SECURING NORTH AMERICAN CRITICAL INFRASTRUCTURE: A COMPARATIVE CASE STUDY IN CYBERSECURITY REGULATION

Scott J. Shackelford, JD, PhD* & Zachery Bohm**

ABSTRACT

The United States and Canada are interdependent along a number of dimensions, including the two nations' mutual reliance on shared critical infrastructure. As a result, regulatory efforts aimed at securing critical infrastructure in one nation impact the other, including in the cybersecurity context. This Article explores one such innovation in the form of the 2014 National Institute for Standards and Technology ("NIST") Cybersecurity Framework. We briefly review the evolution of the NIST Framework, comparing and contrasting it with ongoing Canadian efforts to secure vulnerable critical infrastructure against cyber threats as a vehicle to discover North American governance trends that could impact wider debates about the appropriate role of the public and private sectors in enhancing cybersecurity.

TABLE OF CONTENTS

INTRODUCTION

Neither the United States nor Canada are strangers to cyber attacks that have increasingly targeted both the private and public sectors to, among other things, steal valuable intellectual property including both state and trade secrets. To take just one example, the Canadian government reported a major cyber attack in 2011 that forced the Finance Department and Treasury Board, Canada's main economic agencies, to disconnect from the Internet.[1] Hundreds of systems within the U.S. Department of Commerce have similarly been forced offline due to cyber attacks in recent years.[2] In total, more than 40 million global cyber attacks were reported by one survey in 2014, representing a nearly fifty percent increase over 2013.[3]

In response to this wave of cyber attacks, the U.S. and Canadian governments have created a number of national and bilateral initiatives to enhance North American cybersecurity, such as the 2012 Cybersecurity Action Plan Between Public Safety Canada and the Department of Homeland Security.[4] Such actions are in response to the fact that the U.S. and Canada are interdependent along a number of dimensions, including the two nations' mutual reliance on shared critical infrastructure. For example, in 2012, electricity exports from Canada totaled nearly sixty million megawatt-hours, or roughly one-to-two percent of total U.S. consumption, though certain regions such as the U.S. northeast and Midwest are particularly dependent upon Canadian power supplies.[5] As a result of this interdependence, regulatory efforts aimed at security critical infrastructure in one nation impact the other, including in the cybersecurity

* Assistant Professor of Business Law and Ethics, Indiana University; Senior Fellow, Indiana University Center for Applied Cybersecurity Research; W. Glenn Campbell and Rita Ricardo-Campbell National Fellow, Stanford University Hoover Institution.

** Senior, Indiana University School of Public and Environmental Affairs.

[1] *Significant Cyber Incidents Since 2006*, CSIS, http://csis.org/files/publication/131010_Significant_Cyber_Incidents_Since_2006_0.pdf (last visited Feb. 3, 2014).

[2] *See* Gregg Keizer, *Chinese Hackers Hit Commerce Department*, INFO. WK. (Oct. 6, 2006), https://www.google.com/calendar/render??tab=mc&pli=1#g,

[3] *See* Samantha White, *Global Cyber-Attacks Up 48% in 2014*, CGMA (Oct. 8, 2014). http://www.cgma.org/Magazine/News/Pages/201411089.aspx?TestCookiesEnabled=redirect. However, such surveys should not be taken as gospel. *See, e.g.*, Peter Maass & Megha Rajagopalan, *Ask NSA Director Keith Alexander: Does Cybercrime Really Cost $1 Trillion?*, PROPUBLICA (Aug. 1, 2012,), http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion.

[4] *See generally* CYBERSECURITY ACTION PLAN BETWEEN PUBLIC SAFETY CANADA AND THE DEPARTMENT OF HOMELAND SECURITY (2012), http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cybrscrt-ctn-plan/cybrscrt-ctn-plan-eng.pdf.

[5] *See* U.S. Energy & Commerce Comm., North American Energy Infrastructure Act Will Bolster U.S.–Canada Electricity Relationship (May 7, 2014), http://energycommerce.house.gov/press-release/north-american-energy-infrastructure-act-will-bolster-us%E2%80%93canada-electricity#sthash.VKtC9JA1.dpuf.

context.

This Article explores one such innovation in the form of the 2014 National Institute for Standards and Technology Cybersecurity Framework ("NIST Framework").[6] We briefly review the evolution of the NIST Framework, comparing and contrasting it with ongoing Canadian efforts to secure vulnerable critical infrastructure against cyber threats as a vehicle to discover North American governance trends that could impact wider debates about the appropriate role of the public and private sectors in enhancing critical infrastructure cybersecurity.

