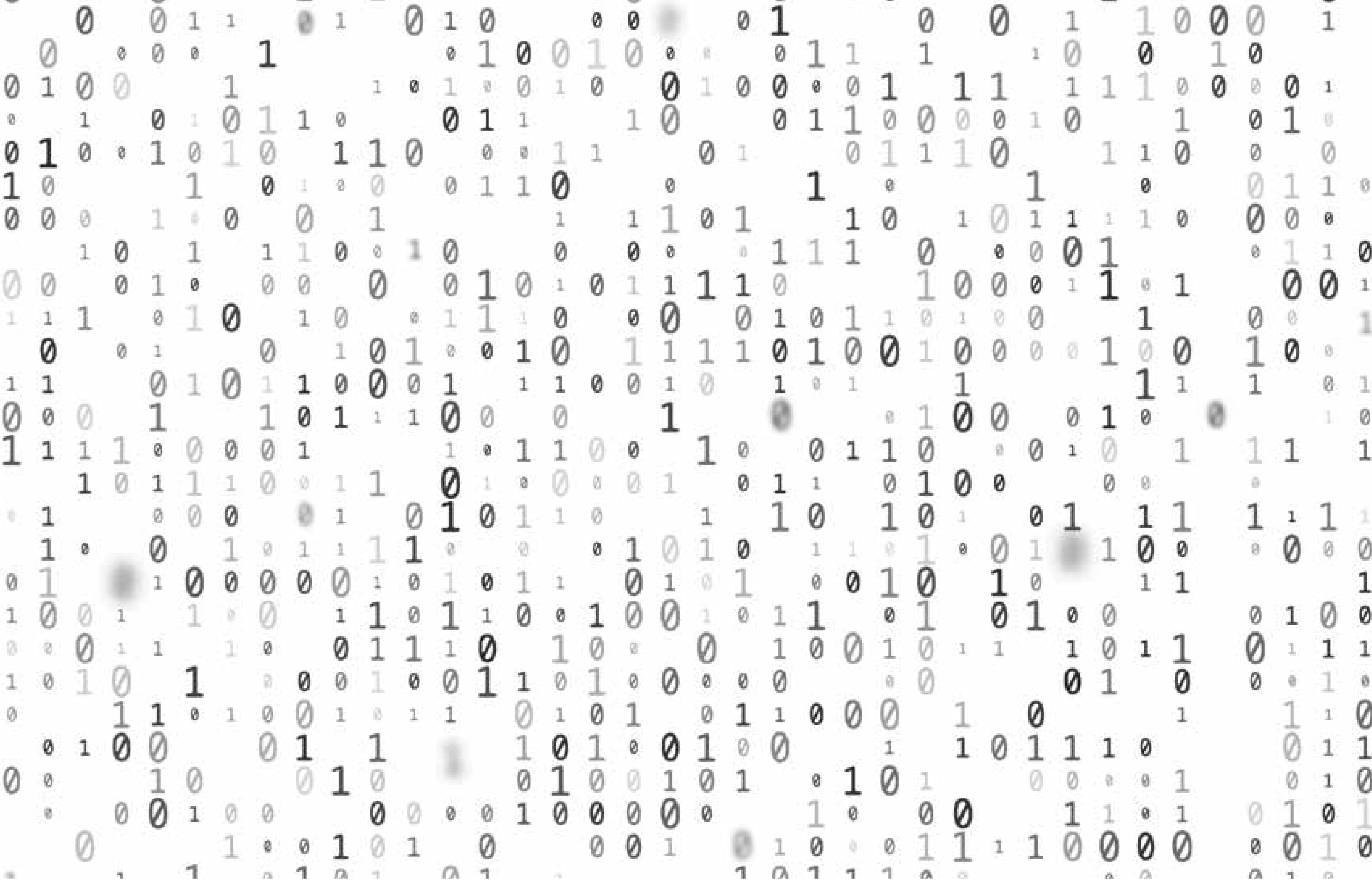
### Communications

For media enquiries, please contact communications@cigionline.org.

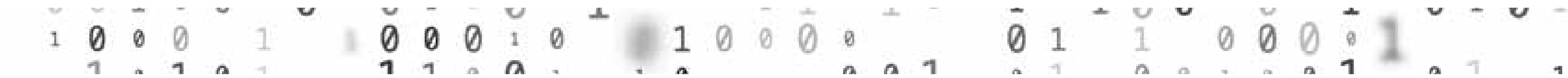
The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the Centre for International Governance Innovation or its Board of Directors.

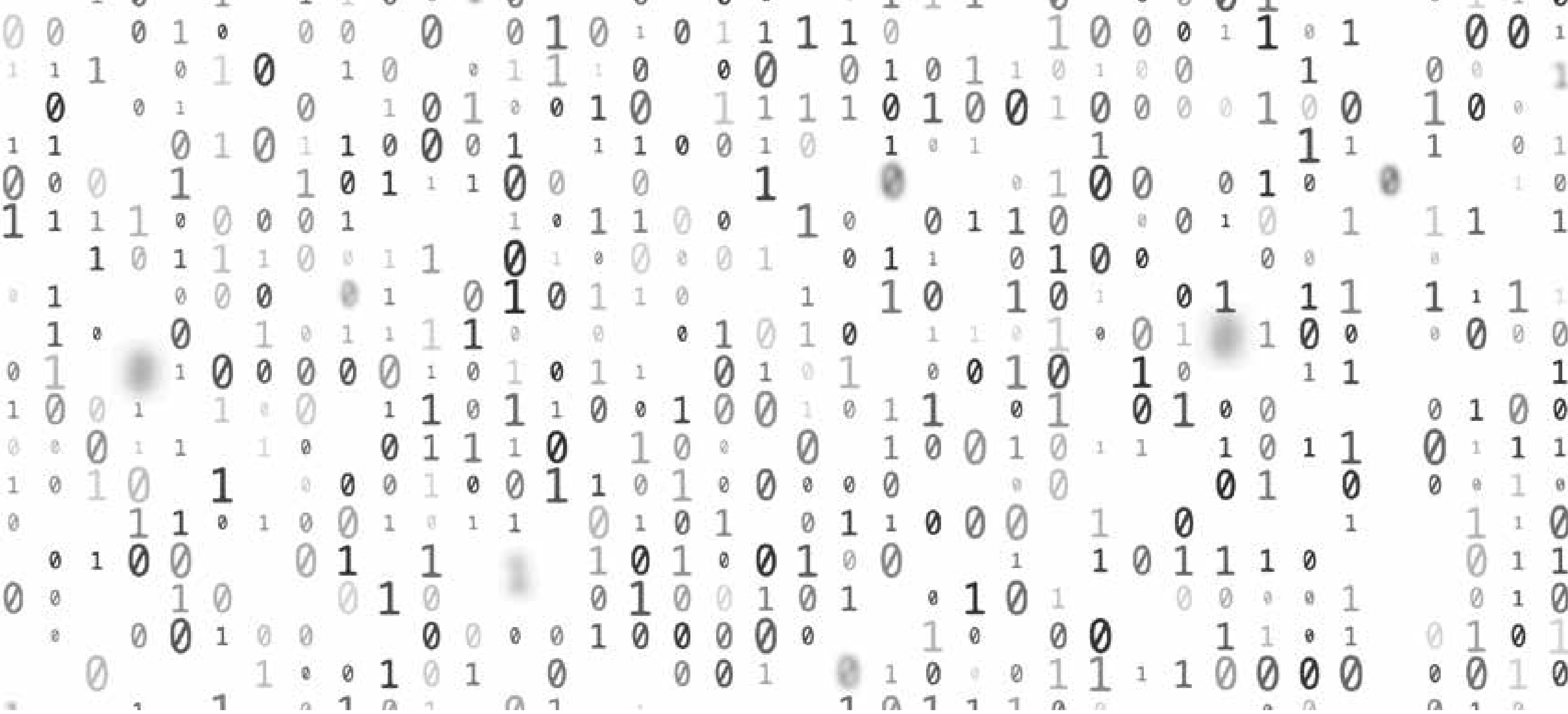
Centre for International
Governance Innovation

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org



# Contents

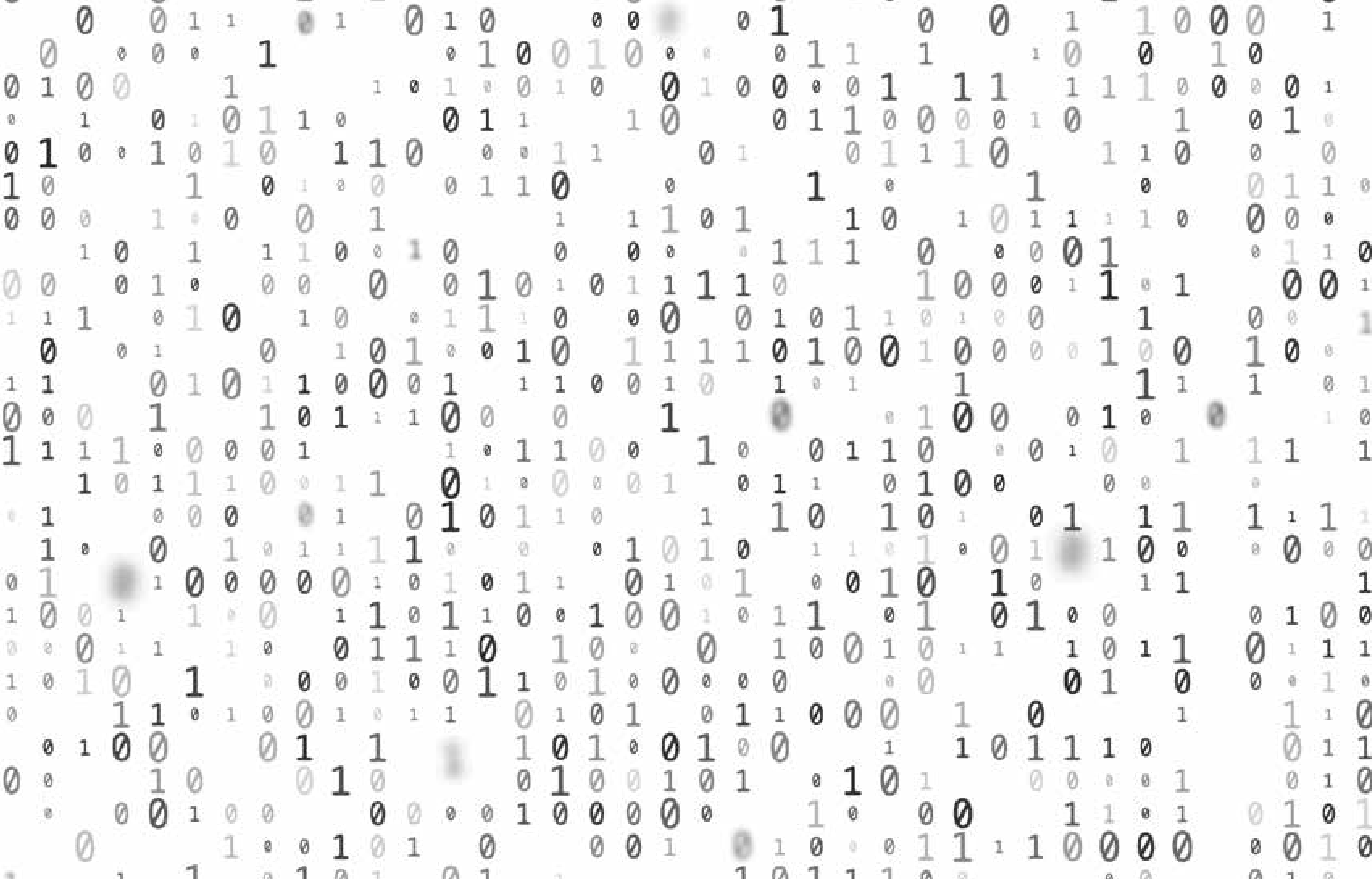




# Acronyms and Abbreviations

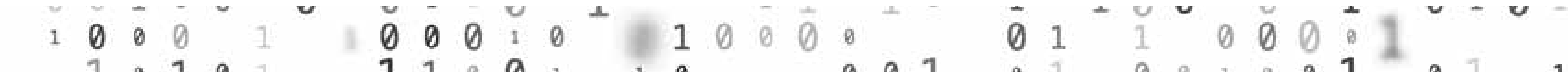
| | |
|---|---|
| ACIC | Australian Criminal Intelligence Commission |
| ACSC | Australian Cyber Security Centre |
| AFP | Australian Federal Police |
| AGD | Attorney-General’s Department |
| APWG | Anti-Phishing Working Group |
| ASD | Australian Signals Directorate |
| ASIO | Australian Security Intelligence Organisation |
| CANDU | Canada Deuterium Uranium |
| CNSC | Canadian Nuclear Safety Commission |
| COAG | Council of Australian Governments |
| COP | Child Online Protection |
| CSA | Canadian Securities Administrators |
| CSA Group | Canadian Standards Association Group |
| CSPG | Cyber Security Peer Group |
| DTA | Digital Transformation Agency |
| EC3 | European Cybercrime Centre |
| eNACSO | European NGO Alliance for Child Safety Online |
| FCACP | Financial Coalition Against Child Pornography |
| FIRST | Forum for Incident Response and Security Teams |
| GPECN | Global Prosecutors E-Crime Network |
| I-24/7 | Interpol’s global police communications system |
| IAEA | International Atomic Energy Agency |
| ICMEC | International Centre for Missing & Exploited Children |
| ICS | industrial control system |
| IGCI | Interpol Global Complex for Innovation |
| IMPACT | International Multilateral Partnership Against Cyber Threats |
| ISAC | information-sharing and analysis centre |
| IT | information technology |
| ITU | International Telecommunication Union |
| JCSC | joint cyber security centres |
| NEI | Nuclear Energy Institute |
| NGOs | non-governmental organizations |
| NICS | National Institutes of Cyber-Security |
| NRC | Nuclear Regulatory Commission |
| OSFI | Office of the Superintendent of Financial Institutions |
| PM&C | Prime Minister and Cabinet |
| SNA | Social Network Analysis |
| UAE | United Arab Emirates |

This special report was produced by the Centre for International Governance Innovation (CIGI) in collaboration with the Smart Cybersecurity Network (SERENE-RISC). SERENE-RISC is a knowledge mobilization network funded by Canada's National Centres of Excellence with the aim of improving the general public's awareness of cyber security risk and empowering all to reduce those risks by mobilizing knowledge.
For more information, please visit www.serene-risc.ca.



# Introduction

Christian Leuprecht and Josh Tupler



Now that cyber vulnerabilities pose serious risks to prosperity, democracy and social harmony, cyber security has become a complex and all-encompassing political, social, economic and technological phenomenon.[1] Since the turn of the century, the nature and scope of the internet and its users have changed fundamentally. In 1995, an estimated 16 million people worldwide had access to the internet, and all users accessed it via fixed-line connections. Twenty years on, more than half of the world's population is online and, among them, more than half access the internet via mobile devices. Over 20 billion devices are projected to become connected to the Internet of Things in the next five years alone (Naughton 2016). Cyberspace has become integral to the flow of goods and services; to support for critical infrastructure (such as electricity, water, banking, communication and transportation); and to the control of industrial, security and military systems (Nye 2017). Technology has garnered much of the attention — in particular, individual actions or vulnerabilities of specific systems in certain countries — along with the way content on the internet is governed.[2]

By contrast, this is a study in the dimensions of intergovernmental relations and multi-level governance on which cyber security and related policy are

[1] For the purposes of this special report, the term "cyber" is used in its broadest sense: "of, relating to, or involving computers or computer networks (such as the Internet)" (www.merriam-webster.com/dictionary/cyber).

[2] For an overview of the history of the internet, see Naughton (2012; 2016). For non-technical explanations of how the internet works and associated governance issues, see Goldsmith and Wu (2006); Blum (2012); DeNardis (2014); MacKinnon (2013). For non-technical summaries of the offensive capabilities and impact on national security of cyber weapons, see Nye (2017); Negroponte, Palmisano and Segal (2013); Singer and Friedman (2014); Clarke and Knake (2010).

ultimately contingent but which, thus far, have received short shrift. The essays in this collection ponder the division of authority and responsibility — for cyber, in general, and cyber security, in particular — between public and private actors and different levels of government. Optimizing governance arrangements is a function of how cyber security is conceptualized, as well as of the stakeholders involved. Drawing on expertise and insights from business, law, policy and academia, the authors posit normative models of cyber security governance; gauge the advantages and disadvantages of different approaches; and formulate policy proposals.

Each essay considers at least one of these five questions:

→ Is cyber security a public or private good, and who are the key actors involved in its administration?

→ What should the division of authority and responsibility between public and private actors and different levels of government look like in the provision of cyber security in Canada?

→ What is the current Canadian approach to cyber security governance, and is it consistent with normative models and best practices of cyber security governance?

