



MSU Graduate Theses

Spring 2019


Cybersecurity for Critical Infrastructure: Addressing Threats and Vulnerabilities in Canada

Samuel A. Cohen

Missouri State University, Cohen145@live.missouristate.edu

As with any intellectual project, the content and views expressed in this thesis may be considered objectionable by some readers. However, this student-scholar's work has been judged to have academic value by the student's thesis committee members trained in the discipline. The content and views expressed in this thesis are those of the student-scholar and are not endorsed by Missouri State University, its Graduate College, or its employees.

Follow this and additional works at: <https://bearworks.missouristate.edu/theses>

 Part of the [Defense and Security Studies Commons](#), [Information Security Commons](#), [Infrastructure Commons](#), and the [Science and Technology Studies Commons](#)

Recommended Citation

Cohen, Samuel A., "Cybersecurity for Critical Infrastructure: Addressing Threats and Vulnerabilities in Canada" (2019). *MSU Graduate Theses*. 3340.

<https://bearworks.missouristate.edu/theses/3340>

This article or document was made available through BearWorks, the institutional repository of Missouri State University. The work contained in it may be protected by copyright and require permission of the copyright holder for reuse or redistribution.

For more information, please contact bearworks@missouristate.edu.

**CYBERSECURITY FOR CRITICAL INFRASTRUCTURE: ADDRESSING THREATS
AND VULNERABILITIES IN CANADA**

A Master's Thesis

Presented to

The Graduate College of
Missouri State University

In Partial Fulfillment

Of the Requirements for the Degree

Master of Science, Defense and Strategic Studies

By

Samuel A. Cohen

May 2019

Copyright 2019 by Samuel A. Cohen

CYBERSECURITY FOR CRITICAL INFRASTRUCTURE: ADDRESSING THREATS AND VULNERABILITIES IN CANADA

Department of Defense and Strategic Studies

Missouri State University, May 2019

Master of Science

Samuel A. Cohen

ABSTRACT

The aim of this thesis is to assess the unique technical and policy-based cybersecurity challenges facing Canada's critical infrastructure environment and to analyze how current government and industry practices are not equipped to remediate or offset associated strategic risks to the country. Further, the thesis also provides cases and evidence demonstrating that Canada's critical infrastructure has been specifically targeted by foreign and domestic cyber threat actors to pressure the country's economic, safety and national security interests. Essential services that Canadians and Canadian businesses rely on daily are intricately linked to the availability and integrity of vital infrastructure sectors, such as the financial, water, healthcare, electricity, and transportation systems. These sectors continue to become increasingly connected to Information Technology (IT) assets and processes that are vulnerable to malicious computer activity. To assess these vulnerabilities, the technical components of this paper analyze the current cybersecurity challenges impacting critical infrastructure owners, operators, regulators and vendors with regard to legacy IT systems and new emerging technologies—such as cloud computing and 5G. This includes analysis on the integration of corporate Internet-linked networks with traditionally isolated Industrial Control System (ICS) and Supervisory Control and Data Acquisition (SCADA) networks. It also includes a non-industrial sector case study focusing on the financial system, which discusses the cybersecurity challenges facing the national Large-Value Transfer System (LVTS). From a national security perspective, the thesis maps Canada's cyber threat landscape and analyzes actors such as nation-state governments, Advanced Persistent Threat (APT) groups, terrorist organizations, malicious and negligent insiders, and hacktivists. As a recommendation, the thesis constructs a three-tiered public-private partnership that draws on a new Canadian-based cybersecurity assessment framework, the adoption of an Assumption of Compromise (AoC) security culture, and the improvement of cyber threat information-sharing programs.

KEYWORDS: cybersecurity, critical infrastructure, national security, SCADA, ICS, Public Safety Canada, cyber attack, control networks, corporate networks, NIST framework

**CYBERSECURITY FOR CRITICAL INFRASTRUCTURE: ADDRESSING THREATS
AND VULNERABILITIES IN CANADA**

By

Samuel A. Cohen

A Master's Thesis
Submitted to the Graduate College
Of Missouri State University
In Partial Fulfillment of the Requirements
For the Degree of Master of Science, Defense and Strategic Studies

May 2019

Approved:

Brian Mazanec, Ph.D., Thesis Committee Chair

Andrei Shoumikhin, Ph.D., Committee Member

Ilan Berman, J.D., Committee Member

Julie Masterson, Ph.D., Dean of the Graduate College

In the interest of academic freedom and the principle of free speech, approval of this thesis indicates the format is acceptable and meets the academic criteria for the discipline as determined by the faculty that constitute the thesis committee. The content and views expressed in this thesis are those of the student-scholar and are not endorsed by Missouri State University, its Graduate College, or its employees.

TABLE OF CONTENTS

Introduction	Page 1
Thesis Objective and Statement	Page 4
Roadmap	Page 6
Role and Composition of Canadian Critical Infrastructure	Page 8
Sector Identification and Overview	Page 9
Public and Private Infrastructure Governance	Page 10
Ontario’s Electrical Grid Case Study: Recognizing Sector Complexity	Page 12
Identifying Technical Vulnerabilities	Page 16
Industrial IT Risk: Blurring of Corporate and Control Networks	Page 17
Understanding Control Network Architecture	Page 18
Cybersecurity Challenges in the Control Environment	Page 20
Non-Industrial IT Risk: Financial System Case Study	Page 28
Canada’s Financial Market Infrastructure (FMI)	Page 29
FMI Cybersecurity Challenges	Page 32
Emerging IT Systems and New Cyber Risks	Page 40
Software-Defined Networking (SDN) and Cloud Computing	Page 40
5G and Internet of Things (IoT)	Page 46
Mapping Canada’s Cyber Threat Landscape	Page 53
Nation-States, Advanced Persistent Threats (APT) and Cyber Warfare	Page 54
Cyber Terrorism and Hacktivism	Page 65
Insider Threats: Foreign Espionage To Accidental IT Disruptions	Page 74
The Strategic Impact of Cyber Attacks On Critical Infrastructure	Page 82
Ukraine Electrical Grid Shutdown, 2015	Page 83
Stuxnet Computer Worm in Iran, 2010	Page 89
WannaCry Ransomware Virus and Britain’s Healthcare System, 2017	Page 96
Implications for Canada	Page 100
Policy-Based Solutions, Recommendations and Remediations	Page 103
Critical Infrastructure Cybersecurity: A Framework Approach	Page 104
Fostering an Assumption of Compromise (AoC) Culture	Page 112
Improving Cyber Threat Information-Sharing	Page 117
Areas of Future Research	Page 124
Conclusion	Page 127
Bibliography	Page 131

INTRODUCTION

Canada's economic stability and national security depend on resilient critical infrastructure, such as secure and reliable access to banking, healthcare, communications, food distribution and transportation systems. The safe and uninterrupted operation of this infrastructure is a strategic imperative for the government, and any actor aiming to disrupt these operations poses a real and immediate risk to the safety and prosperity of the country. Previous cybersecurity incidents involving essential services and infrastructure have demonstrated the social and financial costs information system disruptions can induce. To ensure Canadian citizens, businesses and organizations are protected from the strategic consequences such a disruption could yield, the federal government must continue to expand and evolve their activities aiming to improve the country's national cyber resiliency in the essential service and infrastructure space.

In May of 2017, Britain's National Health Service (NHS) experienced the WannaCry ransomware worm—developed and executed by North Korean threat actors—which resulted in the cancellation of at least 19,494 healthcare appointments and the delay of 139 urgent cancer treatments nationwide.¹ More than 1,200 pieces of diagnostic equipment were inflected, including MRI scanners and devices for testing blood and tissue samples. In December of 2015, a highly complex and calculated cyber attack against Ukraine's electrical infrastructure resulted in power outages lasting six hours, impacting 225,000 citizens and regional businesses.² In

¹ Owen Hughes, "WannaCry Impact On NHS Considerably Larger Than Previously Suggested," *Digital Health: News, Networks and Intelligence*, October 21, 2017, https://www.chicagomanualofstyle.org/tools_citationguide/citation-guide-1.html.

² Dustin Volz, "U.S. Government Concludes Cyber Attack Caused Ukraine Power Outage," *Reuters*, February 25, 2016, <https://www.reuters.com/article/us-ukraine-cybersecurity/u-s-government-concludes-cyber-attack-caused-ukraine-power-outage-idUSKCN0VY30K>.

January of 2019, a zero-day vulnerability resulted in a computer virus disabling critical Information Technology (IT) infrastructure based in the Health Sciences North (HSN) facility, located in Ontario, Canada. The incident at HSN, who provides IT services for other regional medical centers, forced 24 hospitals throughout Northern Ontario to experience sustained critical service disruptions.³ These disruptions included electronic medical records system downtime at 21 hospitals, cancer program downtime at 12 hospitals, medical imaging system downtime at 10 hospitals and back-office software and email service downtime at four hospitals.⁴ These are a few examples of the real impact and cost malicious cyber actors and poor IT security and risk management practices can induce to services Canadian citizens, businesses and organizations rely on 365 days a year.

Rapid evolutions in the Information and Communications Technology (ICT) environment continue to alter the control systems, operating procedures and risks associated with the country's essential services and critical infrastructure environment. Included in this evolution are the introduction of 5th Generation wireless networks (5G) and the application of Internet of Things (IoT) devices nationwide, which will vastly increase the amount and types of connectivity experienced across the country in addition to increasing the reliance on remote operation over geographically dispersed assets. As connectivity grows so will the attack surface for malicious cyber actors, which invariably raises the prospect of a successful operation or damaging incident. Not only are new processes of digital interaction creating vulnerabilities, but the actual tools used to manage the changing ICT landscape are also posing new challenges. For example, Software-defined Networking (SDN) and Network Functions Virtualization (NFV) are

³ Carly Weeks, "Computer Virus Causes Delays At Dozens Of Northern Ontario Hospitals," *The Globe and Mail*, January 18, 2019, <https://www.theglobeandmail.com/canada/article-computer-virus-causes-delays-at-dozens-of-northern-ontario-hospitals/>.

⁴ CBC News, "Virus Affecting IT System At Health Sciences North Impacting Health Care Across The Region," *CBC*, January 17, 2019, <https://www.cbc.ca/news/canada/sudbury/hsn-it-virus-update-1.4982267>.

altering the architecture of the country's telecommunication backbone, creating new cybersecurity risks that traditional monitoring and protection policies will fail to address. Since the reliability and integrity of the ICT environment is universally important to all critical infrastructure sectors in Canada, these specific technological changes represent one example that will lead to cross-sector risks impacting multiple industries and essential services simultaneously. Further, as global supply chains continue to grow, so will the risk of embedded malware or maliciously altered software and hardware being acquired by important Canadian infrastructure operators and their systems.

To address the changing cyber threat landscape, the federal government and its agencies have begun to review cybersecurity policy and implement new risk, control and management standards. For example, Public Safety Canada's use of the Canadian Cyber Resilience Review (CCRR) and the Critical Infrastructure Resilience Tool (CIRT) reflect proactive measures being undertaken to increase cybersecurity in the essential services ecosystem. Additional government publications reinforce this effort, such as Public Safety Canada's 2016 "Fundamentals of Cyber Security for Canada's Critical Infrastructure Community" and the Canadian Centre for Cyber Security's 2018 "National Cyber Threat Assessment."⁵ However, more awareness, mapping, audit and security control development needs to occur to properly respond to the rapidly evolving IT risks within the critical infrastructure space. This particularly includes third-party vendors and new unique challenges posed by advanced and dedicated threat actors.

Since the majority of Canadian critical infrastructure is operated and owned by the private sector, there is a large and complex non-governmental vendor system providing daily

⁵ "Cyber Security: Publications And Reports," *Public Safety Canada*, last modified November 19, 2018, <https://www.publicsafety.gc.ca/cnt/ntnl-scert/cbr-scert/index-en.aspx>.

maintenance and support services across the country's key industries.⁶ These commercial enterprises and their subcontractors interact with both public and other private entities to ensure timely, consistent and safe delivery of essential services to Canadians. Critical infrastructure stakeholders have historically overlooked detailed and tested cybersecurity policies as an attempt to reduce any barriers to communication, business efficiency or sensory reading speed—specifically in industrial control environments. This approach attracted hardware equipment and software optimized for an environment focused on operational efficiency and uptime, which has led to a digitally networked and Internet-linked Canadian infrastructure lacking key security controls. Similar risks have emerged in non-industrial sectors, though the technical challenges vary in scope and function. Foreign intelligence agencies, hacktivists, cyber criminals and terrorist organizations are becoming increasingly sophisticated and determined to infiltrate these types of industrial and non-industrial networks, which poses an active strategic threat to the most important systems Canadians depend on daily. Therefore, if Canada fails to address cyber vulnerabilities throughout its critical infrastructure environment, the prospect of a malicious actor or a catastrophic IT accident disrupting an essential service to the country will continue to increase.

Thesis Objective and Statement

The aim of this thesis is to assess the unique technical and policy-based cybersecurity challenges impacting Canada's critical infrastructure environment and how current private industry and government policies are not sufficiently equipped or implemented to address these growing strategic threats. Further, the thesis will also provide evidence highlighting that

⁶ "Fundamentals Of Cyber Security For Canada's CI Community," *Public Safety Canada*, June 24, 2016, <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/2016-fndmntls-cybr-scrty-cmmnty/index-en.aspx>.

Canada's critical infrastructure faces a distinctive cyber threat landscape, including a range of actors who have demonstrated intent and capability to infiltrate nationally important IT systems to pressure the country's economic and security interests. To mitigate these new cyber-based challenges threatening the country's long-term safety, security and financial wellbeing, this thesis will advocate for a new three-tiered critical infrastructure cybersecurity strategy implemented and regulated by a coordinated public-private partnership.

First, the government should create an appropriate minimum cybersecurity standard for any operator, vendor or company—and their hardware and software products—supporting the critical infrastructure system. Using a framework as an assessment tool, these standards would leverage control-based cybersecurity practices and include mandatory risk assessments of services to be provided from third parties. It would also audit and test vendors and operators to ensure their information security posture and products are adequately prepared to address Canada's threat landscape. Second, government and private sector stakeholders operating or servicing critical infrastructure must develop an assumption of compromise (AoC) culture to proactively defend their network from breach. These principles will ensure Canadian critical infrastructure maintains a layered defense against a range of cyber threats—malicious, environmental and accidental—while constantly searching for indicators of compromise and threats already within the networks. Third, the federal government needs to leverage Canadian intelligence, industry and cybersecurity bodies, such as the Communications Security Establishment (CSE) and the Canadian Cyber Threat Exchange (CCTX), to improve the provision of real-time threat data to critical infrastructure operators and vendors. This tier allows intelligence to be disseminated throughout the critical infrastructure apparatus, so cybersecurity

policies, practices and tooling can be tailored to defend against new exploit techniques and kits, a specific threat actor or a newly discovered zero-day vulnerability.

Roadmap

The first chapter of the thesis will provide an overview of the composition and governance arrangements associated with Canadian critical infrastructure, particularly emphasizing the pervasiveness of private industry servicing, operating or owning essential IT and physical assets.

The second chapter will highlight and explain the primary technical risks that Canada's industrial and non-industrial infrastructure sectors are currently experiencing, highlighting the existence of exploitable vulnerabilities in some of the country's most important IT systems and processes. This chapter includes an in-depth case study reviewing cybersecurity challenges throughout core elements of the country's financial market infrastructure.

The third chapter builds off of the technical analysis in chapter two and outlines how the linking of legacy IT systems with emerging technologies will create new risks and vulnerabilities for Canadians and Canadian businesses dependent on the availability of essential infrastructure services. Key technologies assessed in this section include IoT devices, 5G and cloud computing.

The fourth chapter maps and assesses Canada's critical infrastructure cyber threat landscape by providing evidence of nation-state governments, foreign intelligence agencies, insider threats, hacktivists and terrorist organizations seeking to disrupt, degrade and infiltrate nationally important IT systems. This chapter also analyzes motives, capabilities and the level of risk associated with the different threat actors.

The fifth chapter examines the policy and technical features of three past cyber attacks on critical infrastructure that resulted in catastrophic physical or financial damage. These strategic attacks are analyzed and then contextualized to gauge the possible impact an attack on the same or greater scale could have across Canada. The attacks assessed in this section include the Ukraine electrical grid shutdown in 2015, the Stuxnet computer worm in 2010, and the WannaCry Ransomware Virus in the context of Britain's Healthcare System in 2017.

The sixth and final chapter constructs and describes a three-tiered public-private cybersecurity recommendation capable of mitigating both technical and policy shortcomings currently residing across Canada's industrial and non-industrial critical infrastructure environments. This chapter leverages the threat actor risk analysis, the technical breakdown of current vulnerabilities and the mapping of relevant stakeholders in previous chapters to identify where policy reform could be beneficial and how it will address the strategic threat of critical infrastructure cyber risk.

ROLE AND COMPOSITION OF CANADIAN CRITICAL INFRASTRUCTURE

It is important to define a common understanding of critical infrastructure to be able to recognize its importance and role in supporting the prosperity of Canada. A report developed in March of 2014 by the Governments of Australia, Canada, New Zealand, the United Kingdom (U.K), and the United States (U.S.) outlined each country's approach and definition of critical infrastructure. According to the Canadian Government, critical infrastructure refers to, "Processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of the government."⁷ A previous 2011 Public Safety report, titled "National Strategy for Critical Infrastructure," highlighted that, "Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects, and significant harm to public confidence."⁸ Although these reports do not specifically or thoroughly address current cybersecurity concerns, the documents do highlight the intrinsic relationship between a country's national security and the integrity and availability of its essential services and infrastructure.