The Article proceeds as follows. Part I unpacks the multifaceted cyber threat facing North American critical infrastructure operators. Part II then delves at regulatory efforts aimed at enhancing U.S. critical infrastructure cybersecurity focusing on the NIST Framework. Finally, Part III investigates Canadian critical infrastructure regulation with a special emphasis on that government's reception to the NIST Framework. We conclude by couching this investigation within the wider debates surrounding international critical infrastructure protection including the emergence of cybersecurity norms in this space.

I. UNPACKING THE CYBER THREAT IMPACTING NORTH AMERICAN CRITICAL INFRASTRUCTURE

It is notoriously difficult to find verifiable data on the number, type, and severity of cyber attacks afflicting various nations and regions around the world.[7] Without clear definitions, shared and meaningful values, or reliable data, information about cyber attacks impacting North American critical infrastructure remains limited and unsophisticated. That being said, more than one-third of Canadian firms have reported being the victim of cyber attacks according to one 2014 survey,[8] while according to Kaspersky Labs as of March 2015 Canada is the number ten

[6] *See* WHITE HOUSE PRESS SEC'Y, EXECUTIVE ORDER ON IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (Feb. 12, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0; Mark Clayton, *Why Obama's Executive Order on Cybersecurity Doesn't Satisfy Most Experts*, CHRISTIAN SCI. MONITOR, Feb. 13, 2013, *available at* http://www.csmonitor.com/USA/Politics/2013/0213/Why-Obama-s-executive-order-on-cybersecurity-doesn-t-satisfy-most-experts.

[7] For more on why this is the case, see Chapter 5 of SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS: IN SEARCH OF CYBER PEACE (2014).

[8] *See* David Paddon, *Cyber Attacks Have Hit 36 Per Cent of Canadian Businesses, Study Says*, Globe & Mail (Aug. 18, 2014), http://www.theglobeandmail.com/report-on-business/cyber-attacks-have-hit-36-per-cent-of-canadian-businesses-study-says/article20096066/.

most attacked nation in the world.[9] In contrast, Kaspersky notes that the United States is the number three most attacked nation as of March 2015,[10] while from 2000 to 2008, U.S. cybersecurity surveys found that the proportion of organizations reporting cyber attacks ranged from forty-three to seventy percent.[11] Globally, according to a 2010 Symantec report, seventy-five percent of surveyed IT executives in twenty-seven countries stated that they had detected one or more attacks, and forty-one percent characterized such attacks as "somewhat/highly effective."[12] Verizon's 2012 Data Breach Investigations Report found that "174 million records were compromised in 2011, the second-highest total since the company began tracking breaches in 2004."[13] Even that figure was surpassed in 2013.[14]

Yet despite this multifaceted and growing threat, audits from the Canadian government itself have noted the absence of "action plans [that] have hindered progress[,]" the slow pace of private-sector critical infrastructure partnership building, and that "[m]onitoring the cyber threat environment [to critical infrastructure] has not been complete or timely."[15] What is more, a 2012 report from the Auditor General of Canada noted that the Canadian government had appropriated only some $780 million in funding to improve security for Canada's critical infrastructure, but that far less that this total was directed toward enhancing cybersecurity.[16] Other data points support the need for reform. As noted by the Canadian Security Intelligence Service:

> The speed of evolving new cyber threats, the lack of geographic boundaries and the problem of determining attribution impede efforts to counter attacks on information systems. Obstacles include not only domestic jurisdictional barriers to effective regulation, legislation and information-sharing but also the fragmented ownership and regulatory control of ICT infrastructure, which represents a major challenge at the global level . . . Accordingly, it would seem appropriate that the costs of protecting critical infrastructure against certain threats to national security

[9] *See* Kaspersky, Cyberthreat Real-Time Map, http://cybermap.kaspersky.com/ (last visited Mar. 10, 2015).
[10] *See id*.
[11] *See* Robert Richardson, *CSI Computer Crime & Security Survey*, CSI at 13 (2008), http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf.
[12] STATE OF ENTERPRISE SECURITY STUDY, SYMANTEC, at 7 (2010), http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=sesreport2010.
[13] Joel Griffin, *Report Sheds Light on Intellectual Property Theft*, SEC. INFOWATCH (Oct. 24, 2012), http://www.securityinfowatch.com/article/10819280/report-sheds-light-on-intellectual-property-theft.
[14] *See* Hadley Malcolm, *Target: Data Stolen From Up to 70 Million Customers*, USA TODAY (Jan. 10, 2014), http://www.usatoday.com/story/money/business/2014/01/10/target-customers-data-breach/4404467/.
[15] 2012 Fall Report of the Auditor General of Canada, http://www.oag-bvg.gc.ca/internet/English/parl_oag_201210_03_e_37347.html (last visited Mar. 10, 2015).
[16] CAN. SEC. INTELLIGENCE SERV., ASSESSING CYBER THREATS TO CANADIAN INFRASTRUCTURE, https://www.csis.gc.ca/pblctns/ccsnlpprs/20121001_ccsnlpprs-en.php (last visited Mar. 10, 2015).