→ Are there lessons to be learned from international cyber security governance models, especially in closely allied countries, and are there best practices to be adopted from non-cyber sectors?

→ Given the shortcomings and constraints identified, where do Canadian policy makers and cyber security practitioners go from here?

The initial essays offer an overview of the state of play of cyber security governance in Canada and two of its close allies, explaining the principal actors and underscoring the importance of governance. Brent J. Arnold provides a legal perspective on Canada's cyber policies. He reviews current Canadian policy in addressing cyber risk; positions Canada's efforts in an international context; and considers the prospects for an intergovernmental approach to managing cyber risk, in Canada and internationally. By analyzing Canadian policy in the context of other international cyber legal regimes and models, Arnold puts Canadian cyber policy in perspective and isolates key actors whom the Canadian government should focus on to increase cooperation and improve its approach to cyber security.

David Mussington critically assesses the sources, and impediments to progress, of US cyber policy. He offers insights into how political, economic and constitutional factors have created a complex intergovernmental environment that both shapes American cyber policy and encourages myriad non-governmental actors with competing interests to influence it. Mussington posits federalism as an impediment to governments, both federal and state, to take action to minimize cyber risk: on the one hand, the federal government has hegemonized US cyber policy; on the other hand, with a couple of nascent exceptions, states have been happy to disavow any responsibility for this policy area.

Liam Nevill discusses how Australia has changed its cyber security governance practices to adapt to the multi-faceted nature of the threat. Australia has preferred to retrofit existing governance institutions — by co-locating agencies to work toward a singular approach — rather than to significantly change existing institutions. Nevill details initiatives in Australia's 2016 Cyber Strategy that have increased cyber resiliency by clarifying roles and responsibilities and broadening partnerships among the Commonwealth, states or territories, and the private sector.

Subsequent essays in this collection offer descriptive and prescriptive insights on Canadian and international cyber security policy regimes. Scott Hilts offers a rare case study in multi-level governance that has yielded positive outcomes with his examination of the cyber-related vulnerabilities of Canadian critical infrastructure systems. In the process, he identifies lessons and best practices developed by the nuclear power industry, which includes significant private sector involvement. In analyzing the regulation of the Canadian Nuclear Safety Commission and its development of cyber security standards, Hilts distills pragmatic advice to protect other non-nuclear-related infrastructure.

Benoît Dupont offers insight into the actors and institutional arrangements that were and are being formed to fight transnational cybercrime. Dupont uses social network analysis to measure, visualize and analyze how a diverse set of actors collaborate in cyberspace. His analysis finds that the international security network has a polycentric structure that involves four main groups of organizational actors — national law enforcement agencies, international organizations, private companies and non-governmental organizations (NGOs) — that all play distinct roles in facilitating cyber security.

Finally, Timothy Grayson and Brian O'Higgins argue for more involvement by NGOs in cyber security, to facilitate dialogue and promote best practices. They make the case for a coordinator and facilitator of cyber policy, and recommend the formation of an independent NGO, to assemble the best of Canadian cyber security innovation, policy and practice so as to seize the unique opportunities this rapidly evolving and growing economic space offers.

This collection of essays provides a framework to analyze policy options. Cyber security experts have tended to offer technical advice or recommendations that fail to account for governance arrangements. Academics can be overly focused on normative, institutional or theoretical issues, while policy makers are easily tempted to get too deep into the weeds. This report is an attempt to harness synergies among different perspectives, with the aim of optimizing policy outcomes when jurisdictional responsibilities do not align neatly with the best technical or most rational approach. By way of the aforementioned research questions, the authors aim to contribute to a more informed discussion about the importance and the role of intergovernmental affairs and multi-level governance to cyber security.

## Works Cited

Blum, Andrew. 2012. *Tubes: Behind the Scenes at the Internet*. London, UK: Penguin.

Clarke, Richard A. and Robert K. Knake. 2010. *Cyber War: The Next Threat to National Security and What to Do About It*. New York, NY: Ecco.

DeNardis, Laura. 2014. *The Global War for Internet Governance*. New Haven, CT: Yale University Press.

Goldsmith, Jack and Tim Wu. 2006. *Who Controls the Internet? Illusions of a Borderless World*. Oxford, UK: Oxford University Press.

MacKinnon, Rebecca. 2013. *Consent of the Networked: The Worldwide Struggle for Internet Freedom*. New York, NY: Basic Books.

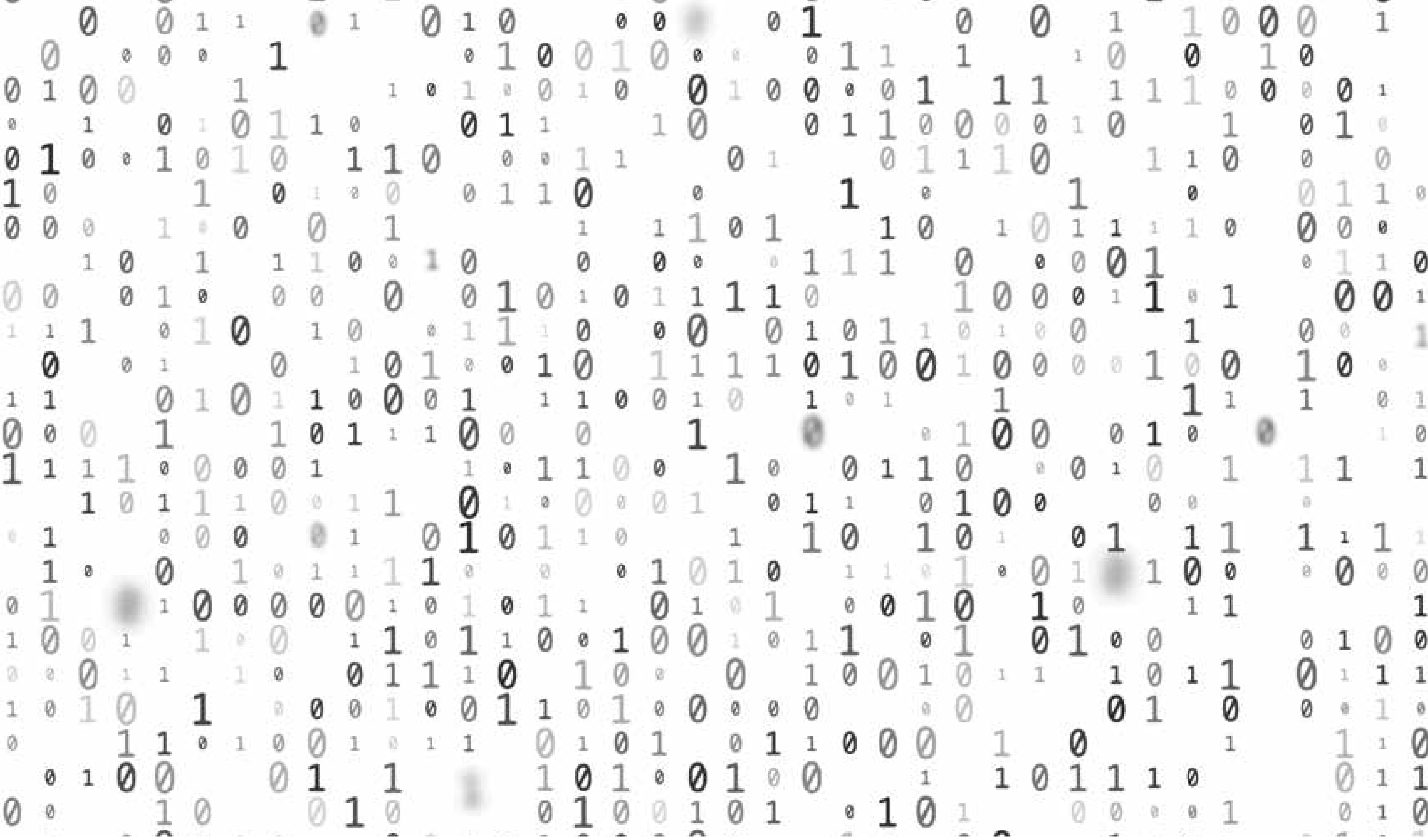
Naughton, John. 2012. *From Gutenberg to Zuckerberg: What You Really Need to Know about the Internet.* London, UK: Quercus.

———. 2016. "The Evolution of the Internet: From Military Experiment to General Purpose Technology." *Journal of Cyber Policy* 1 (1): 5–28.

Negroponte, John D., Samuel J. Palmisano and Adam Segal. 2013. *Defending an Open, Global, Secure, and Resilient Internet*. Independent Task Force Report No. 70. New York, NY: Council on Foreign Relations.

Nye, Joseph S., Jr. 2017. "Deterrence and Dissuasion in Cyberspace." *International Security* 41 (3): 44–71.

Singer, Peter W. and Allan Friedman. 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York, NY: Oxford University Press.



# Cyber Security in Canada: Structure and Challenges

Brent J. Arnold

It is, by now, trite to observe that cyber risk is a global phenomenon, transcending national borders and endangering the infrastructure and citizenry of developing and developed nations, democracies and authoritarian regimes alike. (The WannaCry ransomware attack in May 2017, unprecedented in the speed and scale of its global reach, provides an alarming example.) A trite response to this global problem would posit a global solution — which is far easier to propose than to achieve. This essay reviews the state of the Canadian approach to addressing cyber risk, positions Canada's efforts in an international context and considers the prospects for an intergovernmental approach to managing cyber risk in Canada and internationally.

## Canada's Cyber Regulatory Regime

Scholarship in this area describes different state-level models for regulating cyber security: first, a principle-based framework focused on good practice, and second, a more ad hoc style of regulation focused less on good practice and more on repelling cyber threats, which approaches risk regulation on an industry-specific basis (Kshetri 2016, generally and §5.6).

Canada's cyber regulatory regime favours the second model, at least in some respects. To begin, it adopts threat repulsion rather than best practices as its organizing principle. Canada's national cyber security strategy, in place since 2010 (although legislation to update it was proposed in June 2017), focuses on repelling foreign-state actors, criminals and terrorists (Government of Canada 2010, 1). This strategy advances a three-pillar program: securing federal government systems; partnering with lower levels of government and the private sector to secure cyber systems outside the federal government; and improving online security for Canadians, through a combination of public education and enhanced law enforcement capabilities (ibid., 7).

In practice, this focus has meant a combination of various federal government initiatives to improve its own planning, detection and response capabilities; the development of a national coordination centre to support the private sector and other levels of government; public education programs; and legislation aimed at protecting personal data (Government of Canada 2013). The proposed new Communications Security Establishment Act would also allow Canada's cyber security agency to conduct offensive and defensive cyber operations as a way to mitigate or neutralize attacks against Canada.[1]

Canada's regime is also closer to the ad hoc approach in that it consists of a patchwork of legislative responses to particular issues rather than a comprehensive data security law (ibid.). Federal legislation criminalizes hacking and digital spying (Criminal Code[2]), prevents installation of spyware, regulates collection and use of personal information by federal departments and agencies (Privacy Act[3]), and regulates the collection, use and disclosure of personal information by private sector commercial entities (Personal Information Protection and Electronic Documents Act[4]). Provincial laws cover this last category as well, with provincial acts, where they exist, superseding federal law. Provinces also regulate the collection of personal health information by hospitals and health care providers.

## Private Sector Coordination

Sector-specific legislation is supplemented by guidance from industry regulators, most comprehensively in the financial sector. The Office of the Superintendent of Financial Institutions (OSFI) has published cyber security self-assessment guidance (OSFI 2013), operational risk guidelines (OSFI 2016) and an operational risk self-assessment tool (OSFI 2017) for federally regulated financial institutions. Similarly, the Canadian Securities Administrators (CSA), an umbrella organization of provincial and territorial securities regulators whose pronouncements are selectively adopted and enforced by the local regulators, has released a series of staff notices advising securities issuers to assess and manage their cyber risk (CSA 2013), announcing various initiatives for 2016–2019 (CSA 2016) and, more recently, publishing the results of a review of disclosure documents to address the modest extent to which Canadian issuers are reporting cyber security risks in their disclosure (CSA 2017). The Mutual Fund Dealers Association of Canada (2016) and the Investment Industry Regulatory Organization of Canada (2015) have published guidelines for their members as well. Such guidelines do not have the force of law in themselves, but will undoubtedly be used as the baseline against which courts and regulatory bodies attempting to define standards of care will measure private actors' conduct.

Canada's regulatory regime is also supplemented by non-state actors seeking to fill the gaps between the various government departments and initiatives by providing coordination among private entities and the public and private sectors. The recently launched Canadian Cyber Threat Exchange, an information-sharing and analysis centre (ISAC) with member businesses of various sizes, coordinates the sharing of cyber threat information among members, across sectors and with the government agencies.[5] Similarly, the Bank of Canada has created the Joint Operational Resilience Management program, with the aim of bringing together large financial institutions, government departments and payment systems to coordinate industry response in the event of a severe cyber attack (Gallagher, McMahon and Morrow 2014, 52).

Such organizations remain largely untested, and the extent to which they can successfully coordinate a complex cast of private and public characters to deal with cyber security crises remains to be seen. As with industry-provided guidelines, early indications suggest that membership and participation in ISACs, in particular, may come to form part of the standard of care expected of companies under judicial and regulatory scrutiny after falling prey to cyber attacks.[6]

[1] Bill C-59, *An Act respecting national security matters*, 1st Sess, 42nd Parl, 2017 (first reading 20 June 2017).

[2] *Criminal Code*, RSC 1985, c C-46 at ss184, 243.1.

[3] *Privacy Act*, RSC 1985, c P-21.

[4] *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5.

[5] See https://cctx.ca/mission/.

[6] For example, the recently proposed settlement of US derivative actions against Home Depot (*In re Home Depot Inc. S'holder Derivative Litig., N.D. Ga.*, No. 1:15-CV-2999-TWT), currently awaiting court approval, requires the company to participate in "at least one" ISAC: "Plaintiffs' Unopposed Motion for Preliminary Approval of Shareholder Derivative Settlement and Memorandum of Law in Support," www.dandodiary.com/wp-content/uploads/sites/265/2017/05/home-depot-settlement.pdf, at 2, 7-8.

## International Integration

Canada's cyber security regime exists in the context of a multilateral response to cyber risk that is at best partial and tentative, one in which competing national agendas and approaches have limited prospects for coordinated action.

International law applies to cyberspace, prohibiting direct and indirect cyber attacks by states and setting out the conditions under which they may use cyber force to defend themselves, and obliges states to ensure that cyber infrastructure within their borders is not used against other states. However, the application of international law's broad principles to the unique circumstances of cyber attacks is vague on a number of issues (Schmitt 2013). And, of course, the international law regime focuses on state actions, not cybercrime (although the distinction between the two is grey at best, given the difficulties in attributing acts to particular state actors, and the tendency of states to operate through non-state actors to achieve anonymity).

With respect to cybercrime, as of May 2017, only 55 countries (including Canada) had signed and ratified the Budapest Convention (Council of Europe 2017), the only multilateral treaty focused specifically on cybercrime, and many ratifying nations have joined under numerous reservations (Kshetri 2016, §3.3). Nations have had difficulty in agreeing on a common standards-setting institution due to, for instance, concerns about cementing American hegemony over regulation of the internet (ibid.).

As the problem of cyber security involves infrastructure and expertise largely in private hands, and activity that ignores geographical borders, the solution evolving at the global level reflects that found at the national level in Canada and elsewhere: an "open, multi-stakeholder model [that] mirrors the traditional technical management of the Internet" (Solana 2015) — put differently, a collection of states, companies, non-governmental organizations and academics groping toward consensus and cooperation. The Global Forum on Cyber Expertise (of which Canada is a member) provides a recent example of such efforts. Even those organizations calling for a global approach to cyber security (such as the World Economic Forum) acknowledge that the non-participation of some of the world's largest cyber powers (the United States, China, Russia and North Korea) in key global initiatives limits the horizons of such an approach (ibid.).

## Conclusions

Canada's approach to cyber security is threat-based, federal, multi-stakeholder and international. Its laws are supplemented by sector-based regulators, private corporations and organizations coordinating state and non-state actors and initiatives. This approach both benefits from and, to a large extent, depends on private sector initiative at the national and international levels, and international cooperation between state and non-state actors.

## Works Cited

CSA. 2013. "CSA Staff Notice 11-326 — Cyber Security." Notices/New Releases, September 26. www.osc.gov.on.ca/documents/en/Securities-Category1/csa_20130926_11-326_cyber-security.pdf.

———. 2016. "CSA Staff Notice 11-332 — Cyber Security." September 27. www.osc.gov.on.ca/documents/en/Securities-Category1/sn_20160927_11-332-cyber-security.pdf.

———. 2017. "CSA Multilateral Staff Notice 51-347 — Disclosure of cyber security risks and incidents." Notices/News Releases, January 19. www.osc.gov.on.ca/documents/en/Securities-Category5/20170119_51-347_disclosure-cyber-security.pdf.