The key purpose of this chapter is to highlight the types of industries and sectors this thesis will be referring to when commenting on critical infrastructure cybersecurity. Additionally, it is important to outline the governance and oversight models that preside over the country's infrastructure and associated services to understand how ongoing and future cybersecurity initiatives will be administered, funded, controlled and implemented.

⁷ "Forging A Common Understanding For Critical Infrastructure," *Public Safety Canada*, March 19, 2014, <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/2016-frngng-cmmn-ndrstndng-crtcalnfrstrctr/index-en.aspx>.

⁸ "National Strategy For Critical Infrastructure," *Public Safety Canada*, November 11, 2011, <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx>.

Sector Identification and Overview

The Canadian Government recognizes 10 Critical Infrastructure sectors, which include: Energy and Utilities; Finance; Food; Transportation; Government; Information and Communication Technology; Health; Water; Safety; and Manufacturing.⁹ Although each of these sectors has different control regimes that govern operations and standards, the federal government has identified unique features within these categories that indicate an active and essential role in supporting the daily lives of Canadian citizens, businesses and organizations. It is also important to note that no individual sector is entirely independent, as there are interconnected and interdependent relationships. For example, the financial sector, while having its own internal ICT technologies, policies and oversight programs, does routinely rely on the accessibility and operability of the national public payments system and its associated communications backbone. Another example of cross-sector dependence would be the relationship between water and wastewater management systems and the food supply chain. Irrigation processes, water filtration systems and pumping stations all contribute an essential service supporting Canada's agricultural base and food security.

To address the cross-sector complexities that emerge from interdependences and overlaying functions, Defense Research and Development Canada created the "National Critical Infrastructure Interdependency Model" in 2016.¹⁰ This workshop, which eventually became a government publication, reveals the intricacies between multi-sector relationships, such as fuel shortages hindering ambulatory emergency response and the operation of the country's safety infrastructure. This could result in mobility and transport issues for patients needing access to hospitals, forcing medical facilities to deliver services externally and potentially straining local

⁹ "National Strategy For Critical Infrastructure," *Public Safety Canada*.

¹⁰ "National Critical Infrastructure Interdependency Model: Way Ahead," *Defense Research and Development Canada*, April 26, 2016, pg. 2-3, http://cradpdf.drdc-rddc.gc.ca/PDFS/unc225/p803698_A1b.pdf.

or regional healthcare infrastructure. In 2018, Public Safety Canada released the “National Cross Sector Forum 2018-2020 Action Plan for Critical Infrastructure,” which sought to align the different infrastructure sectors to coordinate development, regulatory, security and operational oversight activities.¹¹ The increasing frequency of multi-sector forums, workshops and initiatives highlights the growing interconnectivity of the country’s infrastructure and essential services landscape. It also reinforces the need to approach the overall cybersecurity challenge from a centralized perspective with input from different industries and different levels of government.

Public and Private Infrastructure Governance

The key objective within this section is to outline the structure and governance models overseeing the operation of critical infrastructure in Canada. It is not necessarily important to highlight detailed management configurations for different sectors, such as the water delivery system versus the financial system, but it is useful to understand how the federal government generally interacts with lower levels of public authority and private industry within the essential services space. This can reveal opportunities and weaknesses for cybersecurity policy reform discussed later in the thesis, and it will reveal the extent of third-party vendor involvement within the environment.

Canada’s 2011 critical infrastructure strategy noted that, “The responsibility for protecting critical infrastructure in Canada is shared by federal, provincial and territorial governments, local authorities, and [industry] critical infrastructure owners and operators—who bear the primary responsibility for protecting their assets and services.”¹² The last portion of this statement is reflective of the current infrastructure landscape in Canada, where government

¹¹ “National Cross Sector Forum 2018-2020 Action Plan For Critical Infrastructure,” *Public Safety Canada*, May 11, 2015, <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/pln-crtcl-nfrstrctr-2018-20/index-en.aspx>.

¹² “National Strategy For Critical Infrastructure,” *Public Safety Canada*.

authorities—primarily federal and provincial—retain little operational oversight of the information systems and networks supporting essential services across the country. For example, at the provincial level in Ontario, the government has specifically designated the private sector responsible for the security and availability of seven of the 10 critical infrastructure sectors. The Ontario Critical Infrastructure Assurance Program (OCIAP), last updated in April of 2017, designates Food, Water, Telecommunication Systems, Electrical Power Systems, Gas and Oil, Financial Services, Health Systems and Transportation Networks under private industry operational control.¹³ Under the program’s policies, private owner-operators are responsible for implementing adequate risk mitigation practices, business continuity plans and incident response mechanisms to reduce physical and cyber risks across their respective sectors. This reliance in Ontario on private operators—and their trusted third-party vendors—is consistent with other provincial infrastructure arrangements across the country.

Another example of the prevalent role of private industry can be found in a 2012 Defense Research and Development Canada report on British Columbia’s provincial critical infrastructure, which noted that, “Infrastructure assets are often owned and operated by private sector companies while government organizations are often responsible for public safety.”¹⁴ The report adds that while responding to a regional or provincial emergency infrastructure event, “It takes a team involving the private sector, the providers of the majority of services, to manage an incident.”¹⁵ Considering the majority of national infrastructure is owned or operated by the private sector, in addition to regulatory, licensing and inspection authorities being legislatively

¹³ Ontario Emergency Management (OEM), “Critical Infrastructure: Provincial Programs,” *Ontario Ministry of the Solicitor General*, last modified April 19, 2017, <https://www.emergencymanagementontario.ca/english/emcommunity/ProvincialPrograms/ci/ci.html>.

¹⁴ Lynne Genik, “Operations Research Support For Critical Infrastructure Resilience In The Province Of British Columbia,” *Defense Research and Development Canada: Center for Security Science*, October 16, 2012, pg. 6, <https://apps.dtic.mil/dtic/tr/fulltext/u2/a568449.pdf>.

¹⁵ *Ibid.*

designated to provincial or federal government bodies depending on the sector, there is an inherent diversity in oversight and control. This complex arrangement of responsibility and the varying organizational priorities between government and industry stakeholders reinforces the need for public and private partners to work collaboratively to ensure there is complete asset awareness and security coverage for each sector.

Additionally, the 2018 National Cyber Threat Assessment and the 2011 National Strategy for Critical Infrastructure recognize that to address this decentralized accountability arrangement, private critical infrastructure owners and operators will need to be equally active participants alongside government stakeholders to ensure expertise and information is shared in a timely and useful manner.¹⁶ Not only will this help entire sectors develop meaningful incident response policies and effective regulatory programs, but also, it can reduce communication barriers and disconnects between private stakeholders who do not know how or who to contact in government for infrastructure cybersecurity assistance. Since the networked and digitally connected infrastructure and essential service base in Canada crosses provincial boundaries, draws on federal and provincial legislative mandates, operates under private corporations and continues to face an increasingly sophisticated cyber threat landscape, coordinated governance and clear segregation of duties and responsibilities is becoming a national security priority.

Ontario’s Electrical Grid Case Study: Recognizing Sector Complexity

Although multiple infrastructure sectors have interconnected relationships, analyzing the oversight structure of the electrical grid in Ontario is a useful case study for understanding how government and private responsibilities intersect and overlap across Canada. Although technical

¹⁶ Canadian Center for Cyber Security, “National Cyber Threat Assessment 2018,” *Communications Security Establishment (CSE)*, pg. 7, December 6, 2018, <https://cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2018>.

challenges will be addressed in a later chapter, this section aims to highlight how even identifying relevant stakeholders, fostering collaboration and establishing adequate oversight mechanisms to cover the entirety of a sector can be extremely difficult. Failing to share security burdens and relying exclusively on the private or public portion of a sector has routinely resulted in a lack of adequate security and risk controls. Any trusted organization or vendor providing products, services or oversight within a given sector—electrical, energy or otherwise—is a potential IT vulnerability. This means that all companies and government bodies who interact with a sector from an operations, management or regulatory standpoint need to be included as a possible entry point for a malicious cyber incident. The general purpose of this section is to use Ontario’s electrical grid as an example of the scale and complexity associated with implementing a robust cybersecurity oversight program at the critical infrastructure level.

The upstream and downstream components of Canada’s provincial electrical grids are functionally integrated, geographically dispersed and involve many private and public stakeholders. In Ontario, for example, power generation providers, regional transmission operators, substation facilities and utility distribution organizations have complex regional interconnectedness in addition to having responsibilities that span across the international border with the U.S.¹⁷ Central to the operation of the overall grid is the Independent Electricity System Operator (IESO), who is regulated and mandated by Ontario’s government and controls the daily overall flow of electricity throughout the province.¹⁸ Key responsibilities of the IESO include balancing inputs from private and public power generators in the nuclear, hydro and wind industries to outputs being delivered by local utility companies.

¹⁷ Doug Vine, “Interconnected: Canadian And U.S. Electricity,” *Center for Climate Change and Energy Solutions*, March 2017, pg. 2, <https://www.c2es.org/site/assets/uploads/2017/05/canada-interconnected.pdf>.

¹⁸ “Ontario’s Energy Sector: Mission And Mandate,” *Ontario Energy Board*, accessed on December 23, 2018, <https://www.oeb.ca/about-us/mission-and-mandate/ontarios-energy-sector>.

Considering information assets supporting the IESO’s 24/7 operations play a paramount role in the availability of electricity throughout the region, protecting these systems from malicious cyber activity is a clear and necessary goal. However, as more stakeholders connect to the grid—either as producers, distributors or vendors—there are more potential organizations and networks that adversaries could attack to induce a cascading affect across the province. For example, Ontario’s IESO energy development maps indicate that there are more organizations being added to the already 129 different generation facilities active in the province combined with the 73 unique distribution companies.¹⁹ The notion of securing the grid by solely protecting cyber-connected assets at a central organization such as the IESO is flawed, as an actor directly targeting multiple generation or distribution organizations can bypass the IESO and still impact the province. This is in addition to the clear impact an IESO disruption itself could induce, which is becoming a more serious risk as new IT interactions and potential vulnerabilities will also be created with more entities connecting to the provincial balancing system.²⁰

Many regional generator and distribution entities in Ontario also provide power for residential and industrial facilities in the northeast U.S., whose power system is managed and controlled by different IESOs. To address safety and operational considerations of cross-region and cross-border activity, the Northeast Power Coordinating Council, Inc. (NPCC), a non-profit regulatory body, was created to act as an additional layer of oversight by monitoring the reliability of the bulk power system servicing the entirety of Northeastern North America. This

¹⁹ Independent Electricity System Operator (IESO), “Ontario’s Electricity System: Generation And Transmission System Maps,” *IESO Organization*, last modified December 3, 2018, <http://www.ieso.ca/localContent/ontarioenergymap/index.html>.

²⁰ Independent Electricity System Operator (IESO), “Standing Committee Cyber Security Forum,” *IESO Organization*, last modified January 2019, <http://www.ieso.ca/en/Sector-Participants/Engagement-Initiatives/Standing-Committees/Cyber-Security-Forum>.

includes four Canadian provinces and seven U.S. states, and Ontario's IESO.²¹ These overlapping provincial and international management systems combined with the large quantity of public and private stakeholders producing or delivering energy directly in Ontario reflects the increasingly complex landscape of the province's electricity sector. Further, with each organization having different systems, vendors, technologies and data processing tools, the amount of IT assets with potential vulnerabilities servicing the sector has grown exponentially—raising the risk of a major incident occurring.²²

Although this section only focused on one essential service in one region, the Ontario electrical grid example highlights how even a provincially focused infrastructure system has a wide range of stakeholders operating under extremely multifaceted and interconnected arrangements. Recognizing this case study as a reflection of the breadth and diversity of infrastructure sectors across Canada reinforces the notion that no entity or authority can sufficiently maintain awareness of a given sector's IT risks and cybersecurity challenges without establishing robust public-private coordination, cooperation, and information-sharing.

²¹ "Northeast Power Coordinating Council: About," *NPCC, Inc.*, last modified July 5, 2017, <https://www.npcc.org/About/default.aspx>.

²² Howard Solomon, "Ontario Electric Utilities To Report Soon On Their On Cyber Security Maturity," *IT world Canada*, January 18, 2019, <https://www.itworldcanada.com/article/ontario-electric-utilities-to-report-soon-on-their-on-cyber-security-maturity/414233>.

IDENTIFYING TECHNICAL VULNERABILITIES

The critical infrastructure IT environment is undergoing rapid change, which has created new opportunities for malicious actors while also introducing opportunities for new proactive security policy and regulatory reform. Legacy IT systems within Canada’s infrastructure were not developed with security as a core objective—particularly in industrial environments.²³ The underlying hardware and software responsible for the control environment and the actual operation of infrastructure—such as water pumps or electricity nodes—were developed from a reliability, safety and maintainability (RSM) perspective.²⁴ This is an alternative approach to system security compared to the standard system attributes of confidentiality, integrity and availability (CIA), which are associated with most non-industrial corporate and government IT environments today. The unique demands of critical infrastructure operation, such as zero downtime and remote connectivity over wide areas, have created challenging conditions for implementing strong cybersecurity programs. For example, although patching software bugs, reconfiguring hardware and conducting vulnerability scans are all critical steps towards ensuring CIA in IT systems, these activities also result in disruptions and delays that can be detrimental in an infrastructure control system.²⁵ These types of technical and policy challenges reinforce the need for a tailored critical infrastructure cybersecurity policy distinct from other industries.

The objective of this chapter is to highlight the technical requirements and posture of Canada’s industrial and non-industrial infrastructure while recognizing the key cyber vulnerabilities associated with different technologies and processes. For example, it is important

²³ Canadian Center for Cyber Security, “National Cyber Threat Assessment 2018.”

²⁴ David Kuipers and Mark Fabro, “Control Systems Cyber Security: Defense In Depth Strategies,” *Idaho National Laboratories and Department of Homeland Security*, May 2006, pg. 5, <https://inldigitallibrary.inl.gov/sites/sti/sti/3375141.pdf>.

²⁵ *Ibid.*, 7.

to understand the demand for Supervisory Control and Data Acquisition (SCADA) processes in industrial environments, as these Internet-linked tools provide significant financial benefits and operating efficiencies. However, it is equally important to recognize the inherent IT risks embedded in the operation of these systems, as growing connectivity with the Internet raises the likelihood of incidents and their potential scale and cost.

Industrial IT Risk: Blurring of Corporate and Control Networks

The IT systems used in critical infrastructure sectors across Canada vary in function and architecture, but two broad categories can be identified. Sectors where IT systems have a role in managing physical technologies—such as IT processes governing the valve flow of natural gas or oil in pipelines across Alberta—are referred to as industrial IT control environments.

Conversely, critical infrastructure sectors where control over physical processes is not a primary function can be described as non-industrial environments. This section will focus on the key technical features of industrial IT systems and their associated vulnerabilities, while the following section will focus on non-industrial IT systems and their vulnerabilities.

The underlying cyber challenges that have emerged in industrial IT environments are a result of two trends: first, corporate networks traditionally isolated from physical control centers and systems are becoming increasingly integrated due to ICT evolutions and changes in operating procedures—such as remote mobile access for corporate executives; second, the actual operating technology that interacts with the physical equipment has become directly integrated with Internet communication protocols and architecture standards.²⁶ The combined effect of these two trends has been the creation of new pathways for malicious cyber actors to

²⁶ Ed Powers et al., “Examining The Industrial Control System Cyber Risk Gap,” *Deloitte LLP*, 2015, pg. 3-4, <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-ics-white-paper.pdf>.

compromise Industrial Control System (ICS) networks. While this integration has enabled organizations to improve their equipment control processes and to become more efficient through robust data collection, new issues such as unauthorized user intrusion or data manipulation are exposing historically closed networks and assets to core vulnerabilities associated with the Internet.

Understanding Control Network Architecture. Modern industrial IT environments rely on the integration of ICS and SCADA processes to create highly optimized, automated, efficient and situationally aware control networks. ICS refers to the different types of processes and associated instrumentation—devices, systems, networks, and controls—used to operate and automate industrial management.²⁷ The resulting operational efficiencies have led to mass adoption of ICS throughout manufacturing, rail and aviation transportation, energy, water treatment and other critical infrastructure and key industries. While ICS tooling assists with the physical operations, SCADA systems are designed to collect field data, transfer it to a central computing facility, and display the information to the technician textually or graphically.²⁸ An organization’s SCADA architecture monitors, gathers, processes and transmits real-time data from basic computing devices called programmable logic controllers (PLCs) to human operators or technicians. These PLCs are directly linked to industrial systems and machinery, making their individual computer security a key priority for the overall system’s cybersecurity.²⁹ Altogether, SCADA and ICS interaction allows industrial operators and any associated corporate or

²⁷ Industrial Control Systems Cyber Emergency Response Team, “Recommended Practice: Improving Industrial Control System Cybersecurity With Defense-In-Depth Strategies,” *Department of Homeland Security*, September 2016, pg. 1-2, https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.

²⁸ *Ibid.*, 17.

