SCHOOL OF LAW
CASE WESTERN RESERVE
UNIVERSITY

Canada-United States Law Journal

Volume 40 | Issue 1

Article 9

2016

Securing Critical North American Infrastructure: A Comparatice Case Study in Cybersecurity Regulation

Scott J. Shackelford

Zachery Bohm

Recommended Citation

Scott J. Shackelford and Zachery Bohm, *Securing Critical North American Infrastructure: A Comparatice Case Study in Cybersecurity Regulation*, 40 Can.-U.S. L.J. 61 (2016)
Available at: http://scholarlycommons.law.case.edu/cuslj/vol40/iss1/9

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

Scott J. Shackelford, J.D., Ph.D. & Zachery Bohm***

ABSTRACT: The United States and Canada are interdependent along a number of dimensions, such as their 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. It reviews the evolution of the NIST Framework, comparing and contrasting it with ongoing Canadian efforts to secure vulnerable critical infrastructure against cyber threats. Its purpose is 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

I. Introduction 61
II. Unpacking the Cyber Threat Affecting North American Critical Infrastructure 63
III. U.S. Approaches to Securing Critical Infrastructure: Enter the NIST Framework 65
IV. An Introduction to Canadian Critical Infrastructure Cybersecurity Law and Policy 66
V. Conclusion 69

I. INTRODUCTION

Neither the United States nor Canada is a stranger to cyber attacks. These have increasingly targeted both the private and public sectors to steal valuable intellectual property, such as state and trade secrets. In one instance, 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 United States

* 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.

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 in 2014, representing a nearly 50% 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 cyber security. This includes the 2012 Cybersecurity Action Plan Between Public Safety Canada and the Department of Homeland Security.[4] Such collaborative actions reflect the fact that the United States and Canada are interdependent along a number of dimensions, including the two nations' mutual reliance on shared critical infrastructure ("CI"). For example, in 2012, electricity exports from Canada to the United States totaled nearly 60 million megawatt-hours, or roughly 1% to 2% of total U.S. consumption. 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 CI in one nation impact the other, even in the cybersecurity context.

This article explores one such innovation, the 2014 National Institute for Standards and Technology Cybersecurity Framework ("NIST Framework").[6] It briefly reviews the evolution of the NIST Framework, comparing and contrasting it with ongoing Canadian efforts to secure vulnerable CI against cyber threats. Its purpose is to discover North American governance trends that may impact wider debates about the appropriate role of the public and private sectors in enhancing CI for cyber security.

The article proceeds as follows. Part I unpacks the multifaceted cyber threat facing North American CI operators. Part II then delves into regulatory efforts

[1] CTR FOR STRATEGIC & INT'L STUDIES, SIGNIFICANT CYBER INCIDENTS SINCE 2006 (Mar. 10, 2014), http://csis.org/files/publication/140310_Significant_Cyber_Incidents_Since_2006.pdf.

[2] *See* Gregg Keizer, *Chinese Hackers Hit Commerce Department*, INFO. WK. (Oct. 6, 2006), http://www.informationweek.com/chinese-hackers-hit-commerce-department/d/d-id/1047684.

[3] *See* Samantha White, *Global Cyber-Attacks Up 48% in 2014*, CGMA MAGAZINE (Oct. 8, 2014), http://www.cgma.org/Magazine/News/Pages/201411089.aspx?TestCookiesEnabled=redirect. *But see, e.g.*, Peter Maass & Megha Rajagopalan, *Does Cybercrime Really Cost $1 Trillion?*, PROPUBLICA (Aug. 1, 2012), http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion (noting that such surveys should be accepted with caution).

[4] *See generally* PUB. SAFETY CAN. AND U.S. DEP'T. OF HOMELAND SEC., 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 North American Energy Infrastructure Act Will Bolster U.S.–Canada Electricity Relationship*, U.S. ENERGY & COMMERCE COMM. (May 7, 2014), http://energycommerce.house.gov/press-release/north-american-energy-infrastructure-act-will-bolster-us%E2%80%93canada-electricity#sthash.VKtC9JA1.dpuf.