Council of Europe. 2017. "Chart of signatures and ratifications of Treaty 185." www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=JcVaqrug.

Gallagher, Harold, Wade McMahon and Ron Morrow. 2014. "Cyber Security: Protecting the Resilience of Canada's Financial System." Bank of Canada *Financial System Review,* December. www.bankofcanada.ca/wp-content/uploads/2014/12/fsr-december14-morrow.pdf.

Government of Canada. 2010. "Canada's Cyber Security Strategy for a Stronger and More Prosperous Canada." www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf.

———. 2013. "Action Plan 2010-2015 for Canada's Cyber Security Strategy." http://publications.gc.ca/collections/collection_2013/sp-ps/PS9-1-2013-eng.pdf.

Investment Industry Regulatory Organization of Canada. 2015. *Cybersecurity Best Practices Guide for IIROC Dealer Members*. www.iiroc.ca/industry/Documents/CybersecurityBestPracticesGuide_en.pdf.

Kshetri, Nir. 2016. *The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies*. Cham, Switzerland: Springer.

Mutual Fund Dealers Association of Canada. 2016. "Bulletin #0690-C — Cybersecurity." May 19. http://mfda.ca/bulletin/Bulletin0690-C/.

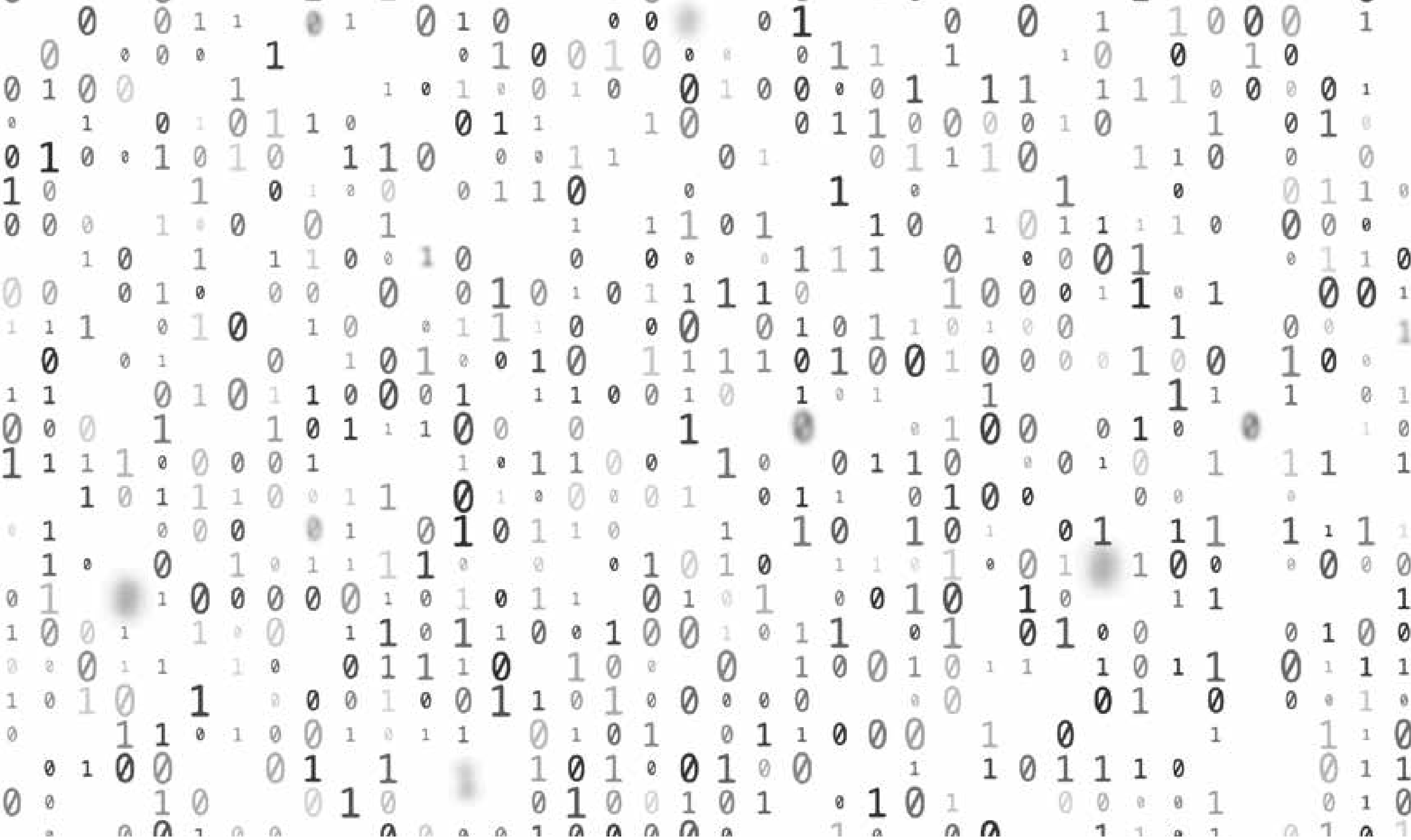
OSFI. 2013. "Cyber Security Self-Assessment Guidance." Memorandum to Federally Regulated Financial Institutions, October 28. www.osfi-bsif.gc.ca/Eng/Docs/cbrsk.pdf.

———. 2016. "Guideline E-21: Operational Risk Management." June. www.osfi-bsif.gc.ca/Eng/Docs/e21.pdf.

———. 2017. "Guideline E-21 — Operational Risk Self-Assessment Template." April 12. www.osfi-bsif.gc.ca/Eng/Docs/e21_slfamnt.pdf.

Schmitt, Michael N. 2013. "Cyberspace and International Law: The Penumbral Mist of Uncertainty." *Harvard Law Review Forum* 126 (5): 176–80.

Solana, Javier. 2015. "Why we need a new global approach to cybersecurity." World Economic Forum, May 1. www.weforum.org/agenda/2015/05/why-we-need-a-new-global-approach-to-cybersecurity/.



# US Cyber Policy: Sources of and Impediments to Rapid Progress

David Mussington

Cyber policy in the United States is often argued to be an executive branch responsibility. Directed from the White House through executive orders, and executed by the Department of Homeland Security, sector-specific agencies and the Department of Defense, cyber activities are framed as highly centralized — a top-down process in which the executive branch sets the terms of debate and proscribes norms and mechanisms for public-private collaboration. From this perspective, the US Congress is argued to be a relatively minor player in policy design, legislating only infrequently on cyber issues, but biased against supporting executive-branch administrative regulation of private sector cyber security practices.

This view is both inaccurate and misleading. A myriad of factors in the US public and private sectors shape both cyber policy and achievable risk-management outcomes. This essay discusses a subset of the factors important to shaping US critical-infrastructure cyber security and resilience policies. The policy environment is characterized by a nascent "net effect" character, with federal policy confronting contending decision centres at the state, local, territorial and tribal levels. More generally, the character of American federalism is a key variable not always taken into account when policy trends and responses are considered.

## First Principles

The US Constitution sets the terms of reference for US cyber security policy. While homeland security and national security are federal responsibilities, state, local, territorial and tribal jurisdictions each play important roles in shaping the conditions and decisions surrounding risk management. In addition, critical infrastructures are almost entirely privately owned. Constitutional rights to control property belong to asset and system owners.[1] Accordingly, investment decisions on upgrades and security must align with the expectations of owners (shareholders) for return on investment. States regulate these infrastructures for safety, environmental and security purposes. Public utilities commissions are regulators at the state level, and occupy the constitutional space that covers cyber security of critical systems and key assets.

Reconciling these non-federal influences on critical infrastructures with national security is a key problem. Policy effectiveness requires the knitting together of policy and law at these different levels. The executive orders and presidential decision or policy directives authored at the White House (for example, executive order 13636 — "Improving Critical Infrastructure Cybersecurity" — and presidential policy directive 21 — "Critical Infrastructure Security and Resilience" — both issued on February 13, 2013 (White House 2013a; 2013b) are primary mechanisms for achieving well-integrated and effective policy — at least, this is the goal. Coordination at this level is contested, however, with the US Congress and state governments both jealously guarding their prerogatives and interests. Without either the properly functioning mechanisms to engender information sharing from federal to state levels or open communications channels between private asset owners and government officials on risk concerns, efforts to manage risk are likely to fall short.

## Defining Policy Failure in Cyber Security

A cyber policy development process with poor multi-level integration produces at least three types of serious policy failures — each of which could derail national cyber security efforts and resilience. An example of such a policy involves the efforts to achieve granular and persistent improvements in the cyber security awareness and performance of small and medium-sized enterprises. Analysis has shown that information sharing is less effective for smaller businesses than it is within and among large firms. In addition, metrics for evaluating cyber security risk identification and performance are poorly developed and not well disseminated.[2] First, guidance and recommendations at the federal level on cyber risk management may be overtaken — or superseded — by mandatory or privately funded changes in infrastructure operation or configurations deriving from non-security planning and operations imperatives. Second, long-term capital investments may involve the deployment of technologies and systems that pose basically unknown (but non-zero) cyber risks to vital services. Additionally, these systems may not be subject to close regulation by the federal government. Most narrowly, these sometimes subtle changes in software and hardware subsystems often carry significant economic and safety benefits. Where long-standing legal mandates exist, these infrastructure changes are often long-term and based in sector and technical risk or reliability judgments less accessible to government — or bound up in concepts of safety and operational risk management. Put simply, businesses know more about their own operations than government agencies do. Ostensibly "sensible" security recommendations may be infeasible or too costly if they are not framed within the current and changing features of a critical infrastructure's operating environment.

Third, cyber threats to critical infrastructures may be uncovered by internal sources (companies) or external entities. For internal risk identification, insiders may successfully provide the earliest possible detection and remediation possibilities for cyber vulnerabilities (Verizon 2017, 8). In practice, however, most cyber breaches are externally detected, by law enforcement, third-party contractors or fully independent academic or non-governmental organizations.[3]

Government may discover breach activity in private critical infrastructures, but these discoveries do not translate into direct risk-remediation actions, for the reasons already given. Assets' exposure to cyber risk is only partially a function of government-prioritized risk or vulnerability concerns.

These three factors are actually interdependent. Nothing guarantees, however, that these issues will be effectively managed: authorities for mandating actions exist in different — and contending — governmental jurisdictions, and at different levels (federal, state, local, territorial and tribal).

Even more seriously, technological change creates new potential risk factors exploitable by potential adversaries. This "external" source of policy challenges confronting both public authorities and the private sector requires the creation of effective mechanisms for coordinated risk response and incident management.

[1] The US Constitution's Bill of Rights (Amendments 1–10 of the Constitution) is the foundation for these rights.

[2] Private sector efforts to make up for public sector shortfalls in cyber information sharing are common, as are business complaints on the availability of actionable information. See Harrison (2017).

[3] The Cybersecurity Information Sharing Act of 2015 is designed to incentivize just this type of behaviour. For an analysis of this legislation, see Harvard University's examination of the issues in play (Karp 2016).

## Implications

The US cyber security policy environment is not centralized. While US federal policy is focused by executive orders and congressional legislation, outcomes — actions taken to mitigate risk and longer-term decision making on priorities — are determined elsewhere by private actors and political jurisdictions at the state, local, territorial and tribal levels. The net impact of these partially independent points of decision is pervasive lags in strategic responses to changes in threat conditions. While cyber incident responses are sector-, jurisdiction- and case-specific, longer-term risk-management activities leveraging intelligence and other insights may not be successful in shaping the risk environment because their impact is blunted by conflicts of interest.

Complex federal-state relations can make US cyber policy difficult to understand. A key point is to be aware of the differing time horizons over which policy change occurs. Federal policy has been driven by executive decisions, with congressional legislation relatively infrequent and narrow in direct impact.

More hidden is the shaping impact over the longer term of basic operational and investment decisions in critical infrastructures, made by the private sector within policy constraints created and maintained by state and local jurisdictions. Cyber security concerns have only recently begun to influence policy making at non-national levels. This creates a gap that can impede timely responses to emerging cyber risks or vulnerabilities. Interestingly, this gap may impede both federal and private sector efforts at managing cyber risk.

Coordination of these three elements of the cyber policy environment is the central requirement for effective and timely risk management. Mechanisms for achieving this reconciliation are mostly ad hoc, leveraging information-sharing channels created by executive order, and intergovernmental structures devised under the auspices of the Department of Homeland Security. As a result, protocols and processes defined at the strategic national level are not necessarily synonymous with effectiveness in cyber risk management.

This essay draws a deliberately sharp contrast between the complex intergovernmental environment where cyber policy emerges, and the fractured public debate on the subject. The point is not that progress on managing cyber risks is impossible. Far from it. Improvements in risk management are readily attainable — but only if the realities of legacy decision making and information asymmetries among the different players in policy development are confronted directly. For the United States, this means the focus should be on the incremental mitigation of cyber risk and the development of performance metrics to evaluate progress and continuing assessment of risk-management practices. As threat conditions continue to worsen, it is important that policy emphasize measurable impact, rather than continue an endless and largely fruitless pursuit of grand strategic visions of a better future. Measurable progress, and innovation in information exchange and policy-persistent impact, must be the focus of activity.

## Works Cited

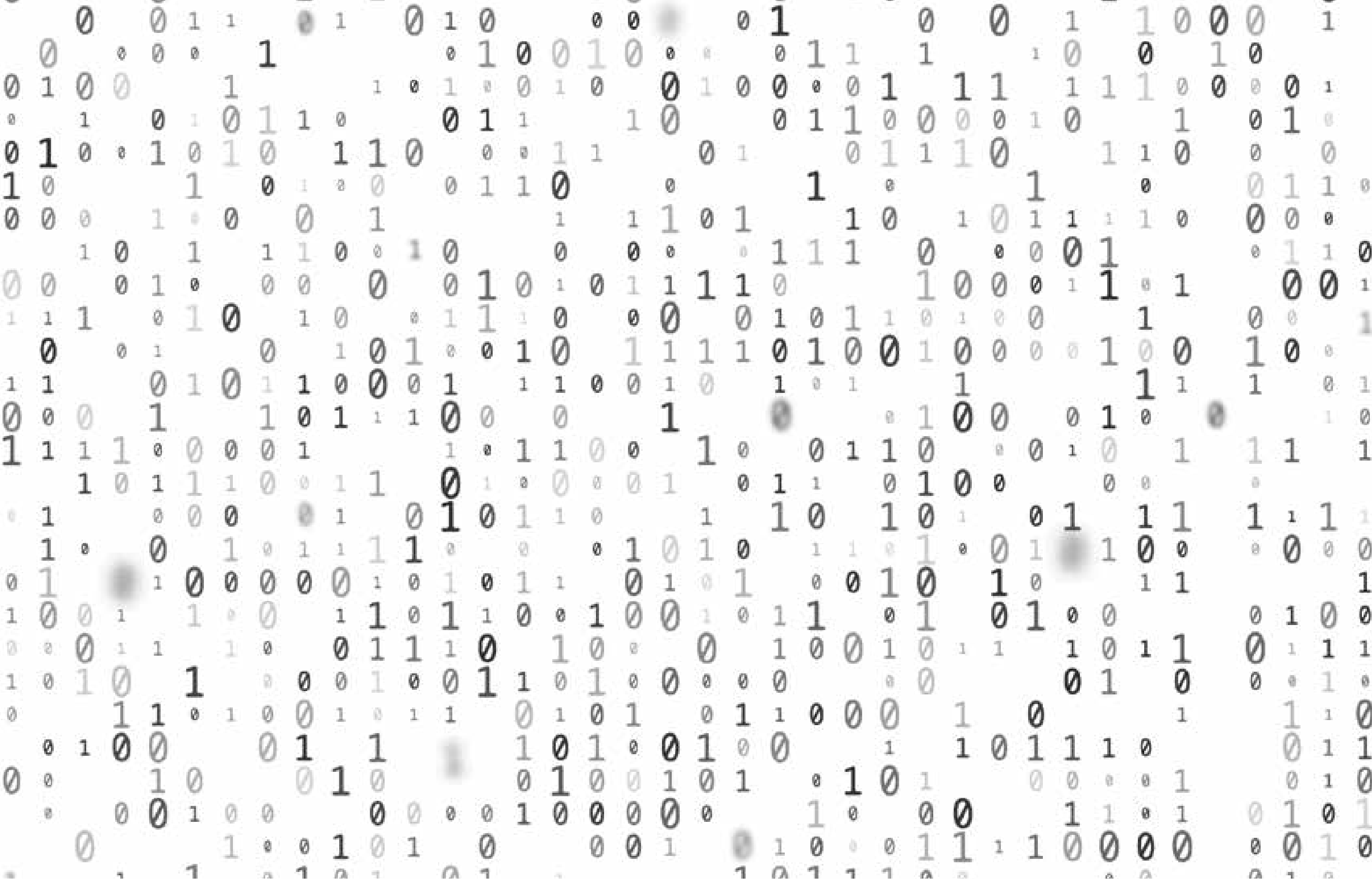
Harrison, Kate. 2017. “The Best Practices in Cyber Security for Small to Medium Sized Businesses.” *Forbes*, May 3. www.forbes.com/sites/kateharrison/2016/05/03/the-best-practices-in-cyber-security-for-small-to-medium-sized-businesses/#5071f89a7346.