²⁹ Kuipers and Fabro, “Control Systems Cyber Security: Defense In Depth Strategies,” 12-13.

government regulators to monitor an entire geographically dispersed system from a central location in real-time.

A key enabler of SCADA architectures and the linking of operational data to corporate IT and management systems is the evolution of the ICT landscape. Wireless communications systems combined with changes in business culture, such as allowing engineers, operators and business executives to have remote access to real-time operational data, have created new arrangements for connecting to corporate and control networks.³⁰ For example, wireless telecommunication infrastructure can enable enterprise decision-makers, such as a CEO, to view the status of his/her railway system operations and make important recommendations while offsite. This scenario requires that the executive have access to the control network's information, which could occur via an external Virtual Private Network (VPN) connection to corporate web servers or directly to the control network's information systems. This scenario demonstrates one instance of how Internet and telecommunication infrastructure has blurred the segregation of control and corporate networks. There are many additional circumstances where remote connection and even direct remote interaction with the control network is necessary, such as delivering real-time data to vendors servicing the infrastructure or to regulators overseeing cross-sector stability and availability—a common feature of large distributed electrical systems as noted in the Ontario grid case study.³¹

By outlining the control architecture, its primary data management processes and operational objectives, this section has provided the necessary background for identifying the key security challenges generated in industrial IT environments. Additionally, this background will be essential in subsequent chapters where previous cyber attacks on critical infrastructure

³⁰ William Shaw, "SCADA System Vulnerabilities To Cyber Attack," *Electric Energy Online*, October 2004, <https://electricenergyonline.com/energy/magazine/181/article/SCADA-System-Vulnerabilities-to-Cyber-Attack.htm>.

³¹ Kuipers and Fabro, "Control Systems Cyber Security: Defense In Depth Strategies," 10.

are analyzed, such as the U.S.-Israeli Stuxnet computer worm targeting Iranian nuclear infrastructure in 2010 or the cyber attack disabling major information assets across Ukraine's power grid in 2015.³²

Cybersecurity Challenges in the Control Environment. Traditionally, the primary tenant of ICS cybersecurity was the idea of security by obscurity, where IT operators relied on the fact that malicious actors and even employees could not understand the complex architecture or mechanics of the IT systems in the control network.³³ However, as corporate externally-facing information assets and isolated control networks overseeing equipment continue to integrate, risk mitigation practices such as security by obscurity are becoming increasingly obsolete. Further, since control domains have historically been separated from the digital threats associated with Internet connection, industrial security practices in the private and public sector have mainly focused on physical issues—such as protecting against unauthorized individuals accessing prohibited work areas or machinery. Evidence of the historic focus on physical threats at industrial sites can be drawn from past Canadian critical infrastructure strategies where acts of physical terrorism were of primary security concern, compared to the now dominating issue of cybersecurity program failures.³⁴

Contemporary cybersecurity issues in the control environment have many similar overlapping challenges experienced in the traditional corporate environment. For example, both networks and their information systems are at risk of hostile mobile code on endpoints,

³² Andrew Ginter, "The Top 20 Cyber Attacks Against Industrial Control Systems," *Waterfall Security Solutions*, December 2017, https://ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/QNL_DEC_17/Waterfall_top-20-attacks-article-d2%20-%20Article_S508NC.pdf.

³³ Industrial Control Systems Cyber Emergency Response Team, "Recommended Practice: Improving Industrial Control System Cybersecurity With Defense-In-Depth Strategies, 1, 7-8.

³⁴ Angela Gendron and Martin Rudner, "Assessing Cyber Threats To Canadian Infrastructure," *Canadian Security Intelligence Service*, March 2012, pg. 40, https://www.canada.ca/content/dam/isis-scrcs/documents/publications/CyberThreats_AO_Booklet_ENG.pdf.

escalations of privileges through code manipulation, covert traffic analysis, network reconnaissance, data gathering and exportation and unauthorized intrusions into the networks either through or around perimeter defenses, such as a firewall.³⁵ However, there are also distinct vulnerabilities that differentiate cybersecurity requirements and limitations in the control environment compared to the corporate environment. For example, the demands of control system availability and reliability compared to the corporate IT perspective emphasizing confidentiality and integrity makes certain security functionality inappropriate for industrial environments.³⁶ Some critical infrastructure sectors, such as transportation, chemical manufacturing and energy distribution have time sensitive operational requirements, so the latency—or the data transfer delay—issues associated with security tooling such as network segmentation, demilitarized zones and patching may create performance disruptions.³⁷ These delays may only last a few (milli)seconds in certain cases, but this can still prove to be detrimental to an ICS process. Another example would be requiring passwords for users working in a control center, which is a universal authentication standard in corporate environments but could hamper or interfere with emergency orders to override an ICS.

There are a range of technical vulnerabilities that threaten SCADA processes and ICS applications, software and hardware due to the growing interconnected relationship between corporate and control networks. A National Institute of Standards and Technology (NIST) Special Publication in 2013 focusing on SCADA and PLC security issues outlined 68 general vulnerabilities that threaten the control environment in a unique manner.³⁸ These vulnerabilities

³⁵ Kuipers and Fabro, “Control Systems Cyber Security: Defense In Depth Strategies,” 7, 17.

³⁶ Shaw, “SCADA System Vulnerabilities to Cyber Attack.”

³⁷ Industrial Control Systems Cyber Emergency Response Team, “Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-In-Depth Strategies,” 43.

³⁸ Marshall Abrams et al., “Guide To Industrial Control Systems (ICS) Security: NIST Special Publication 800-82,” *National Institute of Standards and Technology*, tables C-2—C-7, 2015, <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf>.

are in addition to the ICS vendor-specific software and hardware flaws that are constantly being identified by companies and security researchers across the world. Associated with the vulnerabilities that NIST outlines is a list compiled and maintained by the U.S. ICS Cyber Emergency Response Team (ICS-CERT), which contains Tactics, Techniques and Procedures (TTPs) a malicious actor can deploy to specifically gain entry into a control network or a device associated with an overall industrial system.³⁹

Combining this ICS-CERT vulnerability research with the NIST documentation, in addition to commentary from Public Safety Canada's previous ICS Security Symposiums, it becomes clear that the current threats facing critical infrastructure control environments in Canada are becoming increasingly pervasive, complex and costly to mitigate.⁴⁰ For example, a 2012 report from the Canadian Security Intelligence Service (CSIS) noted that, "The current trend towards Internet-linked connectivity between multiple SCADA systems and central office networks has increased the vulnerability and the risk of cascading consequences across critical infrastructure sectors."⁴¹ The report later adds that, "The Netherlands Office of the National Coordinator for Counterterrorism has forewarned that there exists a real possibility that Stuxnet-type malware will be replicated by adversaries for cyber attacks on vulnerable critical infrastructure systems."⁴² This analysis highlights the growing urgency for cybersecurity policy improvements and the need to address the more technical aspects of emerging and legacy ICS vulnerabilities.

³⁹ Cybersecurity and Infrastructure Security Agency, "Overview Of Cyber Vulnerabilities," *Department of Homeland Security*, accessed January 12, 2019, <https://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities#poor>.

⁴⁰ "2019 ICS Security Symposium," *Public Safety Canada*, last modified January 31, 2019, <https://www.publicsafety.gc.ca/cnt/ntnl-scert/cbr-scert/ndstrl-cntrl-sstms/vnts-en.aspx#smppm1>.

⁴¹ Gendron and Rudner, "Assessing Cyber Threats To Canadian Infrastructure," 40-41.

⁴² *Ibid.*

Although this section will not identify all the vulnerabilities listed by standards, government or vendor organizations working with industrial control technology, a few examples will be outlined to help highlight the relationship of the industrial environment's unique IT architecture with some common exploits routinely compromising ICS and SCADA equipment. A primary vulnerability in the industrial field stems from the corruption or compromise of databases that are storing or processing real-time operational information. Databases used by control systems almost always have a connection to other data libraries or computer historians situated in the business or corporate network, where there are web-enabled applications capable of interacting with untrusted external Internet users—perhaps business partners or regulators requiring control environment information.⁴³ Generally, data-driven applications rely on SQL to navigate and communicate with relational databases and information management systems, such as those in both control and corporate environments. An attacker can exploit the direct communication relationship between these database and data historian systems, thereby bypassing any security features that separate the networks.⁴⁴

Using special SQL injection commands, an attacker can input query information to enable entry into the database or the ability to enter additional commands to corrupt, steal or manipulate its data.⁴⁵ Considering control environments are highly reliant on this data's accuracy and integrity for operational management of equipment, the consequences of such an attack can be severely damaging. SQL injection is a hacking technique that nearly every IT enterprise with externally facing database applications needs to mitigate. However, this technique has unique implications for the industrial environment as a compromise of control system database or its

⁴³ Industrial Control Systems Cyber Emergency Response Team, "Recommended Practice: Improving Industrial Control System Cybersecurity With Defense-In-Depth Strategies, 17.

⁴⁴ "Understanding And Defending Against SQL Injection Attacks," *Beyond Security*, last modified January 2019, <https://www.beyondsecurity.com/about-sql-injection.html>.

⁴⁵ Cybersecurity and Infrastructure Security Agency, "Overview Of Cyber Vulnerabilities."

operational data can induce immediate physical disruption and damage to ICS-linked critical infrastructure equipment—such as electrical units supporting power supply to a hospital.

Another major vulnerability associated with control systems comes in the form of Man-In-The-Middle (MITM) attacks.⁴⁶ Although this technique is also common among malicious attackers targeting traditional corporate environments, the impact on control systems can be particularly significant considering the implications of corrupt and misleading data reaching human or automated operators. MITM attacks do not necessarily rely on infecting computers with malware on either end of a host-client system, but instead, aim to exploit the actual communications equipment between two systems.⁴⁷ MITM techniques do this by interfering and manipulating the technical protocols that guide, deliver, and organize data packets crossing a network. Management of different network communications in industrial IT environments is facilitated by Address Resolution Protocol (ARP), which helps upkeep local routing from network addresses to physical machine addresses at the data-link layer.⁴⁸ Each device on the control network maintains an ARP table so it knows which device address to send information to or request data from to complete a task.⁴⁹ Malicious actors can manipulate the ARP tables on the network, resulting in a targeted device sending its communications to the malicious actor's network address unknowingly.

The end result of a MITM operation is that the attacking host can intercept sensitive data in addition capturing, replaying, and injecting data into the network and have it interpreted as if it were authorized and coming from a valid source. Since the unique speed and timing features

⁴⁶ Oliver Eigner, Philipp Kreimel and Paul Tavolato, "Detection Of Man-In-The-Middle Attacks On Industrial Control Systems," *St. Polten University of Applied Sciences: Information and Security Department*, May 11, 2016, pg. 1-2, https://itsecx.fhstp.ac.at/wp-content/uploads/2016/11/04_PaulTavolato_ITSecX16.pdf.

⁴⁷ *Ibid.*, 6, 8-9.

⁴⁸ Gendron and Rudner, "Assessing Cyber Threats To Canadian Infrastructure," 14-15.

⁴⁹ Anon Delui, "Man In The Middle Attacks Explained Through ARP Cache Poisoning," *Cybrary*, October 1, 2015, <https://www.cybrary.it/0p3n/man-in-the-middle-attack-explained/>.

required in a control network result in local users and hosts usually being designated as trusted sources, data in the ICS environment is generally unencrypted and in plaintext format—further enabling the attacker to digest and reverse engineer any relevant information that gets intercepted.⁵⁰ With this data, the attacker can induce significant damage to industrial equipment. For example, by analyzing the network’s traffic the attacker can replicate a data payload to resemble a normal communication instruction being sent to a piece of equipment, potentially commanding the device to turn off or complete a destructive or disruptive action. The attacker could also patiently collect baseline data and then insert that data to the control center’s display screens to distract technicians or operators from the actual disruption occurring to PLC’s and their normal outputs. Although MITM is a risk for both standard businesses and critical infrastructure sectors, the impact these types of disruptions could have on an ICS environment is exceptionally dangerous and technically challenging to counter.

It is also worth highlighting examples of key patch management and configuration vulnerabilities, and the general operational requirements of the control architecture that make these vulnerabilities difficult to resolve.⁵¹ Since control environments have unique uptime demands, there are challenges for IT security teams aiming to improve the patch management processes of ICS Operating Systems (OS) and other device software in the industrial space. For example, due to the possible modifications to the underlying OS any update or patch may induce, changes must undergo comprehensive testing.⁵² This often takes the vendor and operator

⁵⁰ Marshall Abrams et al., “Guide To Industrial Control Systems (ICS) Security: NIST Special Publication 800-82,” section 3 pp. 11.

⁵¹ David Bisson, “ICS Security: What It Is And Why It’s A Challenge For Organizations,” *Tripwire Cyber Security Solutions*, August 20, 2018, <https://www.tripwire.com/state-of-security/ics-security/ics-security-challenge-organizations/>.

⁵² Industrial Control Systems Cyber Emergency Response Team, “Recommended Practice: Improving Industrial Control System Cybersecurity With Defense-In-Depth Strategies,” 26-27.

extended periods of time, resulting in long windows of unpatched bugs and vulnerabilities residing in ICS software until the updates are approved for implementation.

Additionally, it is common for government and private owner-operators to license ICS and SCADA technologies from vendors for upwards of 20 years depending on the software or hardware, which compares to an average of three years for standard business IT systems.⁵³ The reason for this is a combination of unique IT requirements on the control network and a capability disconnect between vendors and operators in relation to the rapidly evolving security needs of the ICS enterprise. For example, vendor produced off-the-shelf security applications and devices, such as firewalls, antivirus systems, and patch management tools, can usually be universally applied across common IT communication protocols at any company, organization or government entity. However, in the ICS landscape, these same security tools may not have interoperability with the control network's unique protocols.⁵⁴ This results in industrial operators relying on highly tailored and industry-centric vendors to build out custom software, including custom event logging systems, network port lockdown mechanisms, and features for disabling USB media docks on ICS equipment.⁵⁵ Due to this customization process, ICS products are expensive and very difficult to replace, which typically forces IT assets to linger in the industrial environment for longer periods of time compared to the standard business environment.

As vendors develop, market and sell new systems and tools, most of their financial priorities and resources begin to shift from maintaining and updating their legacy products to improving their new offerings.⁵⁶ Consequently, there are often prolonged IT risks stemming from software no longer being updated by the vendor and known vulnerabilities becoming recognized

⁵³ Gendron and Rudner, "Assessing Cyber Threats To Canadian Infrastructure," 8-9.

⁵⁴ David Bisson, "ICS Security: What It Is And Why It's A Challenge For Organizations."

⁵⁵ Ibid.

⁵⁶ Industrial Control Systems Cyber Emergency Response Team, "Recommended Practice: Improving Industrial Control System Cybersecurity With Defense-In-Depth Strategies," 4, 26.

as accepted risk by infrastructure organizations. Corporate executives, recognizing that constantly licensing new software or hardware would be prohibitively costly, accept the risk of sustaining legacy systems to ensure uptime and operational efficiencies are maintained. Further, any approach favoring routine OS updates or hardware component replacements creates substantial technical and resource demands for both IT and ICS engineering staff on top of their daily responsibilities. This occurs because the testing of new software, devices and systems to ensure their compatibility with already deployed ICS tooling can require specialized facilities, training, outsourcing and procedures not available on-demand to the organization.⁵⁷ In certain circumstances, an owner-operator will test these software patches or IT hardware upgrades on a small segment of their live industrial environment to observe its impact, though this can be incredibly dangerous due to the possibility of system disruptions cascading across the environment or embedded malware distributing throughout the live network unbeknownst to the technicians or engineers conducting the test. Although patch vulnerability issues will continue to be explored in subsequent chapters when discussing past critical infrastructure cyber attacks, it is worth briefly noting that poor patch management facilitated a vast portion of incidents during the 2017 WannaCry ransomware attacks.⁵⁸ This highlights the material, financial and strategic impact a lack of software updates and change management procedures for servers and OS beyond their end-of-life date can induce in ICS and SCADA-based enterprises.

By reviewing a select number of key vulnerabilities and TTPs a malicious actor could exploit in an industrial environment, it becomes clear that there are several feasible pathways for unauthorized entry into some of the country's most important industrial data systems and

⁵⁷ Lee Neitzel and Bob Huba, "Top Ten Differences Between ICS And IT Cybersecurity," *The International Society of Automation*, June 2014, <https://www.isa.org/standards-and-publications/isa-publications/intech-magazine/2014/may-jun/features/cover-story-top-ten-differences-between-ics-and-it-cybersecurity/>.

⁵⁸ Mathias Thurman, "The WannaCry Scramble," *Computer World*, May 25, 2017, <https://www.computerworld.com/article/3198473/malware-vulnerabilities/the-wannacry-scramble.html>.

networks. Understanding how these cyber-enabled pathways relate to the control environments' unique architecture and operational objectives will support strategic risk evaluations discussed in following chapters. Key aspects of these evaluations will draw on this section's analysis of SQL injection, patch management limitations and other additional cybersecurity challenges highlighted for the industrial IT environment.