> be borne in a proportionate manner by all those who benefit . . . .[17]

However, Canada is far from alone in struggling to meet the evolving cyber threat to critical infrastructure. In the United States, for example, according to a McAfee report, U.S. "Critical infrastructure owners and operators report that their networks and control systems are under repeated cyberattack, often by high-level adversaries [such as foreign governments]."[18] The consequences of such attacks are potentially devastating. For example, a report by the U.S. Cyber Consequences Unit estimates losses from a major attack on U.S. critical infrastructure at roughly $700 billion.[19] Yet Congress has been slow to meet this challenge, promoting executive action. As such, we next turn to the U.S. approach to changing the unsustainable cybersecurity status quo followed by a comparative look at some of Canada's critical infrastructure cybersecurity reform efforts.

II. U.S. APPROACHES TO SECURING CRITICAL INFRASTRUCTURE: ENTER THE NIST FRAMEWORK

President Obama issued an executive order in 2013 that, among other things, expanded public-private information sharing and tasked the National Institute for Standards and Technology with establishing the NIST Framework to better secure critical infrastructure.[20] The Framework version 1.0, *Framework for Improving Critical Infrastructure Cybersecurity*, was released in February 2014,[21] and is designed to harmonize consensus standards and industry best practices to provide, its proponents argue, a flexible and cost-effective approach to enhancing cybersecurity.[22] Although the Framework does not create any binding obligations for private sector actors and has no means of enforcement for those that choose to adopt it, its widespread

[17] *Id.*

[18] IN THE CROSSFIRE: CRITICAL INFRASTRUCTURE IN THE AGE OF CYBER WAR, MCAFEE/CSIS 1 (2009), http://iom.invensys.com/EN/pdfLibrary/McAfee/WP_McAfee_In_The_Crossfire_03-10.pdf.

[19] *See* JAYSON M. SPADE, INFORMATION AS POWER: CHINA'S CYBER POWER AND AMERICA'S NATIONAL SECURITY 26 (Jeffrey L. Caton ed., 2012) (citing Eugene Habiger, *Cyberwarfare and Cyberterrorism: The Need for a New U.S. Strategic Approach*, CYBER SECURE INST., Feb. 1, 2010, at 15–17).

[20] *See* WHITE HOUSE PRESS SEC'Y, EXECUTIVE ORDER ON IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (Feb. 12, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0; Mark Clayton, *Why Obama's Executive Order on Cybersecurity Doesn't Satisfy Most Experts*, CHRISTIAN SCI. MONITOR, Feb. 13, 2013, *available at* http://www.csmonitor.com/USA/Politics/2013/0213/Why-Obama-s-executive-order-on-cybersecurity-doesn-t-satisfy-most-experts.

[21] NIST FRAMEWORK, *supra* note 6, at 1.

[22] *Improving Critical Infrastructure Cybersecurity*, 78 Fed. Reg. at 11,741.

uptake may well be in the process of establishing a cybersecurity standard of care in the United States even without Congressional action.[23] This holds the potential to spill over beyond traditional CI sectors to the private sector writ large in the United States and perhaps, as we will see, further afield. The White House has announced that as of February 2015, for example, the likes of Intel, Apple, and Walgreens are incorporating the NIST Framework into their cybersecurity efforts, while Bank of America is also requiring its use by vendors.[24]

With a deep degree of private-sector participation, the NIST Framework's basic structure divides cybersecurity into five broad "functions:" identify, protect, detect, respond, and recover.[25] Perhaps most importantly, the Framework provides a series of steps for organizations to follow to assess and address their cyber risk exposure, permitting firms to incorporate cyber risk management in a manner that is consistent with their overarching business goals and financial capabilities. Although it is too early to tell the staying power of the NIST Framework, the flexibility inherent in the Framework has proven attractive to critical infrastructure operators and policymakers alike. Already private-sector clients, for example, are receiving the advice that if their "cybersecurity practices were ever questioned during litigation or a regulatory investigation, the 'standard' for 'due diligence' was now the NIST Cybersecurity Framework."[26] Over time, the NIST Framework not only has the potential to shape a standard of care for domestic critical infrastructure organizations but also could help to harmonize global cybersecurity best practices for the private sector writ large given active NIST collaborations with a number of nations including the United Kingdom, Japan, Korea, Estonia, Israel, Germany, and Australia.[27] The question we turn to is what impact, if any, this initiative is having on reshaping Canada's cybersecurity policymaking landscape.