Karp, Brad S. 2016. “Federal Guidance on the Cybersecurity Information Sharing Act of 2015.” *Harvard Law School Forum on Corporate Governance and Financial Regulation* (blog), March 3. https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/.

The White House. 2013a. “Executive Order on Improving Critical Infrastructure Cybersecurity.” February 12. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0.

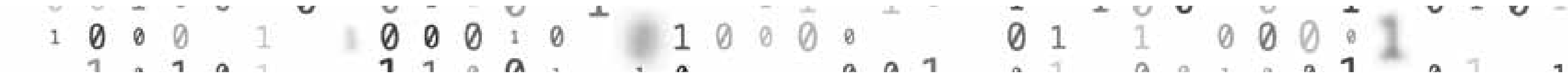
———. 2013b. “Presidential Policy Directive 21: Critical Infrastructure Security and Resilience.” PPD-21. February 12. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

Verizon. 2017. *Verizon Data Breach Investigations Report*. www.verizonenterprise.com/verizon-insights-lab/dbir/2017/.



# Cyber Security Governance in Australia

Liam Nevill



The multi-faceted threats that cyber security presents to national security have challenged states to develop appropriate governance structures to manage their cyber security efficiently and effectively. For advanced states with small populations, the additional challenge is to do so with relatively limited human resources. This challenge lends itself to consolidation and centralization of policy and operational agencies to achieve the necessary efficiencies. Australia, however, has preferred to retrofit existing governance arrangements, including the "co-location" of agencies to achieve the benefits of a single-agency approach, without significantly changing the existing machinery of government. This approach has been dominated by the expertise and capability provided by the Australian Signals Directorate (ASD) (formerly the Defence Signals Directorate), the national signals intelligence agency.

This evolution has happened in isolation from the state or territory governments. This is changing now, in line with the 2016 Cyber Security Strategy's focus on building multi-layered partnerships with states and territories and the private sector to enhance the overall cyber security posture of the country.

## Australian Government Cyber Security Policy and Operations

The Australian government has largely resisted the impulse to form new cyber security policy and operational bodies, instead modifying existing structures to manage cyber security threats. Adjustments to the machinery of government have been made, but the pre-existing government departments have retained their own identities, budgets and chains of command. This has also limited the need for legislative changes as agencies continue to operate under existing laws that govern their operations. The two significant pieces of legislation on cyber security have focused on the private sector, in particular the Telecommunications Security Sector Reforms process that provided for government input and direction regarding security of privately owned telecommunications networks, and the introduction of mandatory data breach legislation (Attorney-General's Department [AGD] 2017; Parliament of Australia 2016a). The arrangements described below are illustrated in Figure 1.

### Operational Responsibilities

Operational cyber security responsibility is divided according to agency responsibilities, but is dominated by the capability and capacity of the ASD, which is an agency of the Department of Defence. ASD's signals intelligence mission means it has the experience and expertise required at a greater scale than other federal government agencies to provide cyber security operational capability. The Attorney-General's portfolio houses the remaining operational capabilities. The national computer emergency response team, CERT Australia, is a constituent element of the AGD, and its portfolio agencies, the Australian Security Intelligence Organisation (ASIO), the Australian Federal Police (AFP) and the Australian Criminal Intelligence Commission (ACIC), maintain operational capabilities that align with their respective responsibilities for security intelligence and counter-espionage, cybercrime enforcement and criminal intelligence.

The division of responsibility among these agencies has remained largely unchanged. The most significant shift took place in 2014 when the ASD, the ASIO, the AFP, the ACIC and CERT Australia were relocated into a joint facility, the Australian Cyber Security Centre (ACSC). Predominately staffed by the ASD and led by an ASD executive, dubbed the ACSC coordinator, the constituent agencies have nevertheless retained their organizational identities, roles and budgets. The ACSC is responsible for responding to cyber security incidents, threat intelligence and analysis, and was originally intended for public-private cyber security engagement and threat information sharing. The ACSC's first home, within the highly secure ASIO headquarters, prevented it from effectively working with the private sector, and it will relocate to a new facility in 2017–2018 (Department of the Prime Minister and Cabinet [PM&C] 2017, 12).

Two new additions are now on the horizon: the pending establishment of a Critical Infrastructure Centre within the AGD and the Cyber Security Advisory Office within the newly formed Digital Transformation Agency (DTA). The Critical Infrastructure Centre will provide security advice to critical infrastructure operators, while the Cyber Security Advisory Office will provide cyber security advice on government information technology procurements and projects. The exact delineation of responsibility for cyber security advice between existing agencies and these new organizations is not well defined, and their establishment will be difficult in a shortage-plagued cyber security job market.

### Policy and Strategy Development

While operational agency responsibilities have changed slightly over time, responsibility for whole-of-government cyber security policy has undergone a relatively dramatic change between 2011 and 2017. Australia has had two national cyber security strategies, first in 2009 (AGD 2009) and later in 2016. Cyber security governance was also addressed in the 2009 Defence White Paper and 2013 National Security Strategy.

Cyber security policy was the responsibility of the AGD until 2011. The AGD produced the 2009 Cyber Security Strategy, which saw the establishment of CERT Australia within the department and incorporated management of cyber security policy with its role of coordinating national critical infrastructure security policy and emergency management.

In 2011, then Prime Minister Julia Gillard announced that policy responsibility would be transferred to the PM&C as part of a broader cabinet reshuffle (PM&C 2011a). No public justification was provided then or since. At the time, as the government was developing a cyber white paper, a national security chief information officer/cyber policy coordinator was installed in the PM&C to manage this process (PM&C 2011b). The cyber white paper was never released, and Australia's turbulent political environment delayed any further updates to national cyber security policy until the 2016 Cyber Security Strategy.

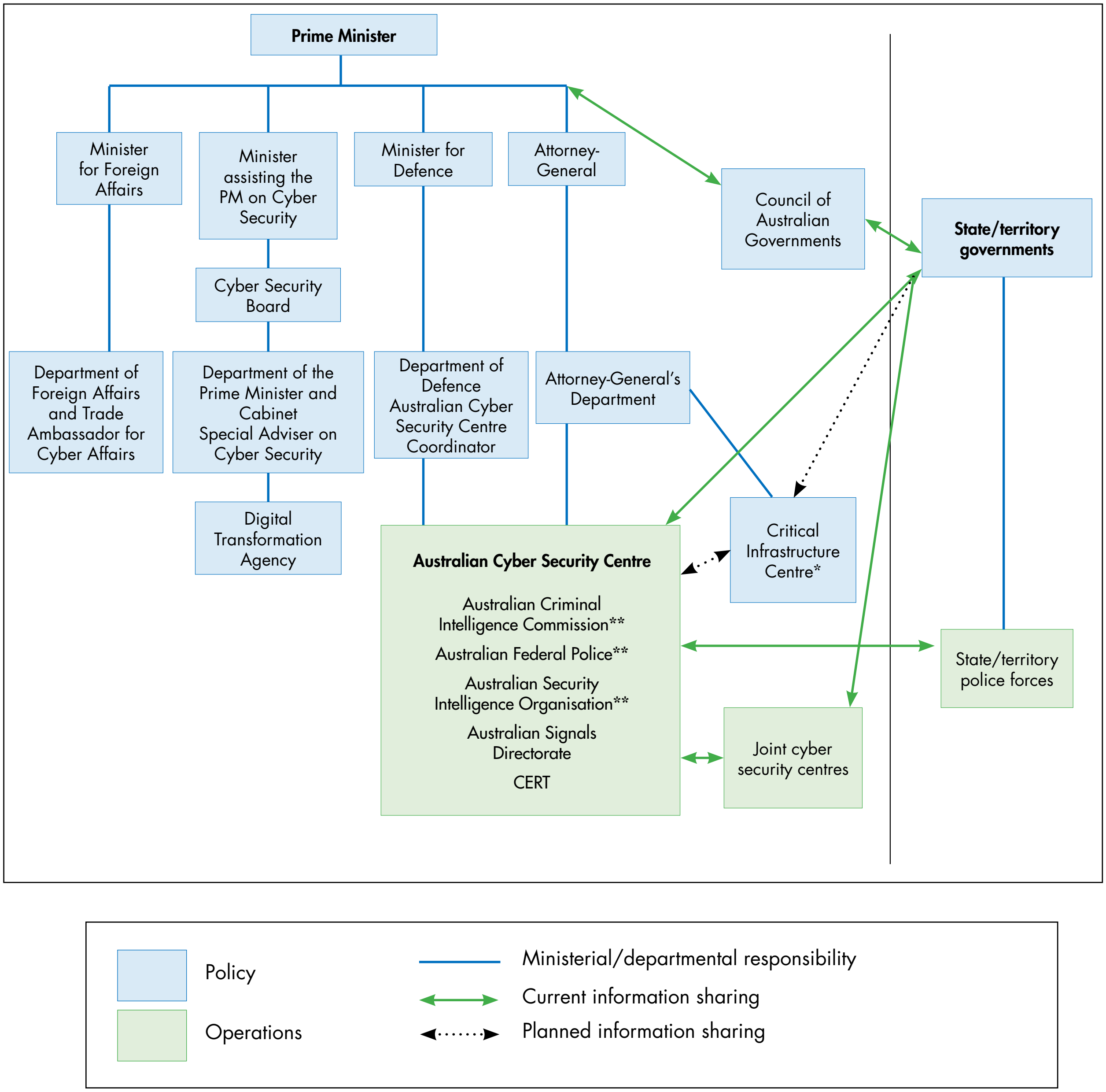
Cyber security governance was also addressed in both the 2009 Defence White Paper produced by the Kevin Rudd government and the 2013 National Security Strategy released by the Gillard government. The 2009 Defence White Paper emphasized the "emerging threat" of "cyber warfare" and established the Cyber Security Operations Centre in what was then the Defence Signals Directorate, now the ASD (Department of Defence 2009). Gillard's 2013 National Security Strategy created the multi-agency ACSC (PM&C 2013).

### 2016 Cyber Security Strategy

The 2016 Cyber Security Strategy saw further significant changes to the governance of cyber policy and operations. A key element of the strategy was an attempt to establish greater clarity regarding roles and responsibilities within a framework of self-responsibility and stronger partnership on cyber security between the federal government, states/territories and the private sector.

The 2016 Cyber Security Strategy included the establishment of a sub-cabinet ministerial post for cyber security, the minister assisting the prime minister for

**Figure 1: Australian Government Cyber Security Policy and Operational Governance Structure, 2016-2017**


Prime Minister
Minister for Foreign Affairs
Minister assisting the PM on Cyber Security
Minister for Defence
Attorney-General
Council of Australian Governments
State/territory governments
Cyber Security Board
Department of Foreign Affairs and Trade Ambassador for Cyber Affairs
Department of the Prime Minister and Cabinet Special Adviser on Cyber Security
Department of Defence Australian Cyber Security Centre Coordinator
Attorney-General's Department
Digital Transformation Agency
Critical Infrastructure Centre*
Australian Cyber Security Centre
Australian Criminal Intelligence Commission**
Australian Federal Police**
Australian Security Intelligence Organisation**
Australian Signals Directorate
CERT
State/territory police forces
Joint cyber security centres
Policy
Operations
Ministerial/departmental responsibility
Current information sharing
Planned information sharing

*Source:* PM&C 2016; 2017.

*Notes:* *The Critical Infrastructure Centre is planned to be established during 2017–2018.

**The Australian Security Intelligence Organisation, the Australian Federal Police and the Australian Criminal Intelligence Commission are portfolio agencies of the Attorney-General's Department; CERT Australia is a constituent part of the Attorney-General's Department.

cyber security. In addition to the ACSC coordinator, two new public service leadership positions were established. The special adviser on cyber security within the PM&C has taken the lead on whole-of-government cyber policy development and coordinates departmental activity in an effort to achieve the outcomes of the Strategy. The ambassador for cyber affairs within the Department of Foreign Affairs and Trade is charged with leadership of the government's international cyber security policy interests. The Strategy also saw the creation of a department-head-level cyber security board; however, its exact role and mandate are not clear.

This new governance structure is intended to create a more coordinated approach to cyber issues across government. The establishment of key leadership positions has also given a more sophisticated voice to cyber issues, both for the Australian public and the region more broadly. The positive role of the minister assisting and the special adviser in the immediate aftermath and subsequent investigation of the 2016 #censusfail incident[1] has highlighted the greater maturity in approach and discourse that the new leadership positions have brought to the management of cyber issues in Australia.

## Federal-State Relations and Cyber Security

The 2016 Cyber Security Strategy recognized that a more resilient national cyber security posture for Australia requires stronger cooperation between the two largest tiers of government and the private sector. This is particularly important as most critical infrastructure is the responsibility of, and often owned and operated by, the state/territory governments.

Before the 2016 strategy, the states/territories had little encouragement from Canberra to take action to manage their own cyber security. The focus of cyber security policy and capability in Canberra left these governments largely outside the scope of national cyber security priorities, and operational engagement has been limited to law-enforcement engagement. State/territory governments are now beginning to take action to manage their own cyber security in partnership with the federal government, and at least two states, New South Wales and South Australia, have now appointed government chief information security officers.

The 2016 Cyber Security Strategy initiated the establishment of new joint cyber security centres (JCSC) in major state capitals. The first centre opened in Brisbane in February 2017. The JCSCs are intended to act as a conduit for cyber threat information among federal and state/territory governments, the private sector and cyber security researchers. These cross-sectoral regional cyber-threat-sharing centres are intended to "build a collective understanding of cyber threats and risks through a layered approach to cyber threat sharing" (PM&C 2016, 6). However, while the JCSCs may enhance operational engagement, discussions at the policy level on national cyber strategy require further attention. Cyber security was discussed for the first time at the Council of Australian Governments (COAG), the pre-eminent forum for federal/state relations, in December 2016, but there is no indication that there will be a regular exchange of views among officials (COAG 2016).

## The Private Sector

Perhaps less neglected has been the Australian private sector. The Australian government has preferred carrots to sticks in its dealings with the private sector on cyber security. Voluntary co-developed or industry-developed standards are preferred to legislative approaches, noting the exceptions discussed earlier. An example of this is the iCode, a voluntary industry-designed code that encourages internet service providers to "inform, educate and protect their customers in relation to cyber security risks" (Communications Alliance Ltd. 2010, i).

## An Effective Model?

For an advanced country with a relatively small population, using the most efficient and effective model for cyber security is critical to managing the scale of cyber security threats. In this context, Australia's reluctance to form a centralized agency appears counterproductive. However, the limited statistics available from the government indicate that major cyber incidents affecting federal government agencies are declining in number (ACSC 2017). This could indicate that the current multi-agency approach is just as effective as centralization, with the additional benefit of avoiding the delays that restructuring and mergers entail. But the significant underengagement of the states/territories may be masking the true extent of malicious cyber security activity in Australia, and more information is required to assess the relative effectiveness of Australia's approach to this issue.

**Author's Note**

On July 18, 2017, the Australian government announced several changes to the governance of Australian intelligence agencies in response to the

[1] "#censusfail" is the now semi-official term for the cyber security incident that caused the 2016 Australian census website to be taken offline during the conduct of the 2016 census. While the actual cyber security incident, a relatively low-scale denial of service attack, was manageable, its misdiagnosis and a mismanaged response saw the eCensus website unavailable to the public for nearly two days. See Parliament of Australia (2016b, 53–55).

2017 *Independent Intelligence Review*. These changes will affect the governance of Australian cyber security policy and operations. This essay was written before this announcement was made and does not address or foreshadow these new arrangements.

## Works Cited

AGD. 2009. *Cyber Security Strategy*. Commonwealth of Australia. www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf.

———. 2017. *Telecommunications Sector Security Reforms*. www.ag.gov.au/telcosecurity.

ACSC. 2016. "2016 Threat Report." Canberra, Australia.

———. 2017. "2017 Threat Report." Canberra, Australia.

Communications Alliance Ltd. 2010. "Industry Code C650:2014 Internet Service Providers Voluntary Code of Practice for Industry Self-Regulation in the Area of Cyber Security." June.

COAG. 2016. "COAG meeting Communique." Council of Australian Governments press release, December 9. www.coag.gov.au/meeting-outcomes/coag-meeting-communiqu%C3%A9-9-december-2016.

Department of Defence. 2009. "Defending Australia in the Asia–Pacific Century: Force 2030." Department of Defence White Paper.

PM&C. 2011a. "Changes to the Ministry." Transcripts from the Prime Ministers of Australia press release, December 12. http://pmtranscripts.pmc.gov.au/release/transcript-18309.