Non-Industrial IT Risk: Financial System Case Study

Unlike industrial IT processes where SCADA technologies and ICS tools are present across multiple sectors, non-industrial IT environments do not have the same widespread use of common systems, processes or assets. This makes it rare for non-industrial IT systems to have technical vulnerabilities that are equally threatening across multiple infrastructures. For example, the core IT features that support 9-1-1 emergency communications within Public Safety infrastructure are vastly different when compared to the IT systems that maintain and distribute electronic personal records throughout healthcare infrastructure. Although both of these IT systems are extremely important in each of their respective sectors, and while they do share some common general vulnerabilities by virtue of being connected to Internet-facing systems, their overall architectures and core system objectives are not the same. Due to the high-level differences IT systems have across different non-industrial environments in Canada and throughout the world, this section will only focus on the security challenges of a single sector—the financial system. This sector's cybersecurity challenges, from a risk and policy standpoint, will be representative of the difficulties facing the non-industrial critical infrastructure environment as a whole.

By outlining and analyzing Canada’s financial system—including the nation’s IT systems supporting transaction, clearing, settlement, payment and overall banking processes—this section will demonstrate how non-industrial cyber vulnerabilities are equally threatening to the operation of an essential service as the more popularized and discussed industrial vulnerabilities. Key components of this case study will draw on security challenges associated with the Society for Worldwide Interbank Financial Telecommunication (SWIFT) infrastructure and Canada’s domestic Large-Value Transfer System (LVTS), in addition to other private and public components of the Payments Canada enterprise. Although this section will not specifically focus on other sectors, it is worth mentioning that industries such as the Healthcare, Public Safety, ICT and the Food Supply Chain are also considered non-industrial IT environments. Alike the financial system, these sectors have limited cyber-physical dependences and interactions relative to industrial environments utilizing ICS and SCADA processes, reinforcing the need to analyze their vulnerabilities and IT risks in a separate technical context.

Canada’s Financial Market Infrastructure (FMI). The Bank of Canada defines an FMI as, “A system that facilitates the clearing, settling or recording of payments, securities, derivatives or other financial transactions among participating entities.”⁵⁹ This infrastructure is the core element of Canada’s economic activity, moving money and ensuring all parties’ accounts involved in a given transaction are balanced and accurate. Public and private stakeholders within the FMI, including banks, credit unions, regulators, insurance companies and large financial services firms process daily cash payments of \$175 billion CAD and more than

⁵⁹ Bank of Canada, “Regulatory Oversight Of Designated Clearing And Settlement Systems,” *BoC Press and Market Notices*, last modified April 2017, <https://www.bankofcanada.ca/2017/04/release-2016-bank-canada-fmi-oversight-activities-annual-report/>.

\$500 billion CAD in trades of stocks and bonds.⁶⁰ The system as a whole enables Canadian consumers and firms to safely and efficiently purchase goods and services, interact with business partners, make financial investments and transfer funds. The Bank of Canada recognizes that disruptions to the FMI, “Have the potential to pose systemic risk to Canada’s financial system, in that the inability of one participant to meet its obligations to the FMI could, by transmitting financial problems through the FMI, cause other participants to be unable to meet their obligations.”⁶¹ This type of cascading effect could cause a liquidity crisis across the country, a major loss of investor confidence and a halt to national economic activity.

An underlying feature of the FMI’s operation is private sector involvement, not only in terms of usage but also from an administrative and oversight standpoint. For example, Canada’s LVTS, which is the primary electronic payment system responsible for clearing, distributing and settling more than \$50 trillion CAD every year across the country, is owned and operated by a consortium of private financial institutions associated with Payments Canada—an organization under the Ministry of Finance.⁶² The direct stakeholders within the LVTS include 17 private institutions and public regulators, including Toronto Dominion Bank (TD), Royal bank of Canada (RBC), Canadian Imperial Bank of Commerce (CIBC), Bank of Montreal (BMO), Scotiabank and the Bank of Canada—who is the primary public operator within the system.⁶³ On the networking side, LVTS relies on SWIFT communications protocol—specifically the SWIFT Secure Internet Protocol Network (SIPN)—to support both domestic and international financial messaging and routing operations, which occurs when Canadian banks or financial institutions

⁶⁰ Filipe Dinis, “Strengthening Our Cyber Defences,” *Payments Canada*, May 9, 2018, <https://www.bankofcanada.ca/2018/05/strengthening-cyber-defences/>.

⁶¹ Bank of Canada, “Regulatory Oversight Of Designated Clearing And Settlement Systems.”

⁶² “Essential Payments Infrastructure: All Our Systems,” *Payments Canada*, last modified 2017, <https://www.payments.ca/about-us/what-we-do>.

⁶³ “High-Value System (LVTS) Participants,” *Payments Canada*, accessed on January 15, 2019, <https://www.payments.ca/our-directories/high-value-system-lvts-participants>.

need to conduct payment transaction services with each other or with foreign entities.^{64 65 66} On the domestic front, the system uses a combination of the LVTS Direct Network and the SWIFT network, which links the Canadian FMI across the country seamlessly.

Although there are many additional components of Canadian FMI beyond LVTS, in terms of oversight, management and technical systems, this transaction infrastructure is a feature of the economy that if disrupted would be strategically damaging to the country's security and prosperity. An example of an additional FMI system important to the Canadian economy is the public-private operated Retail Payment System, formerly referred to as the Automated Clearing Settlement System (ACSS). The ACSS is responsible for processing the vast majority of payments in Canada, clearing and completing nearly 28 million transactions on the average business day in 2017.⁶⁷ This corresponds to about 99% of the daily transaction volume across the country, though it only accounts for 13% of the value being handled in the economy at-large.⁶⁸ This indicates that although LVTS processes only 1% of the transaction and payment traffic in Canada, it handles close to 87% of the total value—which explains the large annual \$50 trillion CAD processing figure previously mentioned. Part of the key transactions that occur through LVTS making it a central system for FMI operations includes wholesale money market lending between banks to meet daily payout or cost obligations, foreign exchange purchases through global markets, and time critical high-sum payments—such as a company needing to guarantee

⁶⁴ National Committee on PKI, "Preliminary PKI Study On Requirements And Comparable Initiatives In Other Countries," Government of Iceland, May 2001, pg. 34, https://www.government.is/media/fjarmalaraduneyti-media/media/Utgefin_rit/KPMG-report.pdf.

⁶⁵ Tom Roberts, "The Impact Of Operational Events On The Network Structure Of The LVTS," *Bank of Canada: Discussion Paper*, August 2011, pg. 2-3, <https://www.bankofcanada.ca/wp-content/uploads/2011/08/dp2011-07.pdf>.

⁶⁶ Canadian Payments Association, "LVTS Rules Overview," *Payments Canada*, August 21, 2017, pg. 1 https://www.payments.ca/sites/default/files/21-Aug-17/lvts_overview_eng.pdf.

⁶⁷ "Retail System: Rules, Standards and Statistics," *Payments Canada*, accessed December 17, 2018, <https://www.payments.ca/about-us/our-systems-and-rules/retail-system>.

⁶⁸ Ibid.

the delivery of funds for a large corporate merger.⁶⁹ Any IT failures within this system would be catastrophic to real-time money markets and the long-term economy, highlighting its position as an important technical enabler of the overall financial system.

FMI Cybersecurity Challenges. When a cybersecurity failure at an individual company or regulatory body threatens an IT asset directly connected to the LVTS or another system at a bank, the implications of that breach could become a core concern for the integrity of the national economy. While this is certainly a worst-case scenario, it is important to recognize the possibility of such an attack to fully understand the strategic risks facing the sector's most important assets. Therefore, this section will aim to demonstrate how a technical vulnerability at an individual institution, and even a single OS or application at that institution, could pose a real threat to the availability and of the overall FMI.

LVTS and SWIFT both utilize unique software and protocols to communicate, log, and process information for the Canadian economy domestically and globally. Each bank or financial institution supporting LVTS and SWIFT networks also utilize in-house or vendor applications to exchange corporate data with the overall system. This interaction is a key attack vector that may be leveraged by malicious actors.⁷⁰ For example, gaining entry into the LVTS software at any one individual bank by compromising a specific corporate IT asset could allow an attacker to manipulate LVTS transaction data, reporting metrics, disrupt management processes and cause delays throughout the entire network. This type of vulnerability was exploited in 2016 when a group of hackers leveraged authentication and network security weaknesses at the Bank of

⁶⁹ Neville Arjani and Darcey McVanel, "A Primer On Canada's Large Value Transfer System," *Bank of Canada*, March 1, 2006, pg. 9, https://www.bankofcanada.ca/wp-content/uploads/2010/05/lvts_neville.pdf.

⁷⁰ Antonino Fazio and Fabio Zuffranieri, "Interbank Payment System Architecture From A Cyber Security Perspective," *Bank of Italy: Questions of Economics and Finance Occasional Papers Series* no. 418 (2018): 8, 17.

Bangladesh to access their national payment system.⁷¹ The Bank had recently implemented an LVTS-type of infrastructure called RTGS to link the country's payment system to the global SWIFT network. As technicians were connecting the new software to the already deployed SWIFT applications and terminals, they had set up a new wireless network that accidentally connected Internet-facing servers with the core systems at the bank.⁷² During this setup process, the technicians failed to properly configure a new switch they had fielded, which allowed traffic from less secure information systems at the Bank to reach what should have been a segmented network where SWIFT and the new RTGS software were situated. The result was financially damaging, as after a year of network reconnaissance and eavesdropping, hackers were able to locate the misconfigurations and find a pathway to deliver malware to the SWIFT and RTGS servers at the Bank.⁷³

Once attackers deployed their tailored malware onto the SWIFT Alliance Access (SAA) application—which creates the technical messages for payment routing through domestic and international financial networks—the malware altered two bytes of data on the SAA's authentication server.⁷⁴ The alteration allowed the malware to bypass any validity checks in the application, which provided the malicious users with authority to conduct a total of 35 SWIFT transactions worth \$951,000,000 USD—though only \$81,000,000 USD was actually transferred.⁷⁵ The stolen money came from the Bank of Bangladesh's account at the New York Federal Reserve, who distributed the funds to multiple accounts around the world. Although this

⁷¹ Peter Bright, "\$1B Bangladesh Heist: Officials Say SWIFT Technicians Left Bank Vulnerable," *ARS Technica*, May 10, 2016, <https://arstechnica.com/information-technology/2016/05/1b-bangladesh-heist-officials-say-swift-technicians-left-bank-vulnerable/>.

⁷² Ibid.

⁷³ Donato Capitella, "Defending SWIFT Payment Systems From Attack," *MWR Security*, May 5, 2017, <https://www.mwrinfosecurity.com/our-thinking/defending-swift-payment-systems-from-attack/>.

⁷⁴ Threat Analysis Team, "SWIFT Systems And The SWIFT Customer Security Program," *MWR Security*, accessed on January 3, 2019, pg. 8, <https://www.mwrinfosecurity.com/assets/swift-whitepaper/mwr-swift-payment-systems-v2.pdf>.

⁷⁵ Ibid.

attack centered on a financial crime, the applications and servers the attackers had compromised would have allowed for manipulation of transaction data registries and system logs, enabling the users to disrupt settling, clearing and payment processes occurring across the country if their objective had been different.

By exploiting the need for LVTS-type of software to have data exchange functionality with both internal banking systems and the more secure and segmented SWIFT applications, the attackers demonstrated how a payment system and an FMI at-large have susceptible IT architectures that face ongoing and active security risks—including in Canada. This risk was reinforced during a 2017 Payments Canada board meeting where new emergency operating conditions were evaluated, which included discussion on network bypassing and re-routing best practices in the event of systemic disruption or total system failure.⁷⁶ Although the impact severity of the Bank of Bangladesh breach is not considered a strategic disruption, it does indicate the possibility for a single institution’s cybersecurity failures to have a cascading financial and IT impact on a national or global payment system.

The Common Vulnerabilities and Exposure (CVE) list maintained by the MITRE Corporation, with the assistance of the U.S. Department of Homeland Security (DHS) and NIST, has a registered entry for a CGI Group Inc. software product—Logica HotScan—that directly interfaces with the SWIFT SAA application and other payment system tools.⁷⁷ This vulnerability was discovered in 2012 by security researchers who identified a buffer-overflow flaw in the product, which led to a filing with the CVE database known as CVE-2012-2624. HotScan has a unique plugin for interaction with SWIFT software allowing banks and other financial

⁷⁶ Canadian Payments Association, “LVTS Rule 12: Emergency Conditions,” *Payments Canada*, April 24, 2017, pg. 4-5, https://www.payments.ca/sites/default/files/lvts_rule_12_eng.pdf.

⁷⁷ MITRE Corporation, “CVE-2012-2624,” Common Vulnerabilities and Exposure Database, May 11, 2012, <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2012-2624>.

institutions to automatically scan different types of payment messages for compliance and due diligence purposes, particularly for interbank or wholesale payments such as those that traverse Canada's LVTS.⁷⁸ The buffer-overflow vulnerability in the product allows an attacker to input arbitrary or executable code into a data buffer, which is an area of information storage on a computer system. Programs typically take inputted commands and store that data within defined parameters of a given buffer, but malformed or malicious written inputs can result in larger amounts of data trying to be stored in a buffer that does not meet the necessary storage capacity.⁷⁹ The result is data spilling over to adjacent buffers, where other code may be disrupted or new malicious code from the input may be executed by one of the software's programs. In either case, the software's functionality can be disrupted or even altered to conduct new damaging behaviors as a result of the overflow attack.⁸⁰

A 2017 operational assessment of the LVTS conducted by Payments Canada, titled "LVTS Rules Overview," specifically notes that CGI Group Inc. is a key software and central system vendor for the payment infrastructure in Canada.⁸¹ ⁸² Further, key services offered in the HotScan product suite are implemented across multiple banks and different financial services in the country, highlighting how a single company's software vulnerability can result in cybersecurity risk to the Canadian FMI at-large.⁸³ Although the CVE database indicates that the programming flaw was fixed, it took at least 34 days for the patch to be released post-discovery,

⁷⁸ "CGI HotScan Watch List Filtering," *CGI Group Inc.*, February 2016, pg. 1-2, https://www.cginederland.nl/sites/default/files/files_nl/brochures/cgi-nl_brochure_hotscan-watch-list-filtering_2017-04-11.pdf.

⁷⁹ Maragaret Rouse and Michael Cobb, "Buffer Overflow," *TeachTarget: Search Security*, last modified September 2016, <https://searchsecurity.techtarget.com/definition/buffer-overflow>.

⁸⁰ *Ibid.*

⁸¹ Canadian Payments Association, "LVTS Rules Overview," 2-3.

⁸² Banking and Capital Markets Division, "Supporting The Entire Payments Value Chain," *CGI Group Inc.*, last modified January 2019, <https://www.cgi.com/en/banking-capital-markets/cross-banking-capabilities/payments>.

⁸³ Consulting Canada News Desk, "CGI Announces Blockchain And Cybercrime Solutions For Banks," *Consulting Canada*, November 22, 2018, <https://www.consulting.ca/news/683/cgi-announces-blockchain-and-cybercrime-solutions-for-banks>.

meaning the vulnerability resided on national systems for an extended period of time.⁸⁴ An International Monetary Fund (IMF) report from 2015 assessing the resiliency of Norway’s FMI and the equivalent of their LVTS noted that, “Software errors have been found to be very time-consuming to locate and correct, and could serve as a single point of failure if not properly resolved or mitigated.”⁸⁵ The report adds that key challenges to updating these core FMI systems is that the software is often developed by third-parties who have their own policies and timelines for patch management, which could result in critical time delays for correcting a vulnerability or bug during a system failure. Although the Canadian LVTS among other national systems often have secondary and even tertiary backup IT infrastructure with dedicated off-site data management systems, an underlying issue with the core OS and a slow patch process could pose a threat to backup operations as well.⁸⁶

The vulnerabilities assessed in this section, such as those associated with an individual piece of software or the product of a single company—HotScan and SAA respectively—highlight that seemingly small-scale cybersecurity failures can enable attackers to access important data and systems essential to the nationwide financial infrastructure. The Chief Operating Officer (COO) of Payments Canada, Filipe Dinis, reinforced this point in 2018 when he stated that, “One area that we are concerned about is the growing operational risk from third-party providers such as the concentrated set of firms that provide many of the new technologies to the financial sector. Reliance on these same third parties and the interconnections between institutions could pose a systemic risk to the financial system. Greater coordination is essential

⁸⁴ Anil Pazvant, “Buffer Overflow Vulnerability On Logica HotScan SWIFT Alliance Access Interface,” *SecLists: Vendor Patches*, October 9, 2012, <https://seclists.org/bugtraq/2012/Oct/50>.

⁸⁵ Financial Sector Assessment Team, “Oversight And Supervision Of Financial Market Infrastructures, And Selected Issues In The Payment System,” *International Monetary Fund (IMF) Country Report* 15, no. 254 (2015): 21.

⁸⁶ Arjani and McVanel, “A Primer On Canada’s Large Value Transfer System,” 11.

for addressing this issue.”⁸⁷ His comments go on to add that many security testing and management services provided by these vendors fall outside of the oversight of LVTS regulators, which forces the system as a whole to depend and trust on the traditionally less rigorous cybersecurity standards and practices of third parties. It is worth noting that Payments Canada aims to launch their new LVTS infrastructure (Lynx) beginning in 2020, where CGI among other vendors will continue playing critical roles in supporting IT and routing systems between the banks—including with partners such as SWIFT.⁸⁸ This means that the involvement of private sector IT vendors, companies and products will continue acting as a central role in supporting the Canadian FMI, indicating that cyber risk will remain and likely grow across this critical infrastructure sector.