[23] *See e.g.*, *NIST's Voluntary Cybersecurity Framework May Be Regarded as De Facto Mandatory*, HOMELAND SEC. NEWS WIRE (Mar. 4, 2014), http://www.homelandsecuritynewswire.com/dr20140303-nist-s-voluntary-cybersecurity-framework-may-be-regarded-as-de-facto-mandatory (stating that experts have warned that many of the recommendations in the framework "may be used by courts, regulators, and even consumers to hold institutions accountable for failures that could have been prevented if the cybersecurity framework had been fully implemented by the respective institution.").

[24] *See* White Hosue, White House Summit on Cybersecurity and Consumer Protection, http://m.whitehouse.gov/the-press-office/2015/02/13/fact-sheet-white-house-summit-cybersecurity-and-consumer-protection (last visited Mar. 19, 2015).

[25] NIST FRAMEWORK, *supra* note 6,, at 7.

[26] *Why the NIST Cybersecurity Framework Isn't Really Voluntary*, INFO. SEC. BLOG (Feb. 25, 2014), http://www.pivotpointsecurity.com/risky-business/nist-cybersecurity-framework.

[27] For example, some stakeholders have already argued that "any time a company's cybersecurity practices are questioned during a regulatory investigation and litigation, the baseline for what's considered commercially reasonable is likely to become the . . . Cybersecurity Framework." Gerald Ferguson, *NIST Cybersecurity*

III. AN INTRODUCTION TO CANADIAN CRITICAL INFRASTRUCTURE CYBERSECURITY POLICY LAW AND POLICY

The Canadian government has taken a variety of approaches to establish cybersecurity frameworks aimed at managing the array of cyber threats facing North American critical infrastructure. First though, before diving into this issue it is helpful to have some context. Canada and the United States are similar in the relatively large number of sometimes overlapping agencies responsible for various aspects of enhancing national cybersecurity. Much of Canada's cybersecurity policymaking authority resides in the Department of Public Safety and Emergency Preparedness Canada ("PSEPC"),[28] which has been referred to as the Canadian version of the U.S. Department of Homeland Security. As with DHS, PSEPC is responsible for ensuring the cyber security of civilian government networks and private industry networks related to critical infrastructure.[29]

In 2005 the government created the Canadian Cyber Incident Response Center ("CCIRC") within PSEPC.[30] The CCIRC was created to help monitor the cybersecurity of both public- and private sector networks including critical infrastructure. In this role, CCIRC is responsible for leading the government's response to and recovery from cyber attacks on critical cyber assets.[31] The CCIRC does this by advising government agencies and private companies on how to prepare for and mitigate cyber threats, providing technical expertise such as forensic cyber analysis, and by helping to share and enhance collaboration among experts in support of critical Canadian cyber infrastructure.[32] The CCIRC is Canada's version of the U.S. Computer Emergency Readiness Team ("US-CERT"), which was established in 2003 under the jurisdiction

Framework: Don't Underestimate It, INFO. WK. (Dec. 9, 2013), http://www.informationweek.com/government/cybersecurity/nist-cybersecurity-framework-dont-underestimate-it/d/d-id/1112978; Update on the Cybersecurity Framework, NIST 4 (July 31, 2014), http://nist.gov/cyberframework/upload/NIST-Cybersecurity-Framework-update-073114.pdf ("NIST and other US government officials have had discussions about the Framework with multiple foreign governments and regional representatives including organizations throughout the world, including – but not limited to – the United Kingdom (UK), Japan, Korea, Estonia, Israel, Germany, and Australia.").

[28] *See Generally* Cyber Security: A Shared Responsibility (2012) http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/index-eng.aspx

[29] *See* U.S. DEP'T HOMELAND SEC., SAFEGUARD AND SECURE CYBERSPACE (2012), http://www.dhs.gov/safeguard-and-secure-cyberspace

[30] *See* Steven Ballew, *U.S. Can Learn from Canadian Cybersecurity Shortcomings*, DAILY SIGNAL (Nov. 5 2012), http://dailysignal.com/2012/11/05/u-s-can-learn-from-canadian-cybersecurity-shortcomings/

[31] *See id*.