———. 2011b. *Annual Report 2010-11*. Commonwealth of Australia, November 21. www.pmc.gov.au/resource-centre/pmc/department-prime-minister-and-cabinet-annual-report-2010-11.

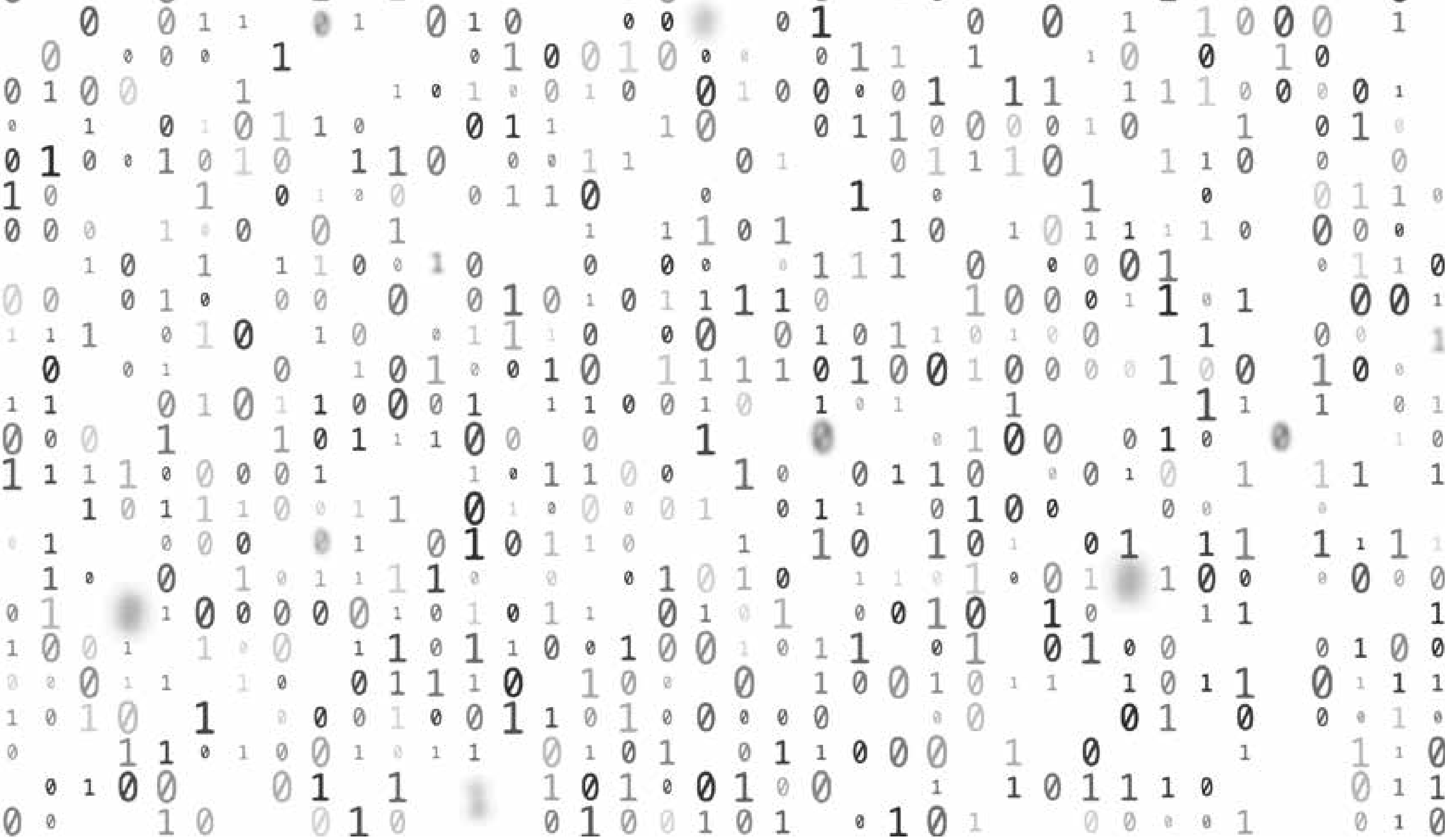
———. 2013. *Strong and Secure: A Strategy for Australia's National Security*. Commonwealth of Australia, January 23. http://apo.org.au/node/33996.

———. 2016. *Australia's Cyber Security Strategy*. Commonwealth of Australia, May.

———. 2017. *Australia's Cyber Security Strategy: 2017 Update*. Commonwealth of Australia, May.

Parliament of Australia. 2016a. *Privacy Amendment (Notifiable Data Breaches) Bill 2016*. February 22. www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r5747.

———. 2016b. *2016 Census: Issues of Trust*. Senate Economics References Committee, November.



# A Perspective on Cyber Security from the Canadian Nuclear Private Sector

Scott Hilts

Not long ago, cyber attacks were the domain of stereotypical individual hackers, such as Kevin Mitnick, who worked alone and caused little more than mischief (Coleman 2013). However, in recent years, cyber attacks have become more organized and, increasingly, are tools of powerful entities such as organized crime and nation-states. Even more alarming developments are the attacks targeting national critical infrastructures: industries that, whether operated by the government or the private sector, provide fundamental services such as electricity, telecom and transportation.

Most critical infrastructure industries still utilize information technology (IT) business computers for the front office, but their physical operations rely heavily on systems that manage "real-world" data and cause tangible, rapid physical responses. For example, a water treatment plant may have a system that monitors water flow and uses this information to automatically adjust a valve in response to changing conditions. This is referred to as an industrial control system (ICS), and en masse these systems perform countless mission-critical duties within critical infrastructure entities, from operating breakers that control the electrical grid to operating intravenous drips in hospitals.

ICSs typically lack even basic security protections or tools that are commonly used to secure IT business systems. For example, most ICSs have no available commercial anti-virus products that can be installed. ICSs are often more difficult to harden against attacks, and updating them can be costly in regulated industries due to qualification requirements. Furthermore, ICS manufacturers are only beginning to build systems with security features, thus much of the onus for securing ICS remains on the operator.

These security shortfalls, together with the value of critical infrastructure as targets, can make ICS attractive to cyber attackers. The first well-publicized cyber attack against an ICS occurred in 2000, when an individual hacker breached an Australian sewage treatment plant, resulting in the release of 800,000 litres of untreated sewage (Abrams and Weiss 2008). More recent cyber attacks against ICSs have moved from the realm of individual hackers into the domain of nation-state actors. For example, the 2010 Stuxnet ICS virus disrupted Iranian centrifuges, purportedly with the purpose of delaying Iranian uranium enrichment (Kushner 2013). In December 2015, hackers caused an electricity outage in Ukraine that affected some 230,000 customers on a cold December day (Lee, Assante and Conway 2016). It is not surprising that the Government of Canada is working at a policy level to protect critical infrastructure sectors from cyber attacks (Public Safety Canada 2016).

The development of a regulatory approach to protect ICSs in nuclear power plants in Canada is a unique case study in that, until recently, there was minimal international guidance or established best practices for policy makers to draw on. Furthermore, both government and private nuclear stakeholders had different, incomplete areas of expertise — there was no single group that had the breadth of knowledge and skills to develop comprehensive policy and guidance.

The Canadian federal government regulates the nuclear industry through the Canadian Nuclear Safety Commission (CNSC), whose mandate is established under the Canadian Nuclear Safety and Control Act. This mandate ensures that the health and safety of both people and the environment are protected in the production and use of nuclear energy and materials. It also ensures that Canada fulfills its international obligations, such as those under the Convention on the Physical Protection of Nuclear Material (International Atomic Energy Agency [IAEA] 1980). Nuclear operators share these health and safety obligations, but they have a critical additional requirement — the cost-effective, reliable generation of electricity to ensure a successful business. At first glance, it might seem that these business drivers could work against regulatory requirements, but nuclear operators are motivated to prioritize security. This motivation is driven by a number of factors: their professional and moral obligation to protect the public; the well-established axiom that “a safe plant is a productive plant;” and the importance of continued public trust and support for nuclear power.

The CNSC must be independent to fulfill its regulatory mandate, but it also works in a consultative manner with nuclear operators in areas such as guidance development. In ICS cyber security, where international and industry guidance was lacking and experts were few, this consultative approach was (and still is) particularly critical.

In 2013, the CNSC took a key step in its process of enhancing nuclear ICS cyber security requirements by initiating the development of a cyber security standard. It intentionally chose to develop those standards through the Canadian Standards Association (CSA) Group,[1] a Canadian not-for-profit standards organization. The CSA Group develops standards (including nuclear standards) through a consensus-based approach, with representation from government, industry and other stakeholders. The new cyber security standard was titled *CSA N290.7-14 Cyber Security for Nuclear Power Plants and Small Reactor Facilities*. The committee that drafted the standard included representation from Canadian nuclear operators, stakeholders in the nuclear supply chain, invited experts and the CNSC. For approximately two years, as the committee developed the standard, they also researched what best practices were available, consulted with experts in other countries and communicated with other international bodies.

At the conclusion of the draft stage, the standard was posted for public comment. During this phase, the standards committee notified a number of experts both nationally and internationally, many of whom gave detailed input based on their own ICS cyber security experience. These comments were reviewed and incorporated, and then the standard was formally released. The final step of the process occurred when the CNSC enacted changes through its nuclear-licensing framework, making the new standard mandatory for Canadian nuclear operators.

Beyond the security offered by implementing the standard itself, the consensus approach used in developing the standard created many added benefits. The multitude of discussions that occurred throughout the standard-development process, both in and out of meetings, resulted in a great deal of cross-pollination of ideas and expertise among the stakeholders. Members from different disciplines such as digital control engineering and IT security staff shared their respective approaches to solving the security problem and worked together to develop mutually beneficial solutions. Staff from different facilities and corporate cultures worked together, as did stakeholders who worked in different parts of the nuclear ICS life cycle. This information sharing improved the quality and applicability of the standard, but it also substantially elevated the expertise of all participants.

Throughout the development time, the working committee members also developed strong professional relationships, built on a foundation of increasing mutual respect and trust. This level of relationship took time to develop, but it proved critical in allowing a frank and open exchange of challenges, ideas and experience. This aspect of the committee was

[1] See www.csagroup.org/.

considered so valuable that the participants elected to continue meeting as a national working group once their standard mandate was complete. The meetings of this Cyber Security Peer Group (CSPG) are still held under the auspices of the Canada Deuterium Uranium (CANDU) Owners Group,[2] a not-for-profit organization that supports collaboration between designers and operators of CANDU reactors (the type of nuclear reactor used to generate electricity in Canada).

One challenge the CSPG faced was ensuring that the delicate balance between mandatory regulatory oversight and member consensus was maintained. Practical solutions to this included beginning each CSPG session with a non-regulatory "members only" component, in which they could discuss areas of mutual interest related to regulatory enforcement. After this in camera session ended, the CNSC was then invited to join the bulk of the meeting as a participating guest.

The CSPG working group's approach has drawn interest internationally, in particular from countries where ICS cyber security has been implemented unilaterally by a government regulator. Even in the United States, there have been cyber security tensions between the regulator and the implementing operators. The US Nuclear Regulatory Commission (NRC) developed regulation 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks," and then developed a comprehensive program example to illustrate how operators could comply with mandatory cyber security regulations, *Nuclear Regulatory Guide 5.71 Cyber Security Program for Nuclear Facilities* (NRC 2010). The NRC held public consultation, but US nuclear operators nonetheless became concerned around issues concerning the efficiency and scope of the regulation and the regulatory guide 5.71. In response, US nuclear operators developed their own compliance approach under the umbrella of the Nuclear Energy Institute (NEI) 08-09 Cyber Security Plan for Nuclear Power Reactors. The NEI has also petitioned the NRC for regulatory changes, based on its field experience with cyber security (Fertel 2015). The divergence between the NRC and the NEI has, at the very least, caused unnecessary duplication of effort.

When the CSPG started its work, international guidance and expertise was lacking, but both of these areas have improved over the past few years. There is an increasing body of international best practice, and a growing body of experts is emerging in the ICS security field. Contacts made through the standard development process have resulted in invitations to CSPG members to participate in a number of best-practice forums nationally and internationally. For example, CSPG members have been selected by the Canadian government to participate in cyber security guidance development and information exchanges through the IAEA. This participation is often alongside CNSC representatives, itself an uncommon approach as most countries only send government officials to IAEA consultancies.

The consensus-based approach to nuclear ICS cyber security used in Canada and, in particular, the ongoing input from the CSPG are examples of how government agencies, private operators, standards bodies and other stakeholders can collaborate on cyber security challenges that span sectors and jurisdictions.

## Works Cited

Abrams, Marshall D. and Joe Weiss. 2008. "Malicious Control System Cyber Security Attack Case Study — Maroochy Water Services, Australia." Paper presented at the Annual Computer Security Applications Conference, Anaheim, CA, December 11. www.acsac.org/2008/program/case-studies/Abrams.pdf.

Coleman, Timothy W. 2013. "Kevin Mitnick: The Hacking Hamburglar." *Forbes*, April 11. www.forbes.com/sites/singularity/2013/04/11/kevin-mitnick-the-hacking-hamburglar/#5740966a4ac9.

Fertel, Marvin S. 2015. Letter to NRC Chairman Stephen Burns on Cyber Security Event Notification Final Rule. NEI, January 15.

IAEA. 1980. "The Convention on the Physical Protection of Nuclear Material." May. www.iaea.org/sites/default/files/infcirc274r1.pdf.

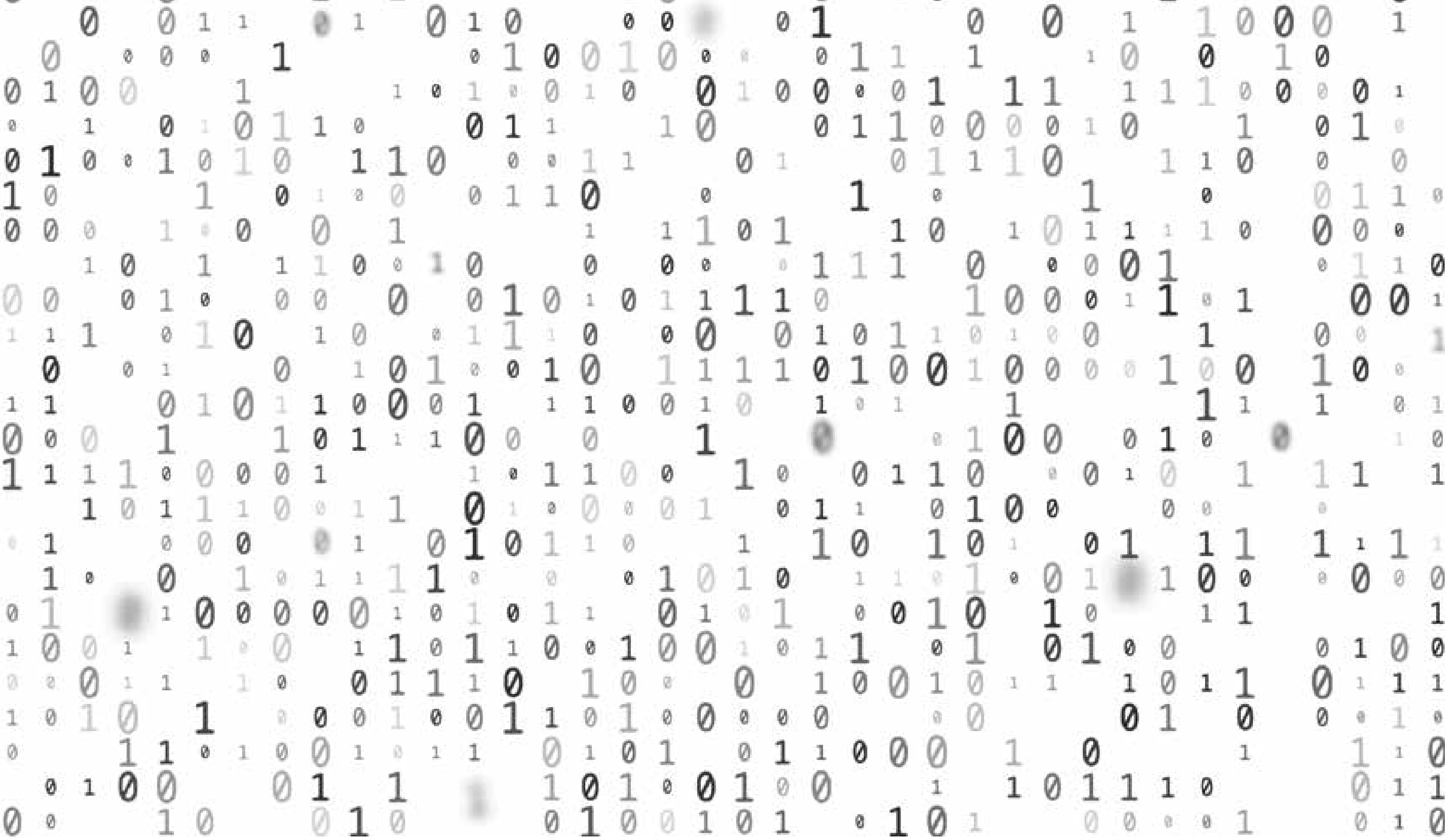
Kushner, David. 2013. "The Real Story of Stuxnet." IEEE Spectrum, February 26. http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

Lee, Robert M., Michael J. Assante and Tim Conway. 2016. "Analysis of the Cyber Attack on the Ukrainian Power Grid." The Electricity Information Sharing and Analysis Center (E-ISAC), March 18. www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.