The last portion of this section will highlight Distributed Denial of Service (DDoS) attacks as an example of a non-strategic but growing risk. Due to their routine occurrence at financial and banking institutions around the world, it is important to recognize DDoS activity as another increasingly relevant threat to FMI operations and systems. For example, DDoS attacks do not necessarily threaten the functionality of the overall FMI or pose a systemic threat to the national economy, but they do threaten the availability of the FMI for the retail customer and consumer base in Canada. A 2013 DDoS attack targeting Canada’s TD Bank is an example of such an occurrence where customers trying to access their online banking portals lost access to primary services.⁸⁹ This event was significant for the bank itself and for thousands of clients, but

⁸⁷ Filipe Dinis, “Strengthening Our Cyber Defences,” *Payments Canada*.

⁸⁸ “Payments Canada Initiates Procurement Of Canada’s New Core Clearing And Settlement System—Lynx,” *Payments Canada*, April 26, 2017, <https://www.payments.ca/about-us/news/payments-canada-initiates-procurement-canada’s-new-core-clearing-and-settlement-system>.

⁸⁹ Michael Lewis, “TD Bank Hit By Cyber Attack,” *The Star*, March 21, 2013, https://www.thestar.com/business/2013/03/21/td_bank_hit_by_cyber_attack.html.

it certainly did not threaten the integrity of the FMI or pose a strategic risk to Canada and other financial institutions.⁹⁰

A DDoS attack is a malicious attempt to disrupt normal traffic flowing towards server, applications or networks.⁹¹ The attackers use malware to infect large numbers of computer or Internet-linked devices to form a botnet, which is then controlled and directed to flood traffic towards a specific target—such as a web server responsible for operating a bank’s website or customer portal. Banks tend to have a large externally facing Internet presence due to their daily interactions with customers, which makes them particularly susceptible to a DDoS operation.⁹² Therefore, it is important to recognize this attack vector as a growing threat to the FMI considering the scale of attacks are growing in addition to the number of institutions that could be targeted during one synchronous operation.

In February of 2018, three international banks based in the Netherlands experienced a coordinated DDoS attack disrupting mobile banking accessibility for over three days.⁹³ In 2012, six major U.S. banks, including Bank of America, JP Morgan Chase, U.S. Bancorp, Citigroup and PNC Bank, faced a highly coordinated and persistent DDoS attack that lasted over a month—completely disrupting certain client services for extended periods of time.⁹⁴ These examples of DDoS sophistication and breadth indicate that a shift in their attack impact is occurring, where financially and administratively damaging operations are beginning to pose a direct strategic challenge. Other evolving threats also exist, such as cyber attacks targeting the

⁹⁰ Harold Gallagher, Wade McMahon and Ron Morrow, “Cyber Security: Protecting The Resilience Of Canada’s Financial System,” *Bank of Canada* 7, no. 14 (2014): 49-50.

⁹¹ CloudFlare, “What is a DDoS Attack?” *CloudFlare: Learning Solutions*, accessed January 7, 2019, <https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/>.

⁹² Lewis, “TD Bank Hit By Cyber Attack.”

⁹³ Dan Gunderman, “Incident Of The Week: DDoS Attack Hits 3 Banks Simultaneously,” *Cyber Security Hub*, February 2, 2018, <https://www.cshub.com/attacks/news/incident-of-the-week-ddos-attack-hits-3-banks>.

⁹⁴ Lucian Constantin, “DDoS Attacks Against U.S. Banks Peaked At 60 Gbps,” *CIO Insider*, December 13, 2012, <https://www.cio.com/article/2389721/security0/ddos-attacks-against-us-banks-peaked-at-60-gbps.html>.

over 18,000 Automated Teller Machines (ATM) across the country or the information systems supporting the Toronto Stock Exchange (TSX).⁹⁵ These types of attacks may induce short term—and in the case of TSX, possibly long-term strategic—credit issues in the economy, a loss of confidence in investment and pose branding, public image and monetary risks for individual companies.

Non-industrial IT environments will have different technical challenges for different critical infrastructures, though a general reliance on core systems interacting with public-private stakeholders nationwide is consistent across all sectors. Whether the LVTS for the financial sector, common wireless networks for the telecommunications sector or synchronized national databases for patients across the healthcare sector, disruptions to these IT assets at a national scale poses severe short and long term risks to the country. Although this section focused on a financial industry case study and the unique technical challenges the FMI must address, every other non-industrial IT landscape will also have their own unique cybersecurity issues—such as the rapidly growing presence of IoT devices in the healthcare sector and in the food supply chain. By highlighting the technical impact breaches and compromises can induce on the financial system, this section has demonstrated that critical infrastructure cybersecurity is a strategic issue equally important to mitigate in the non-industrial IT environment compared to the more commonly analyzed industrial control environment.

⁹⁵ Gendron and Rudner, “Assessing Cyber Threats To Canadian Infrastructure,” 16.

EMERGING IT SYSTEMS AND NEW CYBER RISKS

New technologies in the processing, networking and data management space are changing how critical infrastructure is operated and managed. These changes are not only having an impact on how stakeholders interact with important assets, but they are also having a security impact. For example, sector operators, owners and regulators in both industrial and non-industrial environments are shifting to outsourced cloud architectures for uptime and cost benefits, but at the same time, these stakeholders are recognizing security risks such as not knowing where data is being stored or which external parties have administrative access to critical systems. Although the risks associated with new data and computing technologies are causing issues for both the infrastructure community and more traditional organizations simultaneously, there are some unique challenges that non-infrastructure stakeholders will not need to mitigate—at least not with the same urgency. The key technologies that this chapter will discuss includes SDN, NFV, 5G, IoT and cloud computing. Although only a few examples and applications of these technologies will be analyzed, the chapter will sufficiently demonstrate that new IT processes are creating issues current infrastructure cybersecurity policy and tools are not equipped to address.

Software-Defined Networking (SDN) and Cloud Computing

Software-Defined Networking (SDN) is an emerging trend that is transforming how networking software and hardware are managed—not only in the telecommunications industry but also for the standard business environment. SDN is an approach to network management that allows administrators to have a more holistic and accurate view of a network's assets and

operations.⁹⁶ A key component of this approach is enabling the operator to have access to a centralized interface to control and shape the network in real-time.⁹⁷ As opposed to continuously deploying and reconfiguring a wide-array of connected hardware, SDN allows for a virtual infrastructure to provide a more flexible traffic, bandwidth and patch management system. Network Functions Virtualization (NFV) has facilitated this trend by allowing traditionally hardware-based operations and equipment to become digital.⁹⁸ This has included firewalls, traffic load balancers and other non-customizable hardware devices becoming virtual machines instead of physical machines. For the ICT sector specifically, these technologies are allowing Internet Service Providers (ISP) and Communication Service Providers (CSP) to improve how their data centers, hardware backbones and central management systems interact and function on a daily basis. As of 2018, a large telecommunication provider in Canada, Bell Inc., began deploying NFV and SDN tooling to accelerate its network transformation, highlighting that this shift is already occurring across the country.⁹⁹

In addition to the ICT sector, SDN and NFV are transforming IT operations throughout other critical infrastructure environments. While this has provided operational benefits, these new networking systems are also introducing new cybersecurity challenges into already vulnerable assets. For example, the U.S. President’s National Security Telecommunications Advisory Committee (NSTAC) developed a report in 2017 noting that, “SDN/virtualization

⁹⁶ “What’s The Difference Between Cloud Computing And Software Defined Networks (SDN)?” *QuoteColo*, December 8, 2015, <https://www.quotecolo.com/whats-the-difference-between-cloud-computing-and-software-defined-networks-sdn/>.

⁹⁷ *Ibid.*

⁹⁸ National Security Telecommunications Advisory Committee, “NSTAC Report To The President On Emerging Technologies Strategic Vision,” *Department of Homeland Security*, July 14, 2017, pg. 11, <https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Emerging%20Technologies%20Strategic%20Vision.pdf>.

⁹⁹ Sean Buckley, “2018 Preview: Network Automation Will Take Hold In Operator Networks,” *Fierce Telecom*, December 29, 2017, <https://www.fiercetelecom.com/telecom/2018-preview-network-automation-takes-hold-operator-networks>.

requires the existence of more software than previous security solutions, and software may present more opportunity for bugs or malware to be introduced into the environment.”¹⁰⁰ The report also added that, “Given the centralization of control with SDN, there is increased risk that if the central controller has a software vulnerability issue, then the impact could be dispersed across the entire network.”¹⁰¹ The NSTAC comments essentially highlight that the very flexibility offered by SDN/ NFV to network managers will create a centralized control node that could be exploited by attackers to cause widespread damage at a rapid rate.

During a telecommunications conference in March of 2017, John Stratton, a co-chair of NSTAC’s Emerging Technologies Strategic Vision Subcommittee, noted that, “The Department of Homeland Security should begin to plan strategically for how SDN could affect critical infrastructure, and modify its cybersecurity guidance to accommodate SDN’s impact.”¹⁰² Risks are also apparent from a more technical perspective. For example, increased reliance on NFV and networking protocols will mean that traditionally single-tasked hardware devices are now going to be replaced with virtual machines conducting a wide-range of complex activities. On a standard network switch, router or firewall, these activities were typically designated to an application-specific integrated circuit (ASIC)—such as a data packet processor.¹⁰³ An ASIC is a very effective, hardened and tailored device built for one primary network function.¹⁰⁴ Moving these tasks to a software-based system will significantly increase the risk and potential impact of DDoS attacks, which are significantly more capable of overwhelming an ordinary central processing unit (CPU) supporting common software compared to a traditional hardware device

¹⁰⁰ National Security Telecommunications Advisory Committee, “NSTAC Report To The President,” 15.

¹⁰¹ *Ibid.*

¹⁰² Mark Rockwell, “SDN Looms Large In NSTAC Report,” *FCW: Cybersecurity Desk*, March 3, 2017, <https://fcw.com/articles/2017/03/03/sdn-nstac.aspx>.

¹⁰³ Avi Dorfman, “Four Cyber Security Threats On NFV Networks,” *Telco Systems*, August 10, 2016, <http://www.telco.com/blog/four-cyber-security-threats-on-nfv-networks/>.

¹⁰⁴ *Ibid.*

with dedicated ASICs.¹⁰⁵ Different types of DDoS attacks would be highly effective in increasing traffic loads and compromising the functionality of these software-dependant networks, highlighting how attackers looking to disrupt newly linked emerging and legacy technologies could leverage classic exploitation techniques.

SDN and NFV are emerging trends that have grown alongside the ongoing shift to cloud-based IT architectures. The cloud is a backbone computing infrastructure that allows customers to deploy their software and hardware assets in a data center maintained, supported and monitored by a third-party provider.¹⁰⁶ Customers can remotely create virtual machines within designated digital space in the data center and could also alter the number, interaction and configuration of these machines using a control interface—which is typically referred to as a hypervisor.¹⁰⁷ Cloud computing provides governments, companies and organizations with powerful computing systems at reduced cost, increased performance and rapid scalability. Critical infrastructure stakeholders are becoming increasingly attracted to these cost and operational benefits, indicating that the country’s most vital systems will likely be introduced to new cloud-based security risks moving into the future.

DHS released an information package in 2017 titled “Risks to Critical Infrastructure That Use Cloud Services.”¹⁰⁸ The package not only highlights that U.S. critical infrastructure owners, operators and vendors are increasingly shifting their IT presence from local environments to both hybrid and completely cloud based environments, but also that a range of new security

¹⁰⁵ Dave Larson, “SDN And NVF: Blessing Or A Curse For DDoS Security?” *Corero: Network Security Trends*, September 20, 2016, <https://www.corero.com/blog/761-sdn-and-nvf-blessing-or-a-curse-for-ddos-security.html>.

¹⁰⁶ John Hales, “Comparing SDN, NFV And Cloud Computing,” *Global Knowledge*, August 14, 2014, <https://www.globalknowledge.com/blog/2014/08/14/comparing-sdn-nfv-and-cloud-computing/>.

¹⁰⁷ *Ibid.*

¹⁰⁸ Office of Cyber and Infrastructure Analysis, “DHS Guide: Risks To Critical Infrastructure Using Cloud Services,” *Department of Homeland Security*, March 2017, <https://info.publicintelligence.net/DHS-OCIA-InfrastructureCloudRisks.pdf>.

challenges are emerging as a result. Similar shifts are also occurring across Canada, with public and private stakeholders leveraging cloud architectures for different purposes and processes.¹⁰⁹ The DHS document notes that, “Although cloud services and physical information technology infrastructures are vulnerable to some common attack vectors, such as Denial of Service attacks, cloud services are also potentially vulnerable to a number of unique attack vectors such as Hyperjacking.”¹¹⁰ Considering the previous chapter identified some different attack vectors and techniques an actor could use to infiltrate current and legacy IT systems across different sectors, it is worth identifying some unique new threats that specifically impact cloud computing.

Hyperjacking is a type of attack where a malicious actor will aim to compromise a virtual environment’s hypervisor, which is essentially the software that manages virtual machines on the physical hardware in a data center.¹¹¹ This can include an actor taking over remote root control of the hypervisor or the installation of a rogue hypervisor. If an actor could compromise this central and underlying management software, they would be able run undetectable programs below the OS of different virtual machines on the cloud.¹¹² The sensitive information held on these compromised applications and servers could be maliciously altered or disrupted, meaning an entire organization’s data could be at risk. Dimitri McKay, a Senior Security Architect and Systems Engineering Expert with Splunk Inc. refers to hypervisor compromises as a, “Single point of failure in security.”¹¹³ New attack techniques, such as hyperjacking, are creating significant risks to all industries and organizations who move IT operations to a cloud

¹⁰⁹ Goran Novkovic, “Cloud Computing For Utilities In Canada – Present And Future,” *LinkedIn Publications*, August 22, 2018, <https://www.linkedin.com/pulse/cloud-computing-utilities-canada-present-future-peng-pmp>.

¹¹⁰ Office of Cyber and Infrastructure Analysis, “DHS Guide: Risks To Critical Infrastructure Using Cloud Services.”

¹¹¹ “When Hackers Target Your Hypervisor,” *NexiiLabs*, April 16, 2017, <http://nexiilabs.com/blog/when-hackers-target-your-hypervisor/>.

¹¹² Dimitri McKay, “A Deep Dive Into Hyperjacking,” *Security Weekly*, February 3, 2011, <https://www.securityweek.com/deep-dive-hyperjacking>.

¹¹³ *Ibid.*

environment, though any type of vulnerability that results in a single point of failure is particularly concerning for critical infrastructure stakeholders due to their customer's dependencies.

Another vulnerability unique to cloud environments relates to multi-tenancy or the norm of having shared physical and virtual computing space within data centers where multiple organizations have assets. Although a cloud computing environment allows tenants to have cost-effective on-demand scaling options, it also enables Side-Channel attacks.¹¹⁴ A Side-Channel attack exploits the physical co-residency of virtual machines.¹¹⁵ If an attacker has access to a malicious virtual machine operating on the same physical hardware as a target virtual machine, the attacker can measure circuitry heat, electromagnetic emissions and processing time on the hardware to gather information about the cryptographic encryption keys being used by a certain computer process on the target's machine or server.¹¹⁶ After enough analysis, the attacker can leverage the collected signature information to disturb the process or break into the targeted data. This highly technical vulnerability is unique in cloud environments due to the common overlap of customer data and processes on shared hardware assets. As critical infrastructure IT systems continue shifting to cloud-based operations, executives and security teams need to ensure that the proper controls or mitigation techniques are in place to address this threat.

The vulnerabilities and challenges assessed in this section highlight the active security risks SDN, NFV and cloud computing deployments will pose for any industrial and non-industrial critical infrastructure sector seeking to utilize these technologies without updated cybersecurity practices. Ensuring that policy and strategy address these risks in addition to the

¹¹⁴ Rambus Public Press Team, "An Introduction To Side-Channel Attacks," *Rambus*, May 24, 2018, <https://www.rambus.com/blogs/an-introduction-to-side-channel-attacks/>.

¹¹⁵ *Ibid.*

¹¹⁶ Younis A. Younis, "Securing Access To Cloud Computing For Critical Infrastructure," (PhD thesis, Liverpool John Moores University, 2015), 32.

legacy IT vulnerabilities explored in the previous chapter will be essential mitigating the cyber threats to critical infrastructure in Canada moving into the future.

5G and Internet of Things (IoT)

5G is the next generation of broadband Internet connection and it will enable much faster network speeds with greater data carrying and relaying capacity relative to previous wireless networks. Although the actual national Internet and communication backbone in Canada will undergo a long transformation process to actually build-out the 5G networks, private organizations will begin to deploy local 5G networks much sooner.¹¹⁷ There are numerous technical reasons why 5G will have transformative impacts across multiple infrastructures in Canada, but a key feature is reduced latency and the enabling of a range of new processes and technologies that are not possible over 4G networks.¹¹⁸ For example, autonomously driving vehicles will be able to meet the near-instantaneous needs of inter-vehicle-to-vehicle communications, revolutionizing the Transportation infrastructure. Dr. Joy Laskar, co-founder and Chief Technology Officer of Maja Systems, provides a useful reference for understanding the speed of 5G networks relative to current technology by noting that, “With an advanced Wi-Fi connection, it would take 230 days to transfer a weeks-worth of data from a self-driving car.”¹¹⁹ Without the speeds and data capacities of 5G networks, certain technologies will simply not be scalable. Another example of 5G’s impact relates to how telemedicine (or eHealth) can become a more practical solution for expanding the reach of Healthcare infrastructure, as faster real-time

¹¹⁷ Jerry Hildenbrand, “What Is 5G Technology?” *Android Central*, last modified February 9, 2019, <https://www.androidcentral.com/what-5g>.