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

aimed at enhancing U.S. CI cyber security, focusing on the NIST Framework. Part III investigates Canadian CI regulation, with a special emphasis on the government's reception to the NIST Framework. We conclude by couching this investigation within the wider debate surrounding international CI protection, including the emergence of cybersecurity norms in this space.

II. UNPACKING THE CYBER THREAT AFFECTING 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 that impact North American CI remains limited and unsophisticated. That said, more than one-third of Canadian firms have reported being victims of cyber attacks.[8] In a 2015 survey done by Kaspersky Labs, Canada was named the tenth most-attacked nation in the world.[9] The Kaspersky survey also notes that the United States is third most-attacked nation as of March 2015.[10] Also, from 2000 to 2008, U.S. cybersecurity surveys found that the proportion of organizations reporting cyber attacks ranged from forty-three percent to seventy percent.[11]

In 2010, 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 or 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, the Canadian government audits noted an absence of action plans, the slow pace of private-sector CI partnership building, and the lack of timeliness and completion of monitoring

[7] *See* 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/.

[9] *See Cyberthreat Real-Time Map*, KASPERSKY, http://cybermap.kaspersky.com/ (last visited Mar. 10, 2015).

[10] *See id.*

[11] *See* ROBERT RICHARDSON, COMPUTER SEC. INST., CSI COMPUTER CRIME & SECURITY SURVEY 13 (2008), *available at* http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf.

[12] *See* SYMANTEC, STATE OF ENTERPRISE SECURITY STUDY 7 (2010), https://www.symantec.com/content/en/us/about/presskits/SES_report_Feb2010.pdf.

[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/.

programs that protect CI from cyber threats.[15] What is more, a 2012 report from the Auditor General of Canada noted that the Canadian government appropriated only 780 million dollars in funding to improve security for Canada's critical infrastructure and less than 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 be borne in a proportionate manner by all those who benefit…[17]

However, Canada is far from alone in its struggle to fight the evolving cyber threat to CI. According to a McAfee survey, CI owners and operators from the United States reported that their high-level adversaries, such as foreign governments, repeatedly cyber attacked their networks and control systems.[18] The consequences of such attacks are potentially devastating. In fact, the U.S. Cyber Consequences Unit estimates losses from a major attack on U.S. CI at roughly 700 billion U.S. dollars.[19] Congress, however, has been slow to meet this challenge, which has prompted executive action. As such, what follows is the analysis of the current U.S. approach to changing the unsustainable cybersecurity status quo. Then, we take a comparative look at some of Canada's CI cybersecurity reform efforts.

[15] OFFICE OF THE AUDITOR GEN. OF CAN., REPORT OF THE AUDITOR GENERAL OF CANADA – FALL 2012: CHAPTER 3 (2012), *available at* http://www.oag-bvg.gc.ca/internet/docs/parl_oag_201210_03_e.pdf.

[16] ANGELA GENDRON & MARTIN RUDNER, CAN. SEC. INTELLIGENCE SERV., ASSESSING CYBER THREATS TO CANADIAN INFRASTRUCTURE (MAR., 2012), https://www.csis.gc.ca/pblctns/ccsnlpprs/CyberTrheats_AO_Booklet_ENG.pdf.

[17] *Id.*

[18] STEWART BAKER, SHAUN WATERMAN & GEORGE IVANOV, MCAFEE, IN THE CROSSFIRE: CRITICAL INFRASTRUCTURE IN THE AGE OF CYBER WAR 1 (2010), *available at* http://img.en25.com/Web/McAfee/NA_CIP_RPT_REG_2840.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, CYBER SECURE INST., CYBERWARFARE AND CYBERTERRORISM: THE NEED FOR A NEW U.S. STRATEGIC APPROACH 15-17 (2010), *available at* http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-072.pdf).