NRC. 2010. *Nuclear Regulatory Guide 5.71 Cyber Security Program for Nuclear Facilities.* www.nrc.gov/docs/ML0903/ML090340159.pdf.

Public Safety Canada. 2016. "Fundamentals of Cyber Security for Canada's CI Community." Ottawa, ON: Public Safety Canada. www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-fndmntls-cybr-scrty-cmmnty/index-en.aspx.

[2] See www.candu.org/.



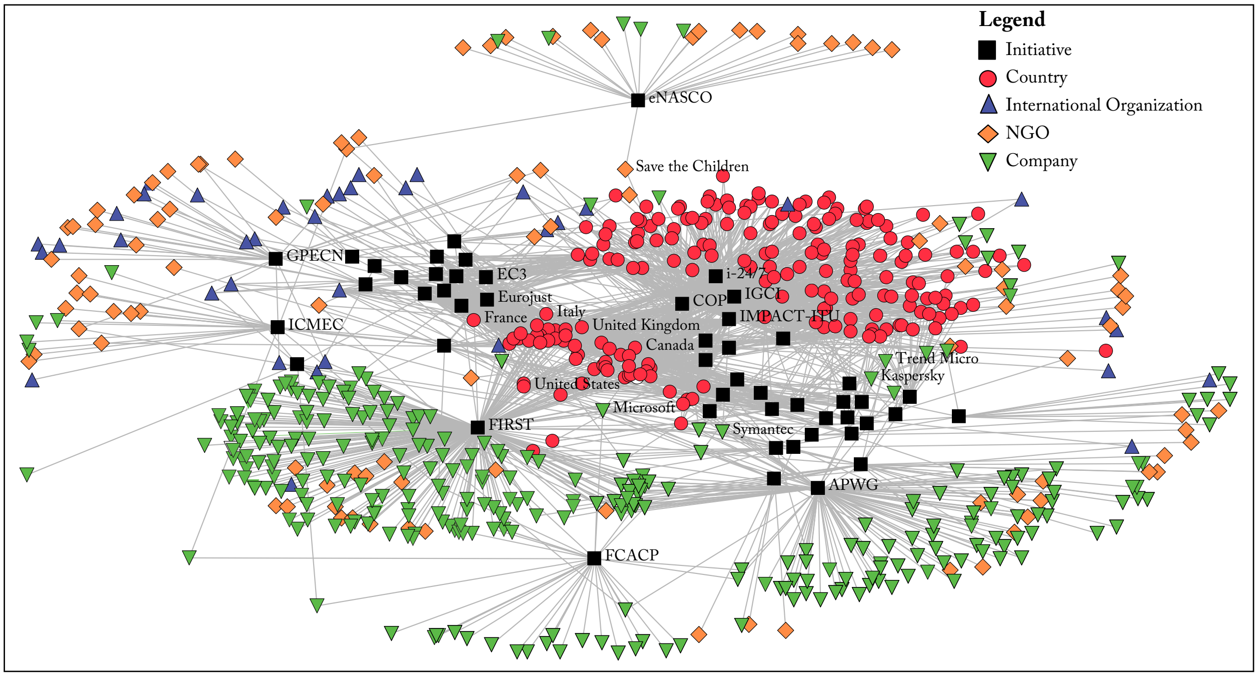
# Mapping the International Governance of Cybercrime

Benoît Dupont

One of the fundamental characteristics of cybercrime is its potentially transnational nature. However, the public and private institutions involved in its governance and the protection of “omni-national” victims seem to have a difficult time adapting to this global threat landscape, which blends local, national and international dimensions. Two arguments are often used to explain these institutions’ difficulties in adjusting to this complex interplay. The first stems from the technical and geographic complexity associated with cybercrime, while the second emphasizes the lack of harmonization in legislation created by different nations in their attempts to deal with this worldwide phenomenon, which has led to ineffective international coordination of police resources.

This less-than-optimal context has not prevented international police cooperation initiatives from proliferating, both in number and scope. A systematic review of existing forums reveals a web of flourishing links connecting a broad range of organizations. In order to systematically describe the features and structure of this international policing network (Dupont 2004), tools directly adapted from the Social Network Analysis (SNA) methodology are used to measure, visualize and analyze on a large scale how a diverse set of actors choose to cooperate with their peers. The international security network uncovered in this study has a polycentric structure that involves four main groups of organizational actors (national law enforcement and justice agencies, international organizations, private companies and non-governmental organizations [NGOs]) whose activities converge on anti-cybercrime initiatives ranging from capacity building and training to intelligence sharing and criminal investigations.

**Figure 1: The Network of International Police Cooperation Initiatives against Cybercrime (2014)**



*Acronyms*: APWG: Anti-Phishing Working Group; COP: Child Online Protection; EC3: European Cybercrime Centre; eNASCO: European NGO Alliance for Child Safety Online; FCACP: Financial Coalition Against Child Pornography; FIRST: Forum for Internet Response and Security Teams; G8 24/7: G8 — Sub-group on High-tech Crime Network of Contact Points; GPECN: Global Prosecutors E-Crime Network; IGCI: Interpol Global Complex for Innovation; ICMEC: International Centre for Missing & Exploited Children; IMPACT: International Multilateral Partnership Against Cyber Threats; ITU: International Telecommunication Union; I-24/7: Interpol's global police communications system.

*Source:* Author.

## The Plural International Network of Anti-Cybercrime Initiatives

Mapping the network of organizations that maintain formal cooperation links to fight cybercrime at the international level involves focusing on two distinct categories of nodes: organizational actors who attempt to reduce their exposure to online criminal risks and the cooperation initiatives they set up collectively to achieve this objective. The dataset includes 657 actors involved in 51 international and multi-lateral initiatives in the fight against cybercrime (Table 1). The data was collected in 2014, and Figure 1 represents the network as it existed then. It suggests that, contrary to what is often stated in the mainstream media, or even in some policy circles, there has been a proliferation of public and private initiatives that address the problem of online harms through a range of strategies, including capacity building (74.5 percent of the sample), information sharing (49 percent), regulatory and legal activities (37.2 percent), criminal investigations and intelligence collection (31.4 percent) and lobbying (9.8 percent).[1]

While most of these initiatives are led by international organizations or government agencies (63 percent), a significant number of them are the creation of NGOs (33 percent) or the private sector (12 percent).[2] This larger-than-expected contribution by non-state actors to the international governance of cybercrime is not entirely surprising, as it reflects the multi-stakeholder governance framework of the internet (Raymond and DeNardis 2015) and the fact that private interests overwhelmingly own and operate the infrastructure and services that enable the internet.

**Table 1: Types of Organizational Actors Participating in the 51 Anti-Cybercrime Initiatives**

| Type and Number of Actor | | Percentage |
|---|---|---|
| Country (national government agencies) | 204 | 31 |
| International organization | 38 | 6 |
| NGO or professional association | 103 | 16 |
| Corporation | 312 | 47 |
| **Total** | **657** | **100** |

*Source*: Author.

[1] The sum is greater than 100 percent as certain initiatives undertake different types of activities.

[2] Jointly led initiatives between NGOs and the private sector again explain why the total is more than 100 percent.

**Table 2: Organizational Actors and Initiatives Ranked According to Their Centrality Scores**

| Degree Centrality | | | | Closeness Centrality | | | | Betweenness Centrality | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Actor | Score | Initiative | Score | Actor | Score | Initiative | Score | Actor | Score | Initiative | Score |
| 1. UK | 0.49 | 1. FIRST | 0.39 | 1. Microsoft | 0.82 | 1. FIRST | 0.47 | 1. Microsoft | 0.062 | 1. FIRST | 0.484 |
| 2. Italy | 0.43 | 2. IMPACT (ITU) | 0.32 | 2. Switzerland | 0.80 | 2. COP (ITU) | 0.46 | 2. Save the Children | 0.057 | 2. APWG | 0.203 |
| 3. Canada | 0.41 | 3. COP (ITU) | 0.32 | 3. South Korea, Colombia, UAE | 0.79 | 3. IMPACT (ITU) | 0.43 | 3. Interpol | 0.033 | 3. COP (ITU) | 0.197 |
| 4. France | 0.41 | 4. IGCI | 0.31 | 4. Brazil, Azerbaijan | 0.78 | 4. I-24/7 (Interpol) | 0.42 | 4. Canada | 0.026 | 4. IMPACT (ITU) | 0.122 |
| 5. US | 0.41 | 5. I-24/7 | 0.30 | 5. Symantec, Telefonica | 0.77 | 5. IGCI | 0.41 | 5. Switzerland | 0.022 | 5. IGCI | 0.083 |
| 6. Germany | 0.39 | 6. APWG | 0.17 | 6. UK, Canada, Interpol, US | 0.76 | 6. APWG | 0.38 | 6. Symantec | 0.021 | 6. I-24/7 (Interpol) | 0.080 |
| 7. Netherlands | 0.39 | 7. Commonwealth Cybercrime Initiative | 0.11 | 7. Australia, Italy, Netherlands Romania, France | 0.75 | 7. Commonwealth Cybercrime Initiative | 0.38 | 7. US | 0.020 | 7. Financial Coalition Against Child Pornography | 0.060 |
| 8. Belgium | 0.37 | 8. Global Alliance Against Child Sexual Abuse | 0.08 | 8. Poland, Germany, Belgium (+13 European countries) | 0.74 | 8. EC3 (Europol) | 0.36 | 8. South Korea | 0.019 | 8. eNACSO | 0.059 |
| 41. China | 0.22 | 9. G8 24/7 | 0.08 | 9. Singapore, Malaysia, India, Japan | 0.73 | 9. Global Project on Cybercrime | 0.36 | 59. China | 0.004 | 9. Commonwealth Cybercrime Initiative | 0.048 |
| 148. Russia | 0.18 | 10. EC3 (Europol) | 0.07 | 10. China, Russia | 0.72 | 10. Virtual Global Task Force | 0.36 | 66. Russia | 0.003 | 10. Global Prosecutors E-Crime Network | 0.044 |

*Note*: Actors and initiatives are listed in descending order and are preceded by their rank number. The three types of centrality scores are normalized, meaning that their raw centrality scores are divided by the maximum scores possible. This operation is performed using UCINET software (Borgatti and Everett 1997; Borgatti, Everett and Freeman 2002).

*Acronyms*: APWG: Anti-Phishing Working Group; COP: Child Online Protection; EC3: European Cybercrime Centre; eNASCO: European NGO Alliance for Child Safety Online; FIRST: Forum for Internet Response and Security Teams; G8 24/7: G8 — Sub-group on High-tech Crime Network of Contact Points; IGCI: Interpol Global Complex for Innovation; IMPACT: International Multilateral Partnership Against Cyber Threats; ITU: International Telecommunication Union; I-24/7: Interpol's global police communications system; UAE: United Arab Emirates.

*Source*: Author.

Three basic network metrics are mobilized and shown in Table 2. The "degree centrality" metric measures the cumulative number of initiatives in which organizational actors participate (Borgatti and Everett 1997). "Closeness centrality" measures how close an organizational actor is to all others in the network, taking into account not only direct ties but also mapping indirect ties (and their length) to all other actors in the network. It is therefore a better reflection of the relative position of an organizational actor within the whole network. Finally, "betweenness centrality" measures the unique capacity of an organizational actor to broker connections between network members that lack other options for connecting (Wasserman and Faust 1994). More concretely, closeness and betweenness centrality can be used to assess how effective information-sharing and capacity-building strategies are at helping central stakeholders empower less-skilled jurisdictions.

## National Governmental Institutions

The international anti-cybercrime network comprises 204 countries. The United States, despite its major political and economic influence over the internet, does not play the most pivotal role in this network. This lack of multi-lateral leadership may result from the United States' preference for bilateral cooperation with a small group of trusted countries. It is interesting to note that great and middle powers such as the United Kingdom, Italy, Canada, France, Germany or the Netherlands occupy the top ranks for the degree centrality metric. That the United Kingdom is in first position can be explained by the diversity of its international commitments to former colonies (through the Commonwealth), its four intelligence allies (in the Five Eyes alliance) and various European law enforcement and justice institutions. Similarly, Canada's relatively high ranking on degree centrality derives from its participation in Commonwealth, Inter-American and Asian initiatives. It is worthwhile to note that Canada also displays the most diversified linkage profile. China and Russia, which are often accused of being the source of a disproportionate share of online risks in the digital ecosystem, find themselves relegated to ranks that do not reflect their actual technological and economic capacities.

## International Organizations

International organizations, such as Interpol, which represent six percent of network members, play a critical role in the development and deployment of international anti-cybercrime initiatives. Regional organizations such as Europol have also developed discrete capacity-building, intelligence-sharing and operational initiatives in an effort to support their membership. One dimension that certainly deserves closer scrutiny is the implicit rivalry between certain international organizations, which leads to a duplication of coordination capacities. The most obvious example is the two high-profile centres of expertise opened by the International Telecommunications Union and Interpol in Asia.

A recent development in anti-cybercrime initiatives led by international organizations has been the growing use of private companies from the information technology (IT) sector to provide additional expertise and intelligence. Interpol for example has signed memorandums of understanding with NEC Corporation, Kaspersky, Trend Micro, Cellebrite and Barclays Bank to share tools and criminal intelligence, effectively embedding them in its network. Europol has followed a similar strategy. The prominent role played by companies in these initiatives highlights the changing international police governance landscape, where governments and international organizations have to find new and creative ways to leverage the private sector without being captured by it. These new arrangements sometimes also raise lawful access and privacy concerns that have not yet been solved.

## Companies

A number of large multinational corporations, such as Microsoft and Symantec, are playing a major role in the coordination of global anti-cybercrime initiatives. Microsoft provides the most striking example of the impact a company with vast resources and a determination to tackle cybercrime can have on international police cooperation. Microsoft is using its global footprint and its substantial financial resources to support 13 of the 51 initiatives analyzed here, effectively making it the top organizational actor for closeness centrality and betweenness centrality, ahead of national government agencies and international organizations. Far from limiting itself to capacity-building activities, in 2010, Microsoft initiated an ambitious botnet takedown program. Leveraging extensive intelligence-gathering capacities, the company and its law enforcement and private sector allies dismantled nine botnets, demonstrating how the private sector could become a catalyst for large-scale anti-cybercrime operations and mobilize technical, analytical and legal resources that far exceed what most countries have available, but also showing the technical and legal limits of this approach when conducted unilaterally (Dupont 2017). The private sector has also been instrumental in developing initiatives that have become key players in the coordination of an international response to computer security incidents (through FIRST, the Forum for Incident Response and Security Teams) and online banking fraud (through APWG, the Anti-Phishing Working Group).

## NGOs and Professional Associations

Massive involvement by the private sector is unsurprising, given that it owns and operates the technological infrastructures and services affected by various digital risks, but the position held by professional associations and NGOs in this global network warrants explanation. Two groups of actors are particularly active: professional associations of police investigators, prosecutors, judges and information security experts; and NGOs defending children's rights against online abuse and sexual exploitation. The role of these NGOs on the international stage is not well known, despite the fact that at least 13 of the 51 initiatives (25 percent) analyzed in this study address child protection and rely on strategic alliances forged with multinational telecommunication companies, the banking sector and international organizations to fight online child pornography. These NGOs thus seem to wield considerable influence. Professional associations such as the International Association of Prosecutors or the International Bar Association are interested in participating in international forums that promote the harmonization of practices conducive to more effective transnational investigations. If NGOs act more as moral entrepreneurs, professional associations can be seen as norm producers within this network (Scherrer 2009).

## Conclusion

For the last quarter of a century, the evolution of criminal activity triggered by the advent of the internet has precipitated a major reconfiguration of social control institutions, which now operate as a network. This essay has attempted to shed some light on the structural properties of these new polycentric arrangements in the international governance of cybercrime. The global cooperation network examined in this essay is composed of collaborative archipelagos that remain very fragmented: NGOs focused on fighting child pornography and sexual exploitation have few links to the large companies that are most concerned with online fraud and data breaches, in the same way European, Asian or Latin American actors prefer associating with local initiatives, where the limited number and more familiar behaviour of participants are more conducive to consensus building. The network changes constantly, and has undoubtedly added new nodes and initiatives since the data was collected in 2014. The next steps are to track its effectiveness, to learn from its successes and fix its shortcomings, to assess how those investments provide value and to focus on the most promising initiatives that are based on sound scientific evidence. A pressing need will be its potential to contribute to the prevention and control of advanced cybercrime operations involving sophisticated malware and ransomware that exploit leaked cyberweapons and vulnerabilities. The cyber physical threats associated with the Internet of Things should also become a major concern, but will involve a new set of industry and critical infrastructure stakeholders. Beyond policing cooperation, which will remain a major challenge, this global network will hence need to scale the linkages described in this essay to enhance the digital resilience of our connected world.