¹¹⁸ Marry-Ann Ruson, “Will 5G Be Necessary For Self-Driving Cars?” *BBC*, September 27, 2018, <https://www.bbc.com/news/business-45048264>.

¹¹⁹ Bijan Khosravi, “Autonomous Cars Won't Work - Until We Have 5G,” *Forbes*, March 26, 2018, <https://www.forbes.com/sites/bijankhosravi/2018/03/25/autonomous-cars-wont-work-until-we-have-5g/#7f0ab85b437e>.

robotic and visual controls will offset the Internet-delays experienced over vast distances during remote treatments, invasive surgeries, operations or scans/ tests.

Perhaps most importantly, 5G will enable the growth and application-at-scale of IoT devices. Having the capacity to manage more connectivity and data will allow for a dramatic increase in Internet-connected processes and systems across consumer, business, infrastructure, and government industries.¹²⁰ As this increase in connectivity occurs with 5G networks and IoT device deployment, multiple sectors will also need to address new cybersecurity challenges. For example, IoT developments will lead to larger botnet and DDoS attacks, creating new risks for all critical infrastructure entities with externally facing systems. This issue has been recognized across the energy sector specifically, where the linking of sensors and small computing or signaling devices across pipelines, drilling sites, field equipment and transport vehicles has become standard practice. Phil Neray, Vice President of industrial cybersecurity at a security firm in Boston called CyberX, noted in October 2018 that, “To reduce costs and optimize operations, oil and gas companies are deploying more and more IoT sensors so they can closely track flows and data related to production operations. This has resulted in increased connectivity between IT and operational networks, which has increased the attack surface and hence the risk.”¹²¹ The same IoT deployments are occurring across Canadian natural gas and oil distribution infrastructure, which has been evident with Canada’s largest telecommunication and Internet provider—Rogers Communications Inc.—restructuring its specialized IoT subscription services to meet growing energy sector demands.¹²²

¹²⁰ National Security Telecommunications Advisory Committee, “NSTAC Report To The President,” 22.

¹²¹ Natalie H. McDonald, “Are Our Nation’s Oil And Gas Pipelines Safe From Cyber-Attack?” *CompTIA*, October 24, 2018, <https://www.comptia.org/about-us/newsroom/blog/comptia-blog/2018/10/24/are-our-nation-s-oil-and-gas-pipelines-safe-from-cyber-attack>.

¹²² Eric E. Wood, “Rogers To Support IoT Networks, Oil And Gas, Food Industries With New Services,” *IT World Canada*, April 6, 2016, <https://www.itworldcanada.com/article/rogers-to-support-iot-networks-oil-and-gas-food-industries-with-new-services/382129>.

There are a several technical cybersecurity challenges associated with IoT devices that will have unique impacts across the industrial IT environments in Canada. For example, many devices that will perform a single-task—such as monitoring gas flow through a pipe—have very small amounts of processing power and memory, which leaves little storage room for security programming or functionality.^{123 124} Another impact of small storage and processing capacity is reduced ability to receive secure software patches, as certain interconnected IoT devices will be unable to manage encrypted data in transit.¹²⁵ This can provide attackers with an opportunity to intercept, alter and add malicious code to over-the-air (OTA) updates being sent to IoT devices. Once the update is installed and the payload of the malware operationalized, the device will be compromised. In addition to encryption issues, another challenge with IoT patch management is that many devices contain an underlying OS that is simply not capable of being updated after being deployed in the wild. These devices may even be cheaper to physically replace than actually patch.¹²⁶ However, since IoT devices in the industrial space tend to be geographically dispersed and in hard to reach places, the products are and will continue to be routinely operated beyond their end-of-life date. This leads to a build-up of vulnerabilities overtime and the accumulation of significant IT risk across the industrial enterprise.^{127 128} While adding 5G enabled IoT technologies to the SCADA and ICS environment will certainly offer increased oversight, monitoring and management capabilities, new patch management challenges—rooted

¹²³ Nermin Hajdarbegovic, “Are We Creating An Insecure Internet of Things (IoT)?” Security Challenges and Concerns,” *Top Tal*, February 2016, <https://www.toptal.com/it/are-we-creating-an-insecure-internet-of-things>.

¹²⁴ Roman Garber, “What Makes IoT Security So Tough?” *DZone*, June 11, 2018, <https://dzone.com/articles/what-makes-iot-security-so-tough>.

¹²⁵ Xu Zou, “IoT Devices Are Hard To Patch: Here’s Why—And How To Deal With Security,” *Tech Beacon*, accessed on January 19, 2019, <https://techbeacon.com/security/iot-devices-are-hard-patch-heres-why-how-deal-security>.

¹²⁶ Hajdarbegovic, “Are We Creating An Insecure Internet of Things (IoT)?”

¹²⁷ *Ibid.*

¹²⁸ Eric Rogge, “Why IoT And Not SCADA?” *Eckerson Group*, September 23, 2015, <https://www.eckerson.com/articles/why-iot-and-not-scada>.

in encryption, processing or other variables—will simply exacerbate the security issues already stressing legacy IT equipment throughout Canadian infrastructure.

It is important to note that supply chain risk is a key technical and policy-based vulnerability emerging from the deployment of 5G networks in Canada. Government and industry stakeholders across Canada are currently debating potential risks emerging from the use of 5G technologies associated with foreign owned enterprises, such as China’s telecommunication giant Huawei and chip manufacturer ZTE. In January of 2019, U.S. Senator Mark Warner stated that, “Our telecom networks are totally meshed together and if there was a vulnerability in the Canadian system, it would make America vulnerable. And vice-versa.”¹²⁹ He added that, “My specific concerns are particularly as we move into the next generation of wireless—the so-called 5G networks—that if a country were to purchase this equipment, it might have built-in backdoors so that, down the line, once the equipment was installed, the Chinese could intercept messages, communications and violate the security of the networks.”¹³⁰ The prospect of a backdoor in the ISP and national communication backhaul infrastructure would be a cybersecurity vulnerability of unprecedented scale, posing a strategic risk to multiple sectors across Canada and raising the prospect of widespread intellectual property (IP) theft. It is significant, however, that there is technical disagreement around the practicality and capability of embedding malware or using malformed firmware on hardware products being delivered as part of Chinese 5G equipment, and that ongoing hardware and software investigations are not necessarily consistent with Warner’s claims.

¹²⁹ Juan P. Tomas, “U.S. Senator Warns About The Use Of Huawei Gear In Canada’s 5G Networks.” *RCR Wireless News*, January 7, 2019, <https://www.rcrwireless.com/20190107/5g/us-senator-warns-about-use-huawei-gear-canada-5g-network>.

¹³⁰ *Ibid.*

Nevertheless, many Canadian allies—including the U.S. Britain, Germany, Japan and Australia—have considered banning Huawei, ZTE and other Chinese telecommunications products.¹³¹ Security researchers at Britain’s Government Communications Headquarters (GCHQ) and from the country’s Huawei Cybersecurity Evaluation Center (HCSEC) have noted in public disclosures that there were instances of unexplainable code in software products and operating issues with 5G-hardware equipment that raised suspicion.¹³² This prompted British security officials to conduct more comprehensive and long-term supply chain investigations. However, in February of 2019, sources from Britain’s National Cyber Security Council (NCSC) acknowledged that a complete ban of Huawei from national telecom networks did not serve a useful cybersecurity purpose.¹³³ Although this contradicts what the council recognized a year earlier, where they emphasized supply-chain issues with Chinese equipment, their new position highlighted that the country’s specialized laboratories—like HCSEC—and national intelligence agencies will be able to mitigate any threats with proactive equipment assessments and risk controls. These new comments stemming from British media and government sources indicate that a select amount of products and services may be banned, but it is unlikely for a comprehensive blanket-based approach to be implemented.

Conversely, Mike Burgess, director-general of the Australian Signals Directorate, led a stronger opposition movement in Australia over the past few years. This was evident by his comments in October of 2018 stating that, “Australia’s critical infrastructure including electricity

¹³¹ Jeremy Horwitz, “U.S. Lobbies Germany, Italy, And Japan To Ban Huawei 5G Equipment,” *Venture Beat*, November 23, 2018, <https://venturebeat.com/2018/11/23/u-s-lobbies-germany-italy-and-japan-to-ban-huawei-5g-equipment/>.

¹³² Jack Stubbs, “UK Government Officials Identify Security Risks With Huawei’s Telecom Equipment,” *Insurance Journal*, July 20, 2018, <https://www.insurancejournal.com/news/international/2018/07/20/495718.htm>.

¹³³ Kanishka Singh and Jack Stubbs, “Britain Does Not Support Total Huawei Network Ban: Sources,” *Reuters*, February 17, 2019, https://www.reuters.com/article/us-britain-huawei-tech-idUSKCN1Q60NR?utm_campaign=trueAnthem:+Trending+Content&utm_content=5c6a2c9d3ed3f000010aa5de&utm_medium=trueAnthem&utm_source=twitter.

grids, water supplies and hospitals could not have been adequately safeguarded if Chinese-owned telecommunications giants Huawei and ZTE Corp. were allowed to help roll out the nation's 5G network."¹³⁴ His statement added that cybersecurity researchers and engineers throughout the intelligence community in Australia had identified these companies and their products as high risk vendors posing an active technical threat to the country's systems—though public release of evidence has yet to occur.

The ICT sector is undergoing rapid change and the growing reliance on 5G networks will continue to deepen cross sector dependencies in Canada. With the majority of critical infrastructure relying on the ICT backbone in some way, developing national cybersecurity policies to address 5G vulnerabilities will continue to be a growing strategic imperative for the government. Steve Buck, COO at a network security company called Evolved Intelligence, reinforced this point in 2018 by stating that, "5G will power critical infrastructure, so a cyber-attack could stop the country."¹³⁵ In addition to forming technical security standards, supply chain policy risks must also be addressed—not just to respond to possible Chinese government-linked issues but to other foreign and domestic threats as well. This is a complex task as new import control mechanisms, IT audit and testing procedures, bill-of-material best practices and approved product list assessments will all need to be implemented and regulated by the federal government.¹³⁶ ¹³⁷ To ensure the country can mitigate these developing risks in a timely manner

¹³⁴ Rod McGuirk, "Spy Chief Wanted Ban On China Telecoms From Australian 5G," *AP News*, October 30, 2018, <https://www.apnews.com/91700da1a9ce43fda41def9d2a3a996d>.

¹³⁵ Matthew Wall, "A Cyber-Attack Could Stop The Country," *BBC*, October 25, 2018, <https://www.bbc.com/news/business-45952693>.

¹³⁶ National Protection and Programs Directorate, "DHS And Private Sector Partners Establish Information And Communications Technology Supply Chain Risk Management Task Force," *Department of Homeland Security*, October 30, 2018, <https://www.dhs.gov/news/2018/10/30/dhs-and-private-sector-partners-establish-information-and-communications-technology>.

¹³⁷ National Protection and Programs Directorate, "DHS Announces ICT Supply Chain Risk Management Task Force Members," *Department of Homeland Security*, November 15, 2018, <https://www.dhs.gov/news/2018/11/15/dhs-announces-ict-supply-chain-risk-management-task-force-members>.

and to maintain similar standards with international allies, Ottawa should prepare—at least conceptually—for how resources will be allocated and which public-private partnerships will be needed for a national 5G supply chain risk management project to succeed.

It is equally important to recognize the closely linked IoT vulnerabilities and risks—previously referenced in this section—that are directly emerging as a result of the new capacity and network speeds of 5G. Dave Burstein, a 5G expert with Wireless One Inc., highlights that, “The problem is that a lot of these IoT devices, think small sensors measuring air humidity or temperature, for example, are cheap and need to have a very long battery life. Implementing good security into such devices will require more processing power and this drives up costs and drains power, which is why it won't happen.”¹³⁸ The operational requirements of certain IoT devices will limit adequate internal countermeasures, meaning public and private critical infrastructure owner-operators will need to develop and field external security mechanisms to mitigate this area of growing cyber risk and IT exposure. Altogether, 5G and IoT technologies, in addition to SDN, NFV and cloud computing, will reshape how individuals, businesses, infrastructure and the government will operate and interact on a daily basis. This transformation will provide many functional and cost benefits, but it will simultaneously introduce unique security challenges and vulnerabilities that may provide adversaries with a strategic advantage over Canada.

¹³⁸ Wall, “A Cyber-Attack Could Stop The Country.”

MAPPING CANADA'S CYBER THREAT LANDSCAPE

There are a variety of threat actors with different levels of technical sophistication, funding, motives and objectives interested in exploiting cyber vulnerabilities in Canada's critical infrastructure. Many of these actors are associated with foreign intelligence agencies and even military computer security groups, while others are linked with international terrorist communities or domestic political extremists. This chapter will identify different individuals, groups or nations who have expressed interest in or have conducted activities consistent with cyber attack on critical infrastructure in Canada or against like-minded allies. Many adversaries, including Iran and China, have demonstrated their ability to infiltrate the information systems supporting different critical infrastructure sectors throughout the world. Although it is highly unlikely that any nation-state would seek to disrupt an essential service in Canada during peacetime, many governments continue to compromise IT assets before conflict for economic purposes or to conduct network reconnaissance and map out possible attack vectors for the future should hostilities arise. This reinforces the need for constant cyber defense at any given geopolitical condition. Further, since non-state actors, such as terrorist groups, could attack during peacetime or conflict, it becomes clear that Canada's critical infrastructure faces disruptive threats on an ongoing consistent basis. By discussing topics such as cyber warfare and cyber terrorism, in addition to analyzing the shift of the cyber domain to being labeled as not just an enabler but also an actual warfighting environment, this chapter will address the issue of Canadian infrastructure being targeted by some of the most advanced cyber actors in the world.

It is also important to recognize that the highly advanced tools and TTPs needed to disrupt infrastructure in Canada may make it difficult for terrorist or hacktivist groups and even

individuals relative to nation-states to conduct a successful cyber attack. However, failing to recognize a threat actor simply due to a lack of technical know-how or resources can lead to gaps in cybersecurity programs, strategy and policy, as that same actor could outsource an operation or develop a capability over time. In addition to nation-state cyber warfare and terrorist group threats, this chapter will also highlight risks emanating from catastrophic IT accidents, insider threats, and espionage. Although a general high-level cyber threat assessment for Canada would also include a range of criminal organizations and individual hackers interested in money laundering, fraud, identity theft and other cyber-enabled crimes, these types of threats do not fall within the scope of actors explicitly targeting critical infrastructure for strategic security or financial purposes impacting the national wellbeing—though this chapter will highlight an exception for intellectual property (IP) theft. Therefore, the focus of this chapter will be on the motivations, technical sophistication and past activities of adversarial state, non-state, foreign and domestic actors who have demonstrated a capability or intent to disrupt critical IT systems supporting the country's most important systems.

Nation-States, Advanced Persistent Threats (APT) and Cyber Warfare

The proliferation of Internet-connected technologies and the reliance on cyberspace to facilitate data and communication networks has resulted in governments, foreign intelligence agencies and militaries around the world funding, researching and deploying offensive and defensive cyber capabilities. The national security policy of most advanced countries now includes some form of cyber strategy, with many supporting the creation of tactical and strategic warfighting doctrines, and defensive countermeasures, in the cyber domain. A comprehensive list maintained by the Center for Strategic and International Studies in Washington, D.C.

identifies that 78 nations have publically released a national military cyber strategy specifically outlining threats, requirements and operational objectives.¹³⁹ Canada has followed this trend with the release of the “National Cyber Security Strategy” in 2018, which calls for developing the Canadian government and military’s use of cyberspace and the need to address a range of threats—including state and state-sponsored hackers.¹⁴⁰

There are several other indications that Canada has recognized and initiated a response to the growing threat of major cyber conflict. For example, the Canadian Armed Forces (CAF) launched a new Cyber Operations Unit in 2018 tasked with computer network attack and defense responsibilities in addition to growing the scope of the military’s Directorate of Cyber Operations Force Development.¹⁴¹ A public statement from the Royal Canadian Navy in 2018 also mentioned that the CAF was undergoing a national cyber exercise, which was referred to as Exercise Cyber Challenge (ECC).¹⁴² The ECC referenced cyberspace as an operational military domain, reinforcing the CAF’s efforts to develop, test and field a range of capabilities for both pre-conflict environments and active hostilities. These efforts are being undertaken in coordination with other partners, such as the Communications Security Establishment (CSE), who is the country’s cryptographic and signals intelligence agency. On the defensive side, the CAF in partnership with Public Safety Canada is working to implement the “Integrated Defense Plan 2018-2023”, which specifically highlights the joint military-government role to, “Protect

¹³⁹ Technology Policy Program, “Global Cyber Strategies Index,” *Center for Strategic and International Studies*, last modified 2019, <https://www.csis.org/programs/technology-policy-program/cybersecurity-and-governance/global-cyber-strategies-index>.