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

President Obama issued an executive order in 2013 that expanded public-private information sharing and tasked NIST with establishing the NIST Framework to better secure critical infrastructure.[20] Version 1.0, *Framework for Improving Critical Infrastructure Cybersecurity*, was released in February 2014.[21] This was designed to harmonize consensus standards and industry best practices. Its proponents argue that it provided a flexible and cost-effective approach to enhancing cybersecurity.[22]

The NIST Framework does not create any binding obligations for private sector actors and has no means of enforcement for those that choose to adopt it.[23] Nonetheless, its widespread implementation may establish a cybersecurity standard of care in the United States, even without Congressional action.[24] This holds the potential to spill over beyond traditional CI sectors into the private sector in the United States. Indeed, the White House announced that, as of February 2015, Intel, Apple, and Walgreens have incorporated the NIST Framework into their cybersecurity efforts. [25] Actually, even Bank of America now requires its use by vendors.[26]

With a deep degree of private-sector participation, the NIST Framework's basic structure divides cybersecurity into five broad functions. [27] These include: identify, protect, detect, respond, and recover.[28] Notably, the NIST Framework also provides a series of steps for organizations to follow to assess and address their cyber risk exposure.[29] This permits firms to incorporate cyber risk management in a manner that is consistent with their overarching business goals and financial capabilities. Though it is premature to predict the permanence of the NIST Framework, its inherent flexibility has proven attractive to CI operators

[20] *See* WHITE HOUSE PRESS SEC'Y, *supra* note 6; *see also* Mark Clayton, *supra* note 6.

[21] WHITE HOUSE PRESS SEC'Y, *supra* note 6, at 1.

[22] Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11739,11741 (February 19, 2013).

[23] *See* WHITE HOUSE PRESS SEC'Y, *supra* note 6

[24] *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").

[25] *See* WHITE HOUSE PRESS SEC'Y, FACT SHEET: WHITE HOUSE SUMMIT ON CYBERSECURITY AND CONSUMER PROTECTION (Feb. 13, 2015), http://m.whitehouse.gov/the-press-office/2015/02/13/fact-sheet-white-house-summit-cybersecurity-and-consumer-protection.

[26] *See id.*

[27] WHITE HOUSE PRESS SEC'Y, *supra* note 6, at 7.

[28] *Id.*

[29] NATI'L INST OF STANDARDS AND TECH, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBER SECURITY VERSION 1.0 (Feb. 12, 2014), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf at 13-14.

and policymakers alike. Already, cyber security consultants are advising private-sector clients that "the 'standard' for 'due diligence' was now the NIST Cybersecurity Framework."[30]

Over time, the NIST Framework has both the potential to shape a standard of care for domestic CI organizations and the capability to help harmonize global cybersecurity best practices for the private sector. This is particularly true given the active NIST Framework collaborations that have begun to occur between a number of nations, including the United Kingdom, Japan, Korea, Estonia, Israel, Germany, and Australia.[31] The question considered below is what impact, if any, this initiative has had on reshaping Canada's cybersecurity policymaking landscape.

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

The Canadian government has established various cyber security frameworks that manage the cyber threats facing North American CI.[32] Before diving into this issue, however, the context will first be briefly summarized. Both Canada and the United States have numerous agencies charged with enhancing national cyber security.[33] Much of Canada's cyber security policymaking authority resides in the Department of Public Safety and Emergency Preparedness Canada ("PSEPC").[34] This agency is similar to the U.S. Department of Homeland Security ("USDHS"). Like USDHS, PSEPC is responsible for ensuring that the cyber security of civilian government networks and private industry networks related to CI.[35]

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

[31] Gerald Ferguson, *NIST Cybersecurity 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 (noting that 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"); NAT'L INST. OF STANDARDS AND TECH., UPDATE ON THE CYBERSECURITY FRAMEWORK (July 31, 2014), http://nist.gov/cyberframework/upload/NIST-Cybersecurity-Framework-update-073114.pdf ("NIST and other U.S. 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.").

[32] *See generally Cyber Security: A Shared Responsibility*,PUB. SAFETY CAN. (Apr. 3, 2014), http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/index-eng.aspx.

[33] *See* Gordon M. Snow., Statement Before the Senate Judiciary Committee, Subcommittee on Crime and Investigation, THE FED. BUREAU OF INVESTIGATION (Apr. 12, 2011), https://www.fbi.gov/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism.

[34] *See* Cyber Security: A Shared Responsibility, *supra* note 32.

[35] *See* U.S. DEP'T HOMELAND SEC., SAFEGUARD AND SECURE CYBERSPACE (Nov. 2, 2012), *available at* http://www.dhs.gov/safeguard-and-secure-cyberspace.