## Works Cited

Borgatti, Stephen B. and Martin G. Everett. 1997. "Network Analysis of 2-mode Data." *Social Networks* 19 (3): 243–69.

Borgatti, Stephen B., Martin G. Everett and Linton C. Freeman. 2002. *UCINET for Windows: Software for Social Network Analysis*. Harvard, MA: Analytic Technologies.

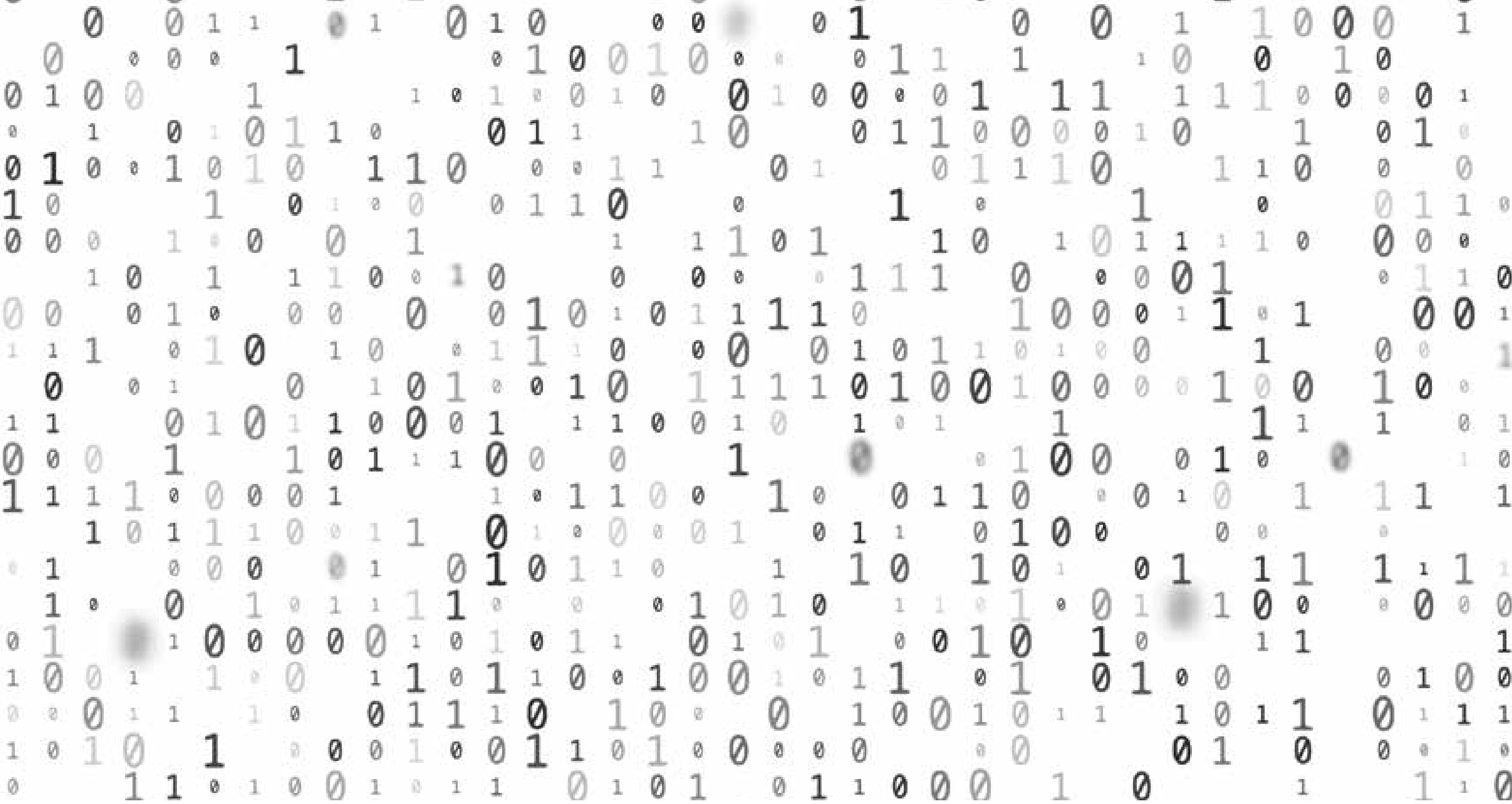
Dupont, Benoît. 2004. "Security in the Age of Networks." *Policing and Society* 14 (1): 76–91.

———. 2017. "Bots, Cops, and Corporations: On the Limits of Enforcement and the Promise of Polycentric Regulation as a Way to Control Large-Scale Cybercrime." *Crime, Law and Social Change* 67 (1): 97–116.

Raymond, Mark and Laura DeNardis. 2015. "Multistakeholderism: Anatomy of an Inchoate Global Institution." *International Theory* 7 (3): 572–616.

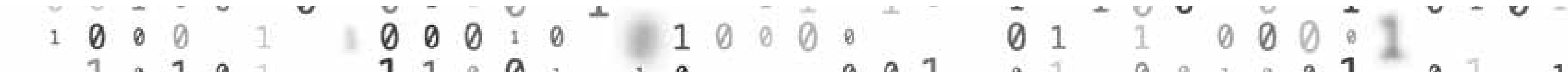
Scherrer, Amandine. 2009. *G8 against Transnational Organized Crime*. Farnham, UK: Ashgate.

Wasserman, Stanley and Katherine Faust. 1994. *Social Network Analysis: Methods and Applications*. Cambridge, UK: Cambridge University Press.



# Cyber Scaffolding: Proposing a National Organization to Support the Canadian Economy and Public Safety

Timothy Grayson and Brian O'Higgins



Rarely does a nation have the chance to enhance its national security, ascend the innovation ladder and increase its economic fortunes at once. Historically, wars have that effect. While well short of war, the cyber battlespace presents just such an opportunity for Canada. Taking advantage of this rare possibility will require a thoughtful, coherent campaign that includes the government.

Whether for public safety or economic development, governments are at a disadvantage in cyber security and need trustable, independent help, aligned to the national interest. The number of second-order impacts demand the best counsel possible.

This essay presents a proposal to raise the probability for maximizing the value to Canada that can be derived from cyber security.

## The Dangerous Life Cycle of Innovation

To understand the cyber security opportunity one must accept that humans often get to the right place only after having suffered choosing the wrong way. Innovation promises the right place; the life cycle of threat inherent in innovation invariably tracks the wrong way. This typical path is the result of (sometimes willful) blindness to risk and second-order effects. Great expectations and trivialized threats play out in the free market until government intercedes. For example, cars were fun and dangerous until governments imposed safety regulations. Similar stories abound for the food and water supply and the environment, among many other things, that required society to encourage the best of innovation and hold back the worst.[1] Crystallizing the wisdom of an informed citizenry rather than instituting the purchased wishes of the economically powerful is, of course, what governments do in their best moments.

For society, there is inevitable pain as the market sorts winners from losers. Ignorant consumers (citizens) want more for less, and some corporate "innovators" use that to effectively externalize costs and risks. This mix favours organizations. In circumstances of information asymmetry and high risk, such as the digital domain, government should be more active.

The incentives of capitalist democracy align with a number of socio-psychological imperatives to systematize and accelerate progress. The casualties of progress have always been legion. Somebody has to be first — and first is dangerous. The danger comes not from the unknown, but from the unsaid. Here is where government, representing society at large, can weigh broad reward and risk using the nuanced calculus of the overall greater good (safety, economy, and so on) rather than the crude arithmetic of return on capital.

Unfortunately, while the plodding pace of government is valuable for avoiding mistakes, the digital environment evolves rapidly and governments lack the specialized cyber security "business" knowledge to intelligently match the speed of change. Government easily ends up addressing yesterday's problems. Yet, even without the skill or capacity to actively participate in this (or any) evolving commercial domain, government has the responsibility to set the field to benefit Canada at large.

## The Cyber World Is the Real World

Our world turns on digital technologies. The stuff of science fiction a mere three decades ago is now woven into the fabric of everyday life. Local and global economies, national infrastructures and so much more are digitally dependent in banal and critical ways from "social" to online banking and "sharing" to education. Even more valuable is how digital technologies maximize the efficiencies of global supply chains, including interbank operations. Meanwhile, rushing at us from the horizon are truly radical changes afforded by the Internet of Things and artificial intelligence, such as self-driving cars and smart cities.

But the benefits are accompanied by risks, putting innovation in the cyber domain at a dangerous nexus. Petty and even organized cybercrime is giving way to the weaponization of cyber space. Around the world, the need to protect cyber structures from persistently evolving threats is driving equally aggressive development of cyber security. The estimated global market for cyber security is in the order of US$1 trillion over the next five years.[2] Businesses everywhere, supported by their governments, are chasing this opportunity.

For Canada, a nation aching for innovation and economic drivers for this century, cyber security must be a top option. With the domestic and global growth rate for cyber security exceeding that of the broad economy by an order of magnitude, Canada can build upon existing capability. Many Canadian firms and researchers have captured global attention for challenges from public key infrastructure to quantum cryptography to digital identity. And right now, the opportunity to take the lead globally based on our talents and ingenuity is augmented by the Edward Snowden- and Donald Trump-fired suspicions of Americans with technology.

## Intervention for Economic Acceleration

The economic opportunity presented by global cyber security will be captured by someone, somewhere. It is too big with too long a lifespan not to be pursued. Canadian businesses are well-positioned to chase this market. But, with so many fierce competitors, they need help.

Globally, governments are actively supporting their commercial cyber security sectors. One valuable type of initiative — pursued in the United Kingdom, the United States, Israel and elsewhere — is government-shepherded cyber security (super) clusters. These groups enable development and rapid scaling of world-class players in both obvious and subtle ways, from outright investment support and direct procurement through to selling support via the nation's network of trade missionaries and so forth. A cyber security (super)cluster pushes researchers and businesses to and over the tipping point where success breeds success. Clustering businesses and research organizations, with financial support and cooperative guidance, ensures effort is magnified for everyone's greater benefit instead of competing for individual smaller benefits.

Cyber security (super) clusters are an example of governments using a breadth of resources not to make a market, but rather to harmonize its private sector to exploit the market. Money alone helps, as does support for education, primary and commercial research and

[1] We have seen this unfold recently in growth industries (Facebook and other social media), disruptive innovators such as Uber and even long-settled industries and companies such as Equifax and Maple Leaf Foods that push forward with innovations at the cost of citizen consumers' privacy and even physical safety.

[2] Cyber security is unsettled, making consensus estimates of market composition and size fluid to say the least. One trillion dollars over the next five years seems to be a relatively safe bet according to a variety of reputable sources and relied-upon sources of cyber security insight that would include Cybersecurity Ventures, Gartner, Forrester and the major cyber security consulting firms.

commercial sales. But in the global cyber security marketplace, a nation's private sector and academic research, development and commercial players together with government must operate as a team against other nations. A team's coach marshalls the best of the team and coordinates the players' individual talents into a strategic thrust. All but a few enormous, mature private sector organizations can pretend to match any state's international reach. To the extent that the same government can prime its cyber security sector as a buyer, so much the better. But that is decidedly secondary.

Regulating cyber safety, by which we suggest a minimum standard for cyber security directed toward organizations and the providers' cyber systems, will serve public safety as well as propagate a market for innovative cyber security solutions. Supporting Canadian commercial efforts by prioritising the purchase of cyber security products of Canadian-owned and headquartered companies would then provide critical sales scaffolding for Canadian cyber security businesses to secure crucial foreign sales.[3]

Most of all, the governance of cyber security innovation and development shapes the commercial vigour of small and large businesses in order to maximize national investment in this market opportunity. That does not mean government picking individual winners. It means government doing what its name implies: governing. Regulating, framing, scaffolding and otherwise harnessing Canada's entrepreneurial vitality for the national good is simply what governments ought to do.

## A Proposal: The National Institutes of Cyber-Security

Achieving the complementary goals of public safety and national economic development is the government's responsibility, but in cyber security, despite noble efforts in various parts of the world, government typically does not have the depth of expertise and currency in the field to support the public policy choices.[4] While there is support from the private sector and academia, each is insufficiently aligned to the complex societal goals that government must navigate. These entities, irrespective of where they are located, are not typically interested in the long-term game of the nation as a whole; their loyalties are to shorter and narrower private considerations.

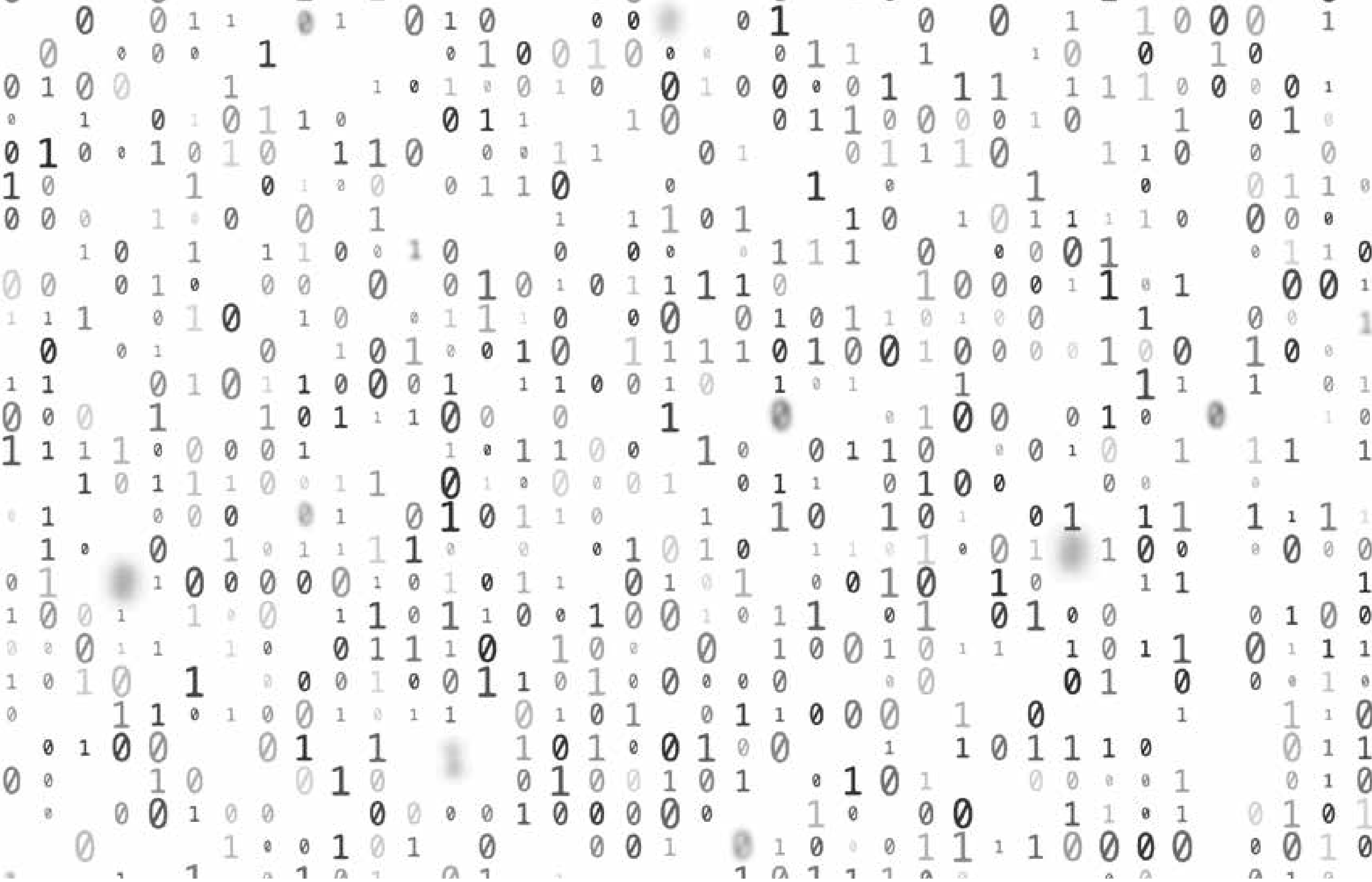
To harness the pockets of cyber security excellence in Canada, and to facilitate innovation, policy and practice, we propose the establishment of an independent, non-governmental organization loyal to the welfare of the nation: the National Institutes of Cyber-Security (NICS). An organization that could act on behalf of the government to assemble and coordinate the very best of Canadian cyber security innovation, policy and practice.