¹⁴⁰ “National Cyber Security Strategy,” *Public Safety Canada*, pg. 5, June 12, 2018, <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/ntnl-cbr-scrtr-strtg/index-en.aspx>.

¹⁴¹ Department of National Defense, “DND/CAF Welcomes First Cyber Operators,” *The Maple Leaf: Defense News*, last modified January 8, 2018, <https://ml-fd.caf-fac.ca/en/2018/01/9092>.

¹⁴² Royal Canadian Navy, “Exercise Cyber Challenge 2018,” *RCN News and Operations*, May 7, 2018, <http://www.navy-marine.forces.gc.ca/en/news-operations/news-view.page?doc=exercise-cyber-challenge-2018/jgb8kpna>.

Canadians and our critical infrastructure from cyber threats.”¹⁴³ Although the CAF deals with a range of tactical issues as well, such as forward unit cyber capabilities in conflict zones and theater-level communication security (COMSEC), this section will only focus on the high-level threats that nation-state cyber warfare, competition and conflict poses to the civil safety of the country and critical infrastructure as a whole.

As Canada continues to grow its military and government presence in the cyber domain, foreign adversaries have done the same and have specifically emphasized critical infrastructure as a priority target. Countries such as China, Russia, Iran and North Korea are actively scanning and exploiting vulnerabilities across the Canadian business, non-profit and government landscape to enable operations at a later date—such as after hostilities initiate. Often, these countries will distribute the cyber tools their intelligence or military forces have developed to private or state-sponsored hacking groups, creating a political liability barrier between the cyber activities of the private group and the orders and objectives disseminating from the government. The 2018 National Cyber Threat Assessment references this challenge in the context of critical infrastructure, noting that, “State-sponsored cyber threat actors will continue to conduct cyber espionage against Canadian businesses and critical infrastructure to advance their national strategic objectives.”¹⁴⁴ An example of this threat was demonstrated in 2013 when an Iranian-linked hacking group, identified as APT33, infiltrated the Ministry of Labour attempting to access Canada’s national Secure Channel Network (SCN).¹⁴⁵ ¹⁴⁶ APT33 is classified as an

¹⁴³ Department of National Defense, “Operating Context And Key Risks,” *DND Departmental Plans: Reports and Publications*, April 16, 2018, <https://www.canada.ca/en/department-national-defence/corporate/reports-publications/plans-priorities/2018-19/supplementary-information/operating-context-and-key-risks.html>.

¹⁴⁴ *Ibid.*

¹⁴⁵ Ben Makuch and Justin Ling, “Iranian Hackers Infiltrated A Canadian Government System,” *Vice News*, July 9, 2015, https://news.vice.com/en_us/article/pa4dxm/iranian-hackers-infiltrated-a-canadian-government-system.

¹⁴⁶ Ben Makuch, “Ottawa Confirms Iranian Hackers Targeted Canadian Systems,” *Vice News*, March 23, 2018, https://news.vice.com/en_ca/article/paxpy7/ottawas-cyberspies-confirm-iranian-hackers-targeted-canadian-systems.

Advanced Persistent Threat (APT), which is a malicious computer attack where a person or group gains unauthorized access to a network and remains undetected for an extended period. The aim of the attack is to patiently map the network for additional vulnerabilities, slowly escalating user privileges or uploading backdoors to enable remote interaction with compromised information systems. APTs have traditionally been associated with nation-state actors due to the significant financial, talent and technical resources that usually support their operations.

Since APT33's espionage operation targeted the SCN, which is a highly secured and encrypted communications system that interacts with many critical infrastructure sectors in Canada, there would have been a significant strategic risk to the country if the hackers successfully escalated their operation.¹⁴⁷ It is important to note the intricate relationship many state-sponsored hacking groups have with their affiliated governments, as this highlights how the country's foreign, geopolitical and strategic objectives in cyberspace are essentially outsourced to private entities. For example, FireEye and a Russian-based cybersecurity firm, Kaspersky Lab, have both released reports detailing the elaborate connections between APT33 and the Iranian government's Nasr Institute.^{148 149} This institute, which is actually a contractor jointly operated by Iran's Islamic Revolutionary Guard Corps (IRGC) and the Basij Cyber Council, has routinely conducted operations directly and indirectly in support of the country's Ministry of Intelligence. Government reports from the U.S. and Israel also indicate that many of the personnel believed to be associated with APT33 have previously worked in other Iranian hacking groups—such as the

¹⁴⁷ Makuch and Ling, "Iranian Hackers Infiltrated A Canadian Government System."

¹⁴⁸ Josiah Kimble, Jacqueline O'Leary and Kelli Vanderlee, "Insights Into Iranian Cyber Espionage: APT33 Targets Aerospace And Energy Sectors And Has Ties To Destructive Malware," *FireEye: Threat Research Team*, September 20, 2017, <https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html>.

¹⁴⁹ Thomas Brewster, "Meet APT33: A Gnarly Iranian Hacker Crew Threatening Destruction," *Forbes*, 20 September 2017, <https://www.forbes.com/sites/thomasbrewster/2017/09/20/iran-hacker-crew-apt33-heading-for-destructive-cyberattacks/#5b5693174a48>.

Nasr Institute—and within the Iranian government itself.¹⁵⁰ When groups such as APT33 target Canada, the threat is not from a group of private individuals but rather a nation-state with a substantial amount of resources and a geopolitical agenda unfavorable to Canadian security.

In addition to Iran, other nation-state adversaries and their contracted affiliates have also demonstrated intent and capability to infiltrate Canadian and allied critical infrastructure networks. This is not only evident by identifying attacks directly impacting Canada, but also by recognizing the cyber activities Canadian adversaries have conducted against partner nations—such as the members in the Five Eyes intelligence alliance or allies like Japan and South Korea. For example, in 2017 after a Chinese-linked attack targeted Australian government systems connected to a defense contractor, the Federal Minister responsible for national cybersecurity policy noted that, “Most concerning, is that these attacks were more elaborate than the attacks we have seen in previous years. It is clear that the malicious actors looking to target major systems and critical infrastructure are increasing the sophistication of their vectors.”¹⁵¹ This came a year before Australia and the U.S. jointly condemned a Chinese hacking group referred to as APT10, who was acting on behalf of the Chinese Ministry of State Security attempting to infiltrate the networks of government and industry stakeholders in at least 12 countries.¹⁵²

Acting Federal Bureau of Investigation (FBI) Director Christopher Wray commented on APT10’s activities, arguing that, “The cyber threats from China, which date back to 2006, have never been more severe or more pervasive. No country poses a broader more severe long term

¹⁵⁰ Levi Gundert, Sanil Chohan, and Greg Lesnewich, “Iran’s Hacker Hierarchy Exposed,” *Recorded Future*, accessed on November 25, 2018, <https://go.recordedfuture.com/hubfs/reports/cta-2018-0509.pdf>.

¹⁵¹ Rafia Shaikh, “Australia Wants To Make Cybersecurity Relevant,” *WCCF Tech*, October 9, 2017, <https://wccftech.com/australia-cybersecurity-relevant-mums-dads/>.

¹⁵² Tara Cosoleto, “Australia Joins Global Condemnation Of Serious China Cyber Hacking,” *SBS News*, December 21, 2018, <https://www.sbs.com.au/news/australia-joins-global-condemnation-of-serious-china-cyber-hacking>.

threat to our nation's economy and cyber infrastructure than China.”¹⁵³ These comments are consistent with China’s creation of the Strategic Support Force (SSF) in 2015, which has now integrated, improved and operationalized the country’s military, commercial and intelligence cyber resources under one branch.¹⁵⁴ Similar recognition of the critical infrastructure risks posed from China and their sponsored affiliates is also apparent in Japan, where a 2017 National Institute of Information and Communications Technology document noted that the majority of the reported critical infrastructure cyber attacks against the country stemmed from Chinese sources—with North Korean APT groups being the second most common source.¹⁵⁵

Within Canada’s closest alliance circles, the U.S. has been the most vocal country in recognizing that advanced Chinese hacking groups, government intelligence agencies, and military units are actively exploiting cybersecurity weaknesses in critical infrastructure for strategic purposes. For example, the 2019 “Worldwide Threat Assessment” developed by the Director of National Intelligence explicitly outlines how China has been targeting the critical infrastructure networks of the U.S. and its allies to support long-term security objectives, short term commercial interests and to gain leverage in the event of major hostilities—kinetic or non-kinetic.¹⁵⁶ The Assessment notes that for many years Beijing has emphasized, “Cyber espionage to collect intelligence and targeted our critical infrastructure to hold it at risk,” adding that, “China has the ability to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks—in the

¹⁵³ Ibid.

¹⁵⁴ Daniel R. Coats, “2018 Worldwide Threat Assessment Of The U.S. Intelligence Community,” *Office of the Director of National Intelligence*, pg. 6, February 13, 2018, <https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf>.

¹⁵⁵ “Cyberattacks Targeting Japan Networks Hit A Record 128.1 Billion In 2016,” *The Japan Times*, February 8, 2017, <https://www.japantimes.co.jp/news/2017/02/08/national/crime-legal/cyberattacks-targeting-japan-networks-hit-record-128-1-billion-2016/#.XHmfQy3MxsN>.

¹⁵⁶ Daniel R. Coats, “2019 Worldwide Threat Assessment Of The U.S. Intelligence Community,” *Office of the Director of National Intelligence*, pg. 5, January 29, 2019, <https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf>.

United States.”¹⁵⁷ However, this risk is equally present in Canada, where cybersecurity experts at CSE and CSIS have routinely highlighted how sophisticated cyber capabilities are being leveraged by nation-states to infiltrate industrial and non-industrial infrastructure sectors. An internal government memo exchanged between Public Safety Canada and intelligence partners in 2016 reinforces the reality of this threat, explaining that, “Other nation states are exploiting cyberspace for their own economic benefit or strategic advantage. Cyber attack for strategic reasons is more subtle and is focused on gaining access and control of key assets. For example, Russia and China have compromised vital cyber systems in Canadian critical infrastructure, placing the safety and security of Canadians at risk.”¹⁵⁸ In addition to the clear strategic threat Chinese cyber activities pose to the availability and integrity of networks and information systems supporting essential services in Canada, it is also important to identify the unique challenges the Russian government and their contracted affiliates are creating for Ottawa’s infrastructure cybersecurity policies.

A useful example to demonstrate the extent of Russia’s infiltration and presence within Canada’s critical infrastructure IT environments relates to an extended hacking campaign involving several breaches across the shared U.S.-Canada electrical grid in 2017. CSE had alerted partners at DHS’s ICS-CERT to the breaches, which then led to the U.S. Cybersecurity and Infrastructure Security Agency (CISA) releasing attack TTPs and indicators of compromise (IOC) to help organizations servicing the grid tailor their defenses.¹⁵⁹ The CISA bulletin describing the computer network attacks notes that, “DHS and FBI characterize this activity as a multi-stage intrusion campaign by Russian government cyber actors who targeted small

¹⁵⁷ Ibid.

¹⁵⁸ Colin Freeze, “Ottawa’s 2016 Memo On Cyber Threats Points Finger At Russia, China,” *The Globe and Mail*, May 4, 2018, <https://www.theglobeandmail.com/canada/article-ottawas-2016-memo-on-cyberthreats-points-finger-at-russia-china/>.

¹⁵⁹ Canadian Center for Cyber Security, “National Cyber Threat Assessment 2018,” 25.

commercial facilities' networks where they staged malware, conducted spear phishing, and gained remote access into energy sector networks."¹⁶⁰ Although the Russian activities during this extended period were primarily targeting U.S.-based utility and power generating organizations—including nuclear facilities according to the CERT report—the risk of a disruptive event surging across Canada's electrical grid prompted CSE to classify the incident as a direct threat to the country's infrastructure.¹⁶¹ At the time of the compromises, Jonathan Homer, chief of the ICS group at DHS's Hunt and Incident Response Team, stated that, "The threat actor had a level of access to be able to cause change, to be able to cause impact to the physical elements of this control system. They got to the point that they could turn the switches, but they didn't."¹⁶² The strategic opportunities Russia gains by infiltrating the electrical grid and other critical infrastructure systems within Canada and in allied countries provides Moscow with a flexible, damaging and direct tool for supporting their geopolitical interests and pressuring their perceived adversaries into undesired decisions or actions.

As outlined in the second chapter, where Ontario's electrical grid was analyzed as a case study for sector breadth and complexity, Canada and the U.S. share a highly interconnected bulk power system. This includes an overlap of federal, state/ provincial, and regional government regulators in addition to thousands of private vendors servicing and sometimes operating the infrastructure across the border. The 2016 "Joint United States-Canada Electric Grid Security and Resilience Strategy" reinforces this point by noting, "Isolated or complex events with cascading effects that take place in either country can have major consequences for both the

¹⁶⁰ Cybersecurity and Infrastructure Security Agency, "Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy And Other Critical Infrastructure Sectors," *Department of Homeland Security*, March 15, 2018, <https://www.us-cert.gov/ncas/alerts/TA18-074A>.

¹⁶¹ Blake Sobczak, "Canadian Utilities Got Head Start Against Russian Grid Threat," *E&E News*, July 26, 2018, <https://www.eenews.net/stories/1060091227>.

¹⁶² *Ibid.*

United States' and Canada's electric grids and adversely affect national security, economic stability, and public health and safety.”¹⁶³ Although the majority of targeted organizations during the 2017 campaign were based in the U.S., with only some Canadian enterprises being impacted, the Russia-electrical grid example clearly demonstrates the advanced capabilities of Moscow's most elite hackers in addition to the vulnerabilities residing inside Canadian infrastructure IT systems. Further, it also shows Russia's willingness to leverage cyberspace as a tool during peacetime to locate new attack opportunities or to occupy their adversary's limited cybersecurity incident response resources. This event supports the idea that adversaries are compromising networks and information systems vital to the country's security and safety while relations are peaceful. By routinely targeting ICS and SCADA equipment in addition to other essential non-industrial IT equipment, Moscow has indicated that cyberspace is not just an environment for IP theft or financial crime, but also for military posture and security projection.

At the 2017 Reuters Cyber Security Summit in Toronto, Scott Jones, an assistant deputy minister at CSE, stated that, “Targeted attacks on Canadian infrastructure is something we are really worried about.”¹⁶⁴ During additional remarks after the event he explained how at least 60 nations currently have the ability to conduct offensive cyber warfare operations, which included ones that could harm the electrical, nuclear, aviation, financial and manufacturing infrastructure of the country. Among the most elite hackers threatening Canada from a geopolitical motivation and capability standpoint is North Korea. Pyongyang's cyber activities and routine espionage campaigns against critical infrastructure are frequent and complex within Canada and in allied

¹⁶³ Government of the United States and Government of Canada, “Joint United States-Canada Electric Grid Security And Resilience Strategy,” *Government of Canada: Public Release Statements*, December 2016, https://www.nrcan.gc.ca/sites/www.nrcan.gc.ca/files/energy/pdf/JOINT%20GRID%20SECURITY%20AND%20RESILIENCE-Strategy_en.pdf.

¹⁶⁴ Alastair Sharp and Jim Finkle, “Canada Worried About Infrastructure Hacks: Intelligence Official,” *Reuters*, October 23, 2017, <https://www.reuters.com/article/us-cyber-summit-canada-infrastructure/canada-worried-about-infrastructure-hacks-intelligence-official-idUSKBN1CS2EZ>.

countries—particularly South Korea, the U.S. and Japan.¹⁶⁵ However, in some cases, Canada has been uniquely selected as a target, resulting in APT groups closely linked with the North Korean government compromising information systems supporting regional critical infrastructures. For example, in 2018, Ontario’s provincial transit authority—called Metrolinx—announced that a group associated with North Korean security agencies had breached their network.¹⁶⁶ At the time, Public Affairs Manager Anne Marie Aikins stated that after provincial authorities provided red teaming assistance and incident response analysis, it was clear that a nation-state was involved and that there was sufficient evidence to attribute the attack to North Korean individuals. Reports on the incident note that while there was no public safety risk, as critical systems supporting provincial commercial and passenger railways were not impacted, the ability for this group to deploy an APT and escalate their attack to control systems would have been possible with more time.¹⁶⁷

Foreign Ministers and representatives of 20 countries from across the world met in Vancouver, British Columbia a week before the Metrolinx incident to discuss nuclear and ballistic missile proliferation on the Korean Peninsula. A joint statement led by the Canadian and U.S. officials at the meeting explicitly stated that, “North Korean cyber-attacks and other malicious cyber activities pose a risk to critical infrastructure in countries around the world and to the global economy.”¹⁶⁸ Only a week later North Korea launched the operation against Metrolinx, which not only indicates a potential geopolitical motivation for the attack, but it also

¹⁶⁵ Coats, “2019 Worldwide Threat Assessment Of The U.S. Intelligence Community,” 5.

¹⁶⁶ Howard Solomon, “Ontario Transit Agency Extremely Confident Cyber Attack Came From North Korea,” *IT World Canada*, January 24, 2018, <https://www.itworldcanada.com/article/ontario-transit-agency-extremely-confident-cyber-attack-came-from-north-korea/401047>.