[32] *See What CCIRC Does*, (2014), http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-eng.aspx.

of the U.S. Department of Homeland Security.[33] Both of these organizations provide their civilian governments and private sectors with the tools and information they need to be able to mitigate the effects of cyber attacks, and also work together on identifying and sharing cybersecurity best practices and threat information.[34]

In February 2014, the Canadian government announced the Cyber Security Cooperation Program ("CSCP"), which is administered by PSEPC. The CSCP was launched as a five year, $1.5 million grant initiative developed to fund research and projects to improve Canada's "vital cyber systems" security.[35] The CSCP is tasked with accomplishing this goal by identifying programs and research that improves best practices, standards, operational methodologies, and cyber assessment tools for critical cyber systems and infrastructure.[36]

Over the past decade PSEPC has published numerous reports related to critical infrastructure cybersecurity. These reports detail what the Canadian government and private sector should do to improve the cybersecurity of critical infrastructure and how these ideas should be implemented. In 2010, for example, PSEPC published a National Strategy for Critical Infrastructure report and an Action Plan for Critical Infrastructure report, both of which were developed to address vital infrastructure safety and security issues.[37] The National Strategy outlines ten areas of critical infrastructure that are vulnerable to cyber attacks and addresses how risks related to these areas of critical infrastructure should be mitigated (as compared to sixteen critical infrastructure sectors designated by the U.S. DHS).[38] The report rationalizes that ultimately the responsibility of securing critical infrastructure rests in the hands of the local

[33] *See* 44 U.S.C. § 3546 (Federal Information Security Incident Center).

[34] *See* CYBER INCIDENT RESPONSE CENTRe (CCIRC) Partners, (2015), http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-prtnrs-eng.aspx.

[35] *See* CYBER SECURITY COOPERATION PROGRAM, http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/cprtn-prgrm/index-eng.aspx.

[36] *See* RESEARCH THEMES (2015), http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/cprtn-prgrm/rsrch-thms-eng.aspx.

[37] *See* CRITICAL INFRASTRUCTURE (2014), http://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-eng.aspx.

[38] NATIONAL STRATEGY FOR CRITICAL INFRASTRUCTURE 2 (2010), http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf (listing energy and utilities, finance, food, transportation, government, information and communication technology, health, water, safety, and manufacturing). *See also What is Critical Infrastructure*, DHS, http://www.dhs.gov/what-critical-infrastructure (last visited Jan. 16, 2014); *What is the ICS-CERT Mission?*, http://ics-cert.us-cert.gov/Frequently-Asked-Questions (last visited Jan. 17, 2014) (The U.S. Cyber Emergency Response Team, which is part of DHS, identifies sixteen critical infrastructure sectors consistent with Homeland Security Presidential Directive 7, including: agriculture, banking and finance, chemical, commercial facilities, dams, defense industrial base, drinking water and water treatment systems, emergency systems, energy, government facilities, information technology, nuclear systems, public health and healthcare, telecommunications, and transportation systems).

owners and operators. Based on this notion, the report describes a framework for how the government plans on sharing important information and addressing challenges faced by local operators and owners of diverse critical infrastructure assets.

The PSEPC also published a report entitled Canada's Cyber Security Strategy in 2010, which described the three main objectives of Canadian national cybersecurity strategy: securing government systems, working with the private sector to ensure nongovernment systems are secure, and helping the Canadian public browse the Internet safely.[39] Subsequently, in 2013 the government published Action Plan 2010 – 2015 for Canada's Cyber Security in order to help flesh out the cybersecurity strategy report. Specifically, the Action Plan details what actions should be undertaken by different stakeholders to achieve identified cybersecurity goals.[40] The Action Plan for Critical Infrastructure was recently updated to reflect vital infrastructure protection for the years 2014–2017. This new Critical Infrastructure Action Plan focuses on how cybersecurity has become an increasingly important aspect of critical infrastructure protection, and as such it focuses on how to implement policies developed by the national cyber and critical infrastructure strategy reports.[41] In particular, the Plan calls for improving public-private partnerships, assessing critical infrastructure risks more effectively, and strengthening critical infrastructure resilience.[42]

Many objectives in the updated Action Plan are similar to those pursued by the authors of the NIST Framework. One such objective is the focus on identifying areas of high cyber risk and working on ways to mitigate that risk.[43] In addition, both the Action Plan and the NIST Framework place a great deal of emphasis on fostering increased communication between the stakeholders of vital cyber infrastructure. While the NIST Framework does not outline which stakeholders are responsible for individual activities related to cybersecurity, it does provide information on how to organize and categorize various activities related to ensuring cybersecurity.[44] Indeed, the NIST Framework has enjoyed the attention of Canadian

[39] CANADA CYBER SECURITY STRATEGY 7 (2010), http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf.