The NICS would be, first and foremost, a home for a broad array of cyber security expertise in technology, commercial strategy, policy and regulatory development. This talent would provide independent and unbiased guidance for long-term decision making and development of cyber security policy or regulation across the economy and throughout Canadian society. The NICS would provide strategic leadership of Canada's centres of cyber excellence to maximize public investment effectiveness and economic value. This way, Canada's clusters of cyber security innovation and development from Moncton to Calgary are more likely to thrive and succeed as a unified force. The power of numbers and the strength of scale comes when these several clusters and the hundreds of commercial and academic institutions they represent act in coordination. With financial support from the Canadian government, their success becomes a national success.

The role of coordinator and facilitator of strategic direction cannot be underestimated in a fast-moving, fast-growing economic space such as cyber security. For Canada as a nation to benefit most broadly from this public safety and economic development opportunity, the government must play a role. This could be most effectively realized with the intellectual counsel and leadership of the proposed NICS.

[3] Admittedly, any kind of "Buy Canadian" position could raise tensions with trading partners. But if there were ever a domain that qualified for a national security basis for excluding non-domestic vendors, cyber security is it.

[4] There is an argument that government should not deplete its precious resources to develop such specific and constantly evolving expertise, but rather rely upon cyber security experts, whose business it is to remain at the cutting edge.



# Conclusion

## Christian Leuprecht and Josh Tupler

The widespread use of the internet and other network-based systems in personal, professional and governmental contexts is creating myriad vulnerabilities that are constantly exploited by foreign, domestic and non-state adversaries. But as personal information and critical infrastructure become ever more prone to attack, domestic governance issues of cyber security have received short shrift in policy discussions. Now that cyber has matured as a security domain in its own right, this deficiency is of particular concern in federal systems, where the division of powers between jurisdictions makes governance all the more complex.

This special report is meant to provide an initial impetus toward filling a gap in the literature on domestic cyber security governance issues in the Canadian federal context in particular, and also by drawing on comparative experience from the United States and Australia and across federations more generally. From the vantage point of intergovernmental relations and multi-level government, this series of essays gauges a number of the security challenges across the cyber domain, the key stakeholders that need to be included for governance to be effective, some of the issues they confront and proposals for addressing these challenges. The authors represent a spectrum of diverse stakeholders from the academic, business, legal and policy-making communities. However, neither the individual essays nor the volume as a whole have any pretense of being comprehensive. Instead, the aim is to stimulate a conversation about pressing governance issues as cyber security risks proliferate.

The contributors to this report have critically assessed the approaches to cyber security and domestic governance taken by Canada and select allies. They observed an ad hoc style of regulation preoccupied with countering network threats and information-security operations. Canada's current approach is federal, multi-stakeholder and international. Its laws are supplemented by a bewildering array of sector-based regulators, private corporations and organizations that coordinate federal, provincial, territorial, local, Aboriginal and non-state actors and initiatives. This approach both benefits from and, to a large extent, depends on private sector initiatives at the federal and international levels, and on international cooperation between state and non-state actors. How changes to the national security legislation that has been tabled in Parliament (as of this writing) will affect these interactions remains to be seen.

By virtue of the constitutional division of powers into federal and provincial jurisdictions, the governance of the provision of cyber security in Canada — and in comparable federal systems with constitutionally distinct levels of government such as the United States and Australia — raises a host of policy-making challenges, including:

→ vertical collective action problems among federal, provincial or local governments;

→ horizontal coordination issues across provincial and local levels of government; and

→ multi-level governance dimensions between the private sector and civil society.

Governance issues are marked by significant information asymmetries, where a disproportionate amount of intelligence and capacity resides with the federal government, quasi-governmental actors (such as the Bank of Canada) and a few large private sector companies (such as financial institutions). Yet provincial and local governments, civil society organizations and small and medium-sized enterprises are no less vulnerable or important to a secure cyber security ecosystem. They are also disproportionately subject to mounting asymmetries in resources, technology and skills to defend against nefarious adversaries who, with relatively primitive skill sets and resourcing, can inflict excessive financial and reputational damage. This asymmetric information problem is compounded when federal recommendations are overtaken — or superseded — by mandatory or privately funded changes at other levels of government.

Improving governance outcomes across the cyber domain in Canada will, at least partially, depend on ensuring decision-making structures work better for all actors in light of the aforementioned information asymmetries. Options range from implementing alternative governance models to improving Canada's existing policy-development infrastructure. By way of example, this special report broaches prospects for a principles-based framework, as well as Australia's strategy of co-locating agencies to harness the benefits of a single-agency approach based on multilayered partnerships with sub-federal governments and non-governmental actors.

More time and research is needed to gauge the efficacy of alternative approaches to overcoming the collective-action problems that intergovernmental relations and multi-level governance raise and their relevance to the Canadian context. Still, the contributions to this report illuminate some preliminary lessons for policy makers:

→ Acknowledge the collective action problems raised by multi-level governance and coordination. Greater awareness of information asymmetries among federal, provincial and local institutions and impediments to long-term strategic investment in cyber security should contribute to a more informed policy discourse and concerted approach.

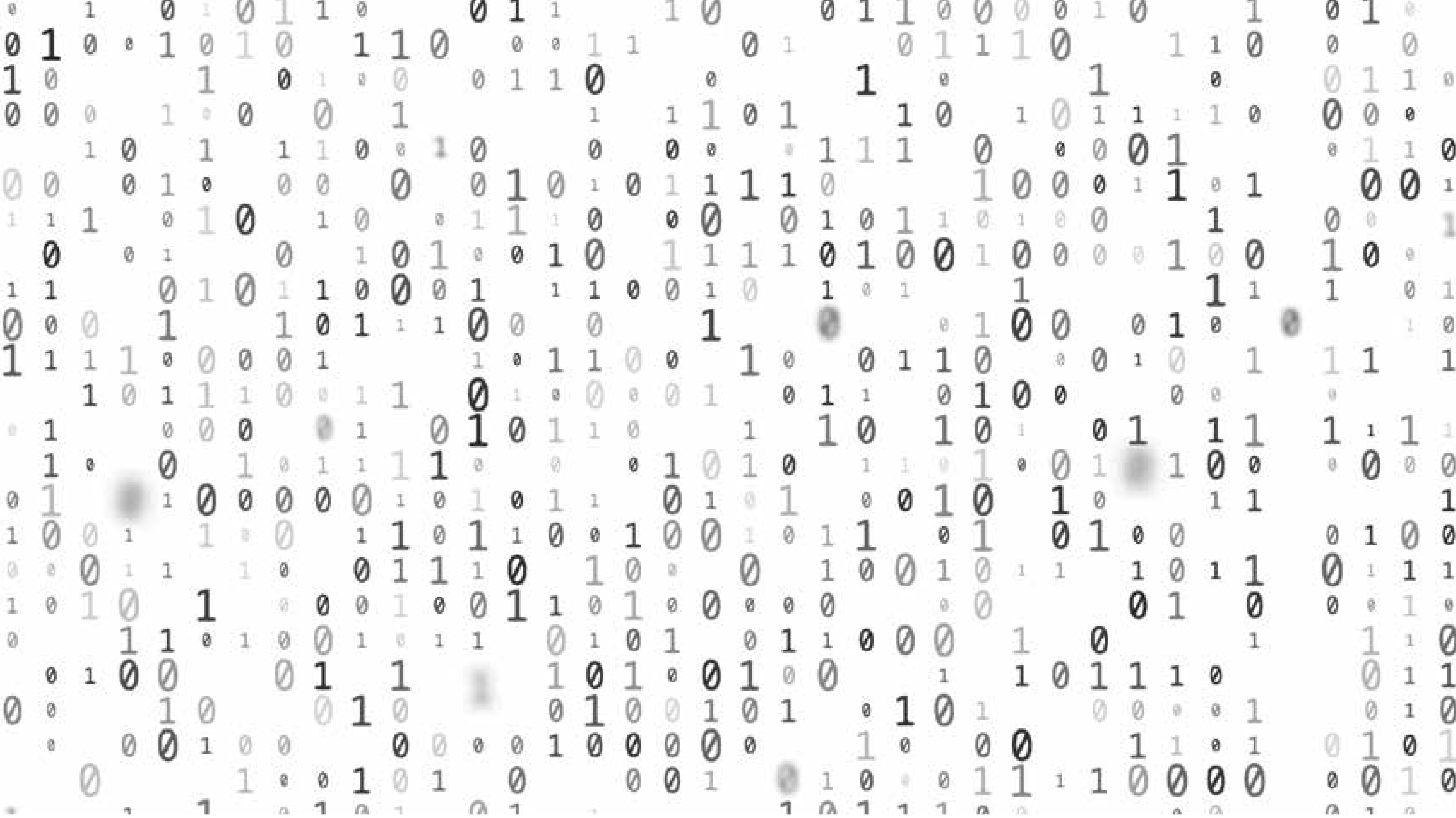
→ Recognize that the expertise and innovation required to keep pace with ever-changing cyber threats will likely be industry-driven, augmented by government support and economic incentives. The cyber threat environment is evolving far more rapidly than government's ability to keep up with policy innovation. New governance approaches are bound to emerge as federations strive to narrow the gap between an evolving threat environment and policy responses.

→ Develop a comprehensive framework for strategic governance, investment and execution. By more clearly delineating responsibilities across levels of government, and by defining less ambiguous roles for the private sector to collaborate with government, governments can better harness the potential for innovation in cyber security and thrive in a safer and more resilient digital economy.

→ Encourage public-private cooperation and development of non-governmental organizations — such as the proposed National Institutes of Cyber-Security — to facilitate dialogue and promote best practices for cyber security, including in the area of governance.

→ Adopt best governance practices for securing critical infrastructure systems across industrial sectors that have been leading by example. The development of an approach to protecting industrial control systems in nuclear power plants offers an example for developing a comprehensive and consensus-based approach to secure infrastructure systems in a domain where failure is not an option.

Countries' prosperity and global competitiveness increasingly hinge on an approach to governance that appreciates cyber security and innovation as corollaries: a cyber ecosystem that encourages investments in research and development yet protects the financial gains and intellectual property that result. In the process, intergovernmental relations and multi-level governance are rapidly emerging as key enablers.



# Contributors

Brent J. Arnold is a partner practising in Gowling WLG's advocacy department. Brent heads the firm's commercial litigation technology sub-group and is a member of its innovation council. Brent's experience includes cyber risk, and consumer, implementation and other disputes for e-commerce vendors and software developers. He has appeared before all levels of court in Ontario, including the Supreme Court of Canada. Brent serves on the executive for the Civil Litigation Section of the Ontario Bar Association and is an active member of the Advocates' Society. He has also served as adjunct faculty at York University, where he taught advanced business law in the School of Administrative Studies. Brent currently serves on the Cybersecurity and Data Privacy Committee of the US-based DRI — The Voice of the Defense Bar.

Benoît Dupont is professor of criminology at the Université de Montréal, where he also holds the Canada Research Chair in Cybersecurity. He is the scientific director of the Smart Cybersecurity Network (SERENE-RISC), one of Canada's Networks of Centres of Excellence. Benoît's research interests include the co-evolution of technology and crime, as well as the polycentric governance of security.

Timothy Grayson is an enterprise transformation consultant and writer with domain expertise in digital identity and cyber security who lives near Ottawa, Canada. Tim is the president of Institute X, which provides both advisory/consulting and policy research focusing on structural impacts of digital transformation of business and society. His cyber security edu-novel is available at http://amzn.to/1Hg9xMv. Find Tim at tim@institute-x.org.

Scott Hilts is the information security manager at Bruce Power, an eight-unit nuclear power facility in Ontario, Canada. He has worked in the cyber security field for over a decade, prior to which he was the director of a secure custody facility for young offenders. Scott chaired the committee that developed the Canadian CSA N290.7 Standard, Cyber Security for Nuclear Power Plants and Small Reactor Facilities, and is the former chair of the Canadian Industry Cyber Security Integration Team. He has also provided input to numerous International Atomic Energy Agency cyber security consultancies and technical meetings, serving as the chair on several occasions. Scott was also a member of the Nuclear Industry Summit 2016 Cyber Security Working Group.

Christian Leuprecht is Matthew Flinders Fellow at Flinders University of South Australia and Class of 1965 Professor in Leadership at the Royal Military College (RMC) in Kingston, Ontario. A recipient of the RMC's Cowan Prize for Excellence in Research, Christian was elected a member of the New College of the Royal Society of Canada in 2016. He is president of the International Sociological Association's Research Committee 01: Armed Forces and Conflict Resolution. Christian is a senior fellow at the Macdonald-Laurier Institute and cross-appointed to the Department of Political Studies and the School of Policy Studies at Queen's University, where he is also a fellow of the Institute of Intergovernmental Relations and the Queen's Centre for International and Defence Policy. An expert on security and defence, political demography, and comparative federalism and multi-level governance, he is regularly called as an expert witness to testify before committees of Parliament.

Stephanie MacLellan joined the Global Security & Politics Program in July 2016, and specializes in internet governance and cyber security. She spent more than a decade working as an editor and reporter for newspapers such as the *Toronto Star*, *The Hamilton Spectator* and *The Slovak Spectator*, an English-language weekly based in Bratislava, Slovakia. Her work has been nominated for three National Newspaper Awards. She holds a bachelor of journalism degree from Carleton University and a master's degree in global affairs from the Munk School of Global Affairs.

David Mussington is a senior fellow at the Centre for International Governance Innovation (CIGI), and professor of the practice and director, Center for Public Policy and Private Enterprise, University of Maryland, College Park. In 2010, David was senior adviser for cyber policy in the US Department of Defense, later serving on the Obama administration's National Security Council staff as director for surface transportation security policy. In addition to his work at the University of Maryland, David is an adjunct member of the research staff at the Institute for Defense Analyses, directing studies for the Department of Defense, the Department of Homeland Security and the Office of the Director of National Intelligence. He holds a B.A. in economics and political science and an M.A. in political science, both from the University of Toronto, and a Ph.D. in political science from Carleton University, as well as the Certified Information Systems Security Professional designation.

Liam Nevill is the principal analyst in the Australian Strategic Policy Institute's (ASPI's) International Cyber Policy Centre (ICPC), researching and writing on international and domestic cyber policy issues. Liam has published on issues including deterrence in cyberspace, Australian Army cyber modernization and digital trade in the Asia-Pacific and provided commentary on cyber issues for Australian news outlets. Liam leads the development of the ICPC's flagship annual report *Cyber Maturity in the Asia Pacific Region*, which assesses the whole-of-nation approach of 25 Asia-Pacific regional countries to cyber issues. Before joining ASPI in 2015, Liam worked at the Australian Department of Defence on strategic and international defence policy issues. Liam holds an M.A. in strategy and security from the University of New South Wales (Canberra) and a B.A. in history, politics and international relations from the University of New South Wales (Sydney).

Brian O'Higgins is a technology entrepreneur who lives in Ottawa, Canada. He is best known for introducing public key infrastructure to the cyber security landscape and as the co-founder of Entrust and Third Brigade. Currently, he assists start-up companies by serving as a board or advisory board member.

Josh Tupler is currently a Yenching Scholar at Peking University, a Young Ambassador at the Carnegie-Tsinghua Center and a fellow at the Centre for International and Defence Policy at Queen's University. He graduated from Dartmouth College and spent the year after graduating serving as a Fulbright Scholar at the Centre for International and Defence Policy researching Canada-US relations, challenges in conventional and nuclear deterrence, Canadian and American cyber security policy. His current research principally focuses on nuclear security challenges and US-China relations.

# About CIGI

We are the Centre for International Governance Innovation: an independent, non-partisan think tank with an objective and uniquely global perspective. Our research, opinions and public voice make a difference in today's world by bringing clarity and innovative thinking to global policy making. By working across disciplines and in partnership with the best peers and experts, we are the benchmark for influential research and trusted analysis.

Our research programs focus on governance of the global economy, global security and politics, and international law in collaboration with a range of strategic partners and support from the Government of Canada, the Government of Ontario, as well as founder Jim Balsillie.

# À propos du CIGI

Au Centre pour l'innovation dans la gouvernance internationale (CIGI), nous formons un groupe de réflexion indépendant et non partisan qui formule des points de vue objectifs dont la portée est notamment mondiale. Nos recherches, nos avis et l'opinion publique ont des effets réels sur le monde d'aujourd'hui en apportant autant de la clarté qu'une réflexion novatrice dans l'élaboration des politiques à l'échelle internationale. En raison des travaux accomplis en collaboration et en partenariat avec des pairs et des spécialistes interdisciplinaires des plus compétents, nous sommes devenus une référence grâce à l'influence de nos recherches et à la fiabilité de nos analyses.

Nos programmes de recherche ont trait à la gouvernance dans les domaines suivants : l'économie mondiale, la sécurité et les politiques mondiales, et le droit international, et nous les exécutons avec la collaboration de nombreux partenaires stratégiques et le soutien des gouvernements du Canada et de l'Ontario ainsi que du fondateur du CIGI, Jim Balsillie.

Centre for International
Governance Innovation
67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org