In 2005, the Canadian government created the Canadian Cyber Incident Response Center ("CCIRC") within PSEPC.[36] CCIRC monitors the cyber security of both public- and private-sector networks including CI. Thus, it is charged with leading the government's response to and recovery from cyber attacks.[37] The manner in which CCIRC achieves this is threefold: (1) it advises the government and private sector how to prepare for and mitigate cyber threats; (2) it provides technical expertise, i.e., forensic cyber analysis; and (3) acts as a framework where experts may share and collaborate their ideas that help support critical Canadian CI.[38]

CCIRC is Canada's version of the U.S. Computer Emergency Readiness Team ("US-CERT"). US-CERT was established in 2003 and is under the jurisdiction of the USDHS.[39] Thus, both CCIRC and US-CERT provide their government and private sectors with the tools and information necessary to mitigate the effects of cyber attacks. These also identify and share cyber security best practices and threat information.[40]

In February 2014, the Canadian government announced the Cyber Security Cooperation Program ("CSCP"), which is administered by PSEPC.[41] The CSCP is a five-year, 1.5 million Canadian dollars grant initiative that funds research and projects created to improve Canada's "vital cyber systems" security.[42] Specifically, CSCP identifies programs and research that improve best practices, standards, operational methodologies and cyber assessment tools for critical cyber systems and CI.[43]

Over the past decade PSEPC has published a number of notable reports related to CI cyber security. These reports detail how the Canadian government and private sectors should improve CI cyber security.[44] In 2010, PSEPC published the *National Strategy for Critical Infrastructure* ("National Strategy") and the *Action Plan for Critical Infrastructure* ("Action Plan") reports, which address vital infrastructure safety and security issues.[45]

[36] *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/.

[37] *See id.*

[38] *See Canadian Cyber Incident Response Centre (CCIRC),* PUB. SAFETY CAN. (Dec. 12, 2014), http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-eng.aspx.

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

[40] *See Cyber Incident Response Centre (CCIRC) Partners,* PUB. SAFETY CAN (Feb. 24, 2015), http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-prtnrs-eng.aspx.

[41] *See Cyber Security Cooperation Program*, PUB. SAFETY CAN (Feb. 6, 2015) http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/cprtn-prgrm/index-eng.aspx.

[42] *Id*.

[43] *See Research Themes,* PUB. SAFETY CAN (Feb. 6, 2015), http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/cprtn-prgrm/rsrch-thms-eng.aspx.

[44] *See Publications and Reports,* PUB. SAFETY CAN (Jan. 23, 2015), https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/index-eng.aspx.

[45] *See Critical Infrastructure* PUB. SAFETY CAN (March 20, 2014), http://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-eng.aspx.

The National Strategy outlines ten CI areas vulnerable to cyber attacks and addresses how these areas should be strengthened.[46] The report rationalizes that local owners and operators are ultimately responsible for securing CI.[47] It then describes how the government plans to share important information and address the challenges faced by local owners and operators of diverse CI assets.

The PSEPC also published *Canada's Cyber Security Strategy* in 2010.[48] This describes the three main objectives of Canadian national cyber security strategy including: securing government systems, working with the private sector to ensure secure nongovernment systems, and helping the Canadian public safely browse the internet.[49] Subsequently, the government published *Action Plan 2010 – 2015 for Canada's Cyber Security* in 2013 to help flesh out the cyber security strategy report. Specifically, this report details what actions different stakeholders should undertake to achieve identified cyber security goals.[50]

The above-mentioned 2010 Action Plan was recently updated to reflect vital infrastructure protection for the years 2014 – 2017. The revised Action Plan details how cyber security has increasingly become an important aspect of CI protection and calls for improving public-private partnerships, assessing critical infrastructure risks more effectively, and strengthening critical infrastructure resilience.[51]

Many objectives in the revised Action Plan are similar to those mentioned in the NIST Framework, such as the objective that identifies the areas of high cyber risk and ways to mitigate this risk.[52] In addition, both the revised Action Plan and the NIST Framework greatly emphasize increasing the communication between the stakeholders of vital CI.

While the NIST Framework does not outline the stakeholders responsible for individual activities related to cyber security, it does provide information on the organization and categorization of various activities related to ensuring cyber

[46] 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).

[47] NATIONAL STRATEGY FOR CRITICAL INFRASTRUCTURE 2 (2009), http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf.