[40] ACTION PLAN 2010 – 2015 FOR CANADA'S CYBER SECURITY STRATEGY 3–4 (2010), http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/ctn-pln-cbr-scrt-eng.pdf.

[41] ACTION PLAN FOR CRITICAL INFRASTRUCTURE 2014 – 2017 at 3–4 (2014), https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pln-crtcl-nfrstrctr-2014-17/pln-crtcl-nfrstrctr-2014-17-eng.pdf.

[42] *See id*.

[43] *Id*. at 7–8.

[44] NIST FRAMEWORK, *supra* note 6,, at 19.

policymakers, as it has with an array of North American industry associations,[45] representing energy, IT, manufacturing, retailing, and other sectors.[46] This process is now playing out beyond North America's borders. For example, industry association Information Technology Industry Council ("ITI") explained that it has recently visited Japan and South Korea, sharing with both countries' governments and business leaders "the benefits of a public-private partnership-based approach to developing globally workable cybersecurity policies."[47] Moreover, "ITI highlighted the [F]ramework as an example of an effective policy developed in this manner, reflecting global standards and industry-driven practices."[48] Time will tell whether this model of a "voluntary" bottom-up cybersecurity framework will effectively meet the multifaceted cyber threat, but given the evolving problem and reluctance by U.S. and Canadian lawmakers to pass binding measures it may well represent the best option available. As such, the U.S. and Canadian public- and private-sectors should collaborate to expand on the 2012 U.S.-Canadian Cybersecurity Action Plan to include cross-border and cross-sector information sharing along with active engagement on updating the NIST Framework beginning with Version 2.0. Without such bilateral buy in, progress made in one nation will still leave the other open to cyber attacks, which in some cases perhaps may have been prevented.

CONCLUSION

In a special report on North America, the Council on Foreign Relations has stated of the interconnection between the North American economies that: "Cyber failures in one country could have ripple effects on neighbors and cross-border production . . . The Task Force recommends that the United States, Canada, and Mexico set baseline standards for cyber protection."[49] The NIST Framework is certainly one candidate for such an undertaking, but it is not alone. There are certainly other cybersecurity frameworks worth pursuing. For example, the CFR Task Force recommended the promulgation of joint cybersecurity frameworks drawn from

[45] *See, e.g.*, *New US Cybersecurity Framework Developed by NIST Features COBIT 5 in the Core*, *supra* note 275.

[46] Ann M. Beauchesne, *Administration Sends cybersecurity Stakeholders a Positive Message: The NIST Framework Should be Voluntary, Flexible, and Collaborative*, U.S. CHAMBER OF COMMERCE (June 11, 2014), https://www.uschamber.com/administration-sends-cybersecurity-stakeholders-positive-message-nist-framework-should-be-voluntary.

[47] *Id.*

[48] *Id.*

[49] NORTH AMERICA: TIME FOR A NEW FOCUS 80 (Council on Foreign Relations, Independent Task Force Rep. No. 71, 2015).

the Critical Security Controls and the U.S. DHS Continuous Diagnostics and Mitigation Program to promote “cyber hygiene.”[50] Moreover, the CFR Report recommended several of the measures discussed in this Article, including deeper integration of national CERTs as well as robust international public-private information sharing. Indeed, these conclusions build from the *U.S.-Canadian Cybersecurity Action Plan*, which, among other things, deepens cooperation between U.S. and Canadian cyber emergency response teams, calls for more robust private-sector information sharing, and better “public awareness” of the multifaceted cyber threat.[51] Over time, such efforts may morph into a combined North American CERT and Information Sharing and Analysis Organization. By leveraging the resources available in the U.S. and Canada, both nations may be able to more effectively meet the evolving cyber threat more effectively than has been the case to date, and in the process help secure North American critical infrastructure and contribute to some measure of a global cyber peace.

[50] *Id*.

[51] *U.S.-Canadian Cybersecurity Action Plan*, *supra* note 4, at 2–4.