[48] *Id*. at 3.

[49] CANADA'S CYBER SECURITY STRATEGY 7 (2010), http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf.

[50] ACTION PLAN 2010 – 2015 FOR CANADA'S CYBER SECURITY STRATEGY 3–4 (2013), http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/ctn-pln-cbr-scrt-eng.pdf.

[51] *See id*.

[52] *Id*. at 7–8.

security.[53] Indeed, the NIST Framework received much attention from Canadian policymakers, as it has with an array of North American industries from the energy, IT, manufacturing, retailing, and other sectors.[54]

This process is now playing out beyond North America's borders. Indeed, the Information Technology Industry Council ("ITI") explained that it recently visited Japan and South Korea, where it shared "the benefits of a public-private partnership-based approach to developing globally workable cyber security policies."[55] Moreover, "ITI highlighted the [NIST Framework] as an example of an effective policy" that "reflect[s] global standards and industry-driven practices."[56]

Time will tell whether this model of a "voluntary" bottom-up cyber security framework will effectively meet the multifaceted cyber threat. However, given the evolving problem and reluctance by U.S. and Canadian lawmakers to pass binding measures, this may currently be the best available option. As such, 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 cooperation, progress made in one nation will still leave the other open to cyber attacks that may have been prevented.

V. CONCLUSION

In a special report on North America, the Council on Foreign Relations ("CFR") noted the interconnection between the North American economies stating, "[c]yber failures in one country could have ripple effects on neighbors and cross-border production" and recommended "that the United States, Canada, and Mexico set baseline standards for cyber protection."[57] The NIST Framework is not the only candidate for the undertaking.[58] Notably, the CFR Task Force

[53] WHITE HOUSE PRESS SEC'Y, *supra* note 6, at 19.

[54] *See, e.g.*, INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION, INC *New US Cybersecurity Framework Developed by NIST Features COBIT 5 in the Core,* ISACA (Feb. 14, 2014), *available at* http://www.isaca.org/About-ISACA/Press-room/News-Releases/2014/Pages/New-US-Cybersecurity-Framework-Developed-by-NIST-Features-COBIT-5-in-the-Core.aspx; 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.

[55] Email from Information Technology Industry Council, to Diane Honeycutt (October, 2014) (on file with author), *available at* http://www.itic.org/dotAsset/f/9/f9ef5f80-ffc5-4035-b274-87489605ab6e.pdf.

[56] Beauchesne, *supra* note 54.

[57] DAVID H. PATRAEUS ET. AL., COUNCIL ON FOREIGN RELATIONS, INC., NORTH AMERICA: TIME FOR A NEW FOCUS, INDEPENDENT TASK FORCE REP. NO. 71 80 (2015), *available at* https://www.google.ch/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CCUQFjABahUKEwi4mNKwq7jIAhWHtBoKHQJlAmA&url=http%3A%2F%2Fi.cfr.org%2Fcontent%2Fpublications%2Fattachments%2FTFR71_North_America.pdf&usg=AFQjCNFGbAgj8mSpT-_MWC3aCI4Tti5xEA&sig2=Ra0Hirvj2q3A36aqSKZHXA&cad=rja.

[58] Petraeus, *supra* note 57, at 80.

recommended joint cyber security frameworks drawn from the Critical Security Controls and the USDHS Continuous Diagnostics and Mitigation Program to promote "cyber hygiene."[59]

Moreover, CFR recommended several of the measures, including deeper integration of national CERTs and robust international public-private information sharing.[60] Indeed, these conclusions build from the *U.S.-Canadian Cybersecurity Action Plan*, which deepens cooperation between U.S. and Canadian cyber emergency response teams, provides for more robust private-sector information sharing, and promotes better "public awareness" of the multifaceted cyber threat.[61] Over time, such efforts may form a combined North American CERT and Information Sharing and Analysis Organization. Leveraging the resources available in the United States and Canada allows both nations to more effectively meet the evolving cyber threat, help secure North American CI, and contribute to global cyber peace.

[59] *Id.*
[60] *Id.*
[61] PUB. SAFETY CAN. AND U.S. DEP 'T. OF HOMELAND SEC., *supra* note 4, at 2-4.