¹⁶⁷ *Ibid.*

¹⁶⁸ “Co-Chairs’ Summary Of The Vancouver Foreign Ministers’ Meeting On Security And Stability On The Korean Peninsula,” *Global Affairs Canada*, January 16, 2018, https://www.canada.ca/en/global-affairs/news/2018/01/co-chair_s_summaryofthevancouverforeignministersmeetingonsecurit.html?_ga=2.150039222.1285958903.1516771858-817845510.1516771858.

demonstrates how Pyongyang could have induced an infrastructure availability or safety issue for an entity overseeing the transport of nearly 70 million Canadian passengers annually¹⁶⁹. The physical threat to the country and the possible secondary and tertiary economic effects such an attack could have posed highlights the active national security risk to Canada stemming from nation-state hackers and their associated APT groups.

According to the “Horizontal Evaluation of Canada's Cyber Security Strategy” report released in 2017 by Public Safety Canada, there were more than 2,500 state-sponsored cyber campaigns launched against core national networks between 2013 and 2015—at federal, provincial, private and infrastructure levels.¹⁷⁰ These statistics in addition to the examples provided in this section highlight how foreign adversaries have operationalized cyberspace as a tool to conduct malicious activity during peacetime and to create opportunities for strategic attacks during conflict or hostile political relations. Although this section did not specifically focus on the developments occurring in Canada related to tactical cyber operations at theater or unit levels in the military, it is important to note that these local combat components of cyber warfare—and the increasingly related cyber-electronic warfare convergence—are not directly challenges for the civil safety and prosperity of Canada. This raises a key issue surrounding the discussion of cyber warfare, as it involves numerous activities that occur during peacetime and outside of the traditional scope of military doctrine. However, as foreign adversaries continue to leverage cyberspace as a medium to threaten the integrity and availability of Canada’s critical infrastructure environment—which in many ways directly supports the CAF—there will be an increasingly important domestic role for the Canadian forces. This will include defending national systems and supporting federal agencies with incident response, in addition to their

¹⁶⁹ Solomon, “Ontario Transit Agency Extremely Confident Cyber Attack Came From North Korea.”

¹⁷⁰ “Horizontal Evaluation Of Canada's Cyber Security Strategy,” *Public Safety Canada*, September 29, 2017, <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/vltn-cnd-scrtr-strtg/index-en.aspx>.

more indigenous responsibilities of developing and fielding tactical cyber capabilities to enable the military in warfighting and digitally contested environments.

Ultimately, state-sponsored cyber espionage and attack occurring throughout Canada's industrial and non-industrial sectors will continue to increase in volume and sophistication due to the strategic priority adversaries have placed on compromising infrastructure assets. While offensive exploit technologies proliferate globally and countries such as Iran and China continue funding and developing advanced capabilities, Canada's government and private sector will need to employ an even greater amount of resources to offset national infrastructure becoming more reliant on Internet-connected systems.

Cyber Terrorism and Hactivism

Although the most advanced cyber threats facing Canada and its allies stem from nation-states and their associated APT groups, there is also an active and growing risk developing from foreign and domestic terrorist actors. Whether operating as a group or individually, these actors have identified critical infrastructure in Canada as a key target for achieving political objectives—using both physical and digital means. In addition to threats from terrorism, there is also the rising trend of hactivism, which Deloitte's Threat and Analytics Team describes as, "The act of carrying out malicious cyber activity to promote a political agenda, religious belief, or social ideology."¹⁷¹ It is sometimes difficult to conceptually differentiate hactivists and terrorists, as their motivations may have similar socio-political end objectives, such as violent environmental activist groups targeting a power plant for its environmental impact and a terror group targeting the same plant to impact public safety.

¹⁷¹ Threat and Analytics Team, "Hactivism: A Defenders Playbook," *Deloitte LLP*, August 12, 2016, <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-hactivism.pdf>.

Traditional definitions of terrorism and activism do not always apply clearly in cyber domain, though it can generally be held that terrorism leverages violence whereas hacktivism leverages financial, social, political or reputational inconvenience.^{172 173} However, as previously noted, traditional approaches to these different threat actors are not always accurate. For example, there are many instances of terror groups using cyberspace for non-physical and non-life threatening activities—such as Hamas’ use of computer network exploitation to send fake propaganda messages to Israeli Defense Forces (IDF) personnel—or hacktivist groups inducing a physical impact—such as the hacking group Anonymous causing delays at Boston Children Hospital in 2014 as a response to a medical abuse case.^{174 175} Although these types of incidents demonstrate an aspect of hacktivism and cyber terrorism convergence, this section will highlight how there are still significant distinctions, particularly in the context of labeling cyber threat actors and evaluating IT risk levels for Canada’s critical infrastructure.

The threat posed by terrorist actors has traditionally been physical, where strong perimeter security and external physical countermeasures meant strong protection of vital systems and assets. However, the growing reliance of Canada’s national infrastructure on cyberspace has provided international terror groups and their affiliates with new attack vectors. The 2012 CSIS document titled “Assessing Cyber Threats To Canadian Infrastructure” notes that, “Although the Energy, Transport and Finance sectors have long been attractive targets in

¹⁷² Ryan Littlefield, “Cyber Terrorism: Understanding And Preventing Acts Of Terror Within Our Cyber Space,” *Medium*, June 7, 2017, <https://littlefield.co/cyber-terrorism-understanding-and-preventing-acts-of-terror-within-our-cyber-space-26ae6d53cfbb>.

¹⁷³ Dan Lohrman, “Understanding New Hacktivism: Where Next For Hackers With A Cause?” *Government Technology*, July 31, 2016, <http://www.govtech.com/blogs/lohrmann-on-cybersecurity/understanding-new-hacktivism-where-next-for-hackers-with-a-cause.html>.

¹⁷⁴ Omer Dostri, “Hamas’ Cyber Activity Against Israel,” *The Jerusalem Institute for Strategy and Security*, October 15, 2018, <https://jiss.org.il/en/dostri-hamas-cyber-activity-against-israel/>.

¹⁷⁵ Ryan Grim, “Why I Knocked Boston Children’s Hospital Off The Internet: A Statement From Martin Gottesfeld,” *Huffington Post*, September 18, 2016, https://www.huffingtonpost.com/entry/why-i-knocked-boston-childrens-hospital-off-the-internet-a-statement-from-martin-gottesfeld_us_57df4995e4b08cb140966cd3.

terms of physical attacks, there are now growing concerns that Islamists will use the Internet to launch cyber attacks to promote their so-called economic jihad. Al-Qaeda has called explicitly for a cyber jihad alongside other terror operations, while certain Islamic scholars have affirmed the religious legitimacy of electronic jihad.”¹⁷⁶ The following year, Public Safety released their 2013 “Building Resilience Against Terrorism” strategy, which highlighted that, “Terrorist groups have expressed interest in developing the capabilities for computer based attacks against critical infrastructure.”¹⁷⁷ These points reinforce the existence of a digital threat to infrastructure safety and integrity stemming from international terror groups and their domestic supporters in Canada.

It is also important to note that while Islamist-linked groups may be recognized as the most direct and active terror threat in Canada, the “Building Resilience Against Terrorism” strategy also notes that other actors with different religious and/ or political motivations are also an ongoing challenge for national security policy. For example, the strategy outlines that, “The threat posed by violent Sunni Islamist extremists may be Canada’s most pressing concern, but Canada faces a broad range of international and domestic terrorist threats.” Within the domestic-based threat section of the document, it references the 1995 Oklahoma City bombing and the 2011 Norway shooting as major terror events where Islamist actors were not involved in the attack and where attribution was officially assigned to a domestic perpetrator.¹⁷⁸

Recognizing the prospect of a domestic-based cyber terrorist is particularly important because there is substantial educational and technical resources available in Canada that are traditionally unavailable in foreign countries where many international terror threats reside. For example, a 2018 National Post article outlined how a Canadian foreign fighter who had travelled

¹⁷⁶ Angela Gendron and Martin Rudner, “Assessing Cyber Threats To Canadian Infrastructure,” 7-8.

¹⁷⁷ “Building Resilience Against Terrorism: Canada's Counter-terrorism Strategy,” *Public Safety Canada*, January 31, 2018, <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/rslnc-gnst-trrrsm/index-en.aspx>.

¹⁷⁸ *Ibid.*

to the Middle East to join the Islamic State of Iraq and Syria (ISIS) was supporting the group's increasingly sophisticated cyber operations.¹⁷⁹ The hacker had been involved in computer network attacks targeting the U.S. Department of Defense (DoD), airports and international media outlets—in addition to hacking online bank accounts to steal money to support ISIS recruitment and operational activities.¹⁸⁰ This individual also developed relatively advanced computer security tools for the terror organization to protect its online information from allied intelligence efforts and to preserve and mask its social media accounts.

According to translations from the Middle East Media Research Institute (MEMRI), the Canadian hacker eventually became a senior specialist operating under the so-called Caliphate Cyber Army, which released a public statement in 2018 referring to the individual as a, “Gifted computer programmer.”¹⁸¹ Although cyberspace enables threat actors to conduct attacks from distant and remote areas, Canadian security agencies and private-public stakeholders need to prepare for a doctrinal shift in ISIS and other international terror group thinking as foreign fighters begin to return home from battlefields in the Middle East, North Africa and South East Asia. For example, the 2018 Department of Public Safety and Emergency Preparedness “Public Report on the Terrorism Threat To Canada” highlights that, “The number of extremist travellers with Canadian connections abroad remains stable at roughly 190. Close to 60 people suspected of engaging in extremist activities abroad have returned to Canada.”¹⁸² While being back in Canada does not necessarily improve their capacity to conduct malicious cyber activity, it does mean that their target scope will narrow and possibly lead to the targeting of Canada's vital

¹⁷⁹ Adrian Humphreys, “Toronto-Born Canadian Is Mystery Man Behind ISIL's High-Profile Cyber Attacks,” *The National Post*, November 7, 2018, <https://nationalpost.com/news/canada/toronto-born-canadian-is-mystery-man-behind-isils-high-profile-cyber-attacks>.

¹⁸⁰ Ibid.

¹⁸¹ Ibid.

¹⁸² “Public Report On The Terrorism Threat To Canada,” *Public Safety Canada*, December 14, 2018, <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/pblc-rprt-trrrsm-thrt-cnd-2018/index-en.aspx>.

national systems both physically and digitally. Whether a given terrorist actor has an advanced know-how in computer science, networking or IT systems, or whether they resort to recruiting or providing a financial incentive for a computer expert to launch or develop a piece of malware for them, the risk to infrastructure from terrorist threats in terms of motive, intent and capability are simultaneously growing. Combining these trends with the Canadian hacker example outlined in the National Post article reinforces the prospect of a domestic or internationally linked cyber terrorist adversely affecting the safety, availability or integrity of a critical infrastructure asset in Canada.

While the motivations and interests of terror groups seeking to exploit cyber vulnerabilities are clear, it is important to evaluate the actual capabilities of these actors to gauge the level of risk facing Canada. The International Institute for Counter-Terrorism in Israel noted in a 2018 report that members of ISIS were attempting to develop cyber capabilities and operational procedures for conducting critical infrastructure attacks.¹⁸³ This report comes six years after Canada's 2012 critical infrastructure cyber assessment, which explained that U.S. officials, "Commenting on the IT capabilities of Islamist terrorist groups, have admitted that they underestimated the time al-Qaeda had spent mapping vulnerabilities. American authorities reportedly detected operatives using telecom switches in several countries, including Saudi Arabia and Pakistan, to explore digital systems that control U.S. nuclear power plants, emergency telephone services, and water storage and distribution."¹⁸⁴ Canada's 2018 National Cyber Security Strategy also highlights that, "Terrorist organizations are also interested in acquiring advanced cyber tools to conduct attacks," although it adds that these groups are not as

¹⁸³ Yonah Jeremy, "Exclusive: Islamic Cyber Terrorists Trying To Target Infrastructure," *The Jerusalem Post*, July 9, 2018, <https://www.jpost.com/Arab-Israeli-Conflict/Exclusive-Islamic-cyber-terrorists-trying-to-target-infrastructure-562052>.

¹⁸⁴ Gendron and Rudner, "Assessing Cyber Threats To Canadian Infrastructure," 24.

capable of nation-state actors and their objectives are generally different in scope.¹⁸⁵ While these points indicate a growing technical foundation among terrorist organizations, it reinforces their current inferiority to the more complex and persistent risks facing Canadian infrastructure sectors from government or state-linked APT groups.

This lack of capability was also highlighted in a 2017 U.S. National Counterterrorism Center (NCTC) report, which explained that the majority of ISIS cyber activities are localized, targeted at regional actors and involve primarily open-source exploit kits with little indigenous technical development. The report refers to their activities as, “Low-level,” but notes that, “We need to anticipate that ISIS will move aggressively to develop increased competency in the cybersphere.”¹⁸⁶ Even though ISIS and other international terror groups are placing a priority on developing offensive cyber expertise and tools—often with an emphasis on critical infrastructure targets—their current technical threat is simply not comparable to the TTPs or code elegance and sophistication of nation-states.

In 2012, the FBI arrested Jeremy Hammond, an individual who operated as part of the hacktivist group Anonymous. The arrest was officially classified as a terrorist-related investigation according to the New York State Division of Criminal Justice Services (DCJS), whose documents on the arrest indicate that Hammond and the group were on the multi-agency Terrorist Screening Database (TSDB) with other well-known terrorist organizations—including Colombia’s leftist FARC movement, al-Qaeda and the Somalia-based extremists al-Shabaab.¹⁸⁷ While this example highlights how one of Canada’s closest allies recognizes the convergence of hacktivism and cyber terrorism, there are still distinct characteristics that separate the two threat

¹⁸⁵ “National Cyber Security Strategy,” *Public Safety Canada*, 13.

¹⁸⁶ Kimberly Underwood, “ISIS Takes Fight To Cyber Battlefield,” *SIGNAL Magazine*, November 1, 2017, <https://www.afcea.org/content/isis-takes-fight-cyber-battlefield>.

¹⁸⁷ Dell Cameron, “FBI Put Anonymous Hacker Jeremy Hammond On A Terrorist Watch List,” *The Daily Dot*, February 24, 2017, <https://www.dailydot.com/layer8/jeremy-hammond-terrorist-watchlist-fbi/>.

actor categories. For example, Gabriella Coleman, who is an international expert on Anonymous from Canada's McGill University, while discussing hacktivist threats to national infrastructure stated that, "I don't think Anonymous is a threat. They're not there to kill people. And I'm not so sure they have the capabilities for that either."¹⁸⁸ These comments provide insights on the socio-political scope of a traditional hacktivist mandate, which does not include any type of cyber operation aiming to induce serious physical or safety damage to the average Canadian or Canadian business. Based on this key distinction, hacktivist actors should generally be excluded from the classification of a key threat under federal, provincial, local or private cybersecurity policies aiming to protect industrial critical infrastructure from failure-based attacks—though hacktivist threats to non-industrial sectors, such as the financial system, remain significant.¹⁸⁹ Conversely, since the mandate of terrorist groups would specifically call for catastrophic cyber attacks on national targets, where an opportunity to hurt the public interest would be viewed as a strategic opportunity, terror groups and their cyber activity need to be closely monitored by every sector as an active risk.

Although hacktivists will generally refrain from targeting critical infrastructure to cause strategic safety risks to Canadians—such as power plants or hospital targets—this does not mean that there is no threat to national security stemming from their activities. For example, other groups such as LulzSec and WikiLeaks have stolen and publically released large amounts of classified data from governments and sold sensitive corporate information on black markets.¹⁹⁰ The Vault 7 data dump reinforces this threat, as the documents that were stolen by hacktivists and released through WikiLeaks revealed technical details on many Central Intelligence Agency

¹⁸⁸ Jordan Press, "Anonymous A Threat To Critical Infrastructure? Expert Says No," *News National*, December 20, 2012, <https://o.canada.com/news/anonymous-a-threat-to-critical-infrastructure-expert-says-no>.

¹⁸⁹ Ibid.

¹⁹⁰ Parmy Olson, "Inside LulzSec: How The Superstar Hackers Met Wikileaks," *Gawker*, May 30, 2012, <https://gawker.com/5914045/inside-lulzsec-how-the-superstar-hackers-met-wikileaks>.

exploits used for communication eavesdropping and circumventing encryption for data in transit on mobile devices.¹⁹¹ Canada's CSE also commented in 2017 that they were preparing for, "Multiple hacktivist groups [to] deploy cyber capabilities in an attempt to influence the democratic process in 2019," which was in reference to Canada's upcoming federal election.¹⁹² Additional hacktivist activities were successful in 2015, when several federal government websites were targeted by denial-of-service operations and subsequently taken offline.¹⁹³ Although these types of threats and actors are challenges for Canada's cybersecurity at-large and Ottawa's approach to national security in cyberspace, they are generally outside the realm of direct strategic risks to the integrity and availability of the country's infrastructure IT systems.

The last consideration for this section's threat actor assessment relates to outsourcing and technology proliferation. As the tools used for offensive cyber activity continue to proliferate, and as educational resources become more commonplace via Internet-enabled courses and programs, terror and hacktivist actors will have more resources to support their objectives and for developing indigenous capabilities. The Ashiyane Digital Security Team, also referred to as Ashiyane or NEST, is a useful example for demonstrating the rapidly changing educational landscape surrounding hacking.¹⁹⁴ Ashiyane is a unique actor within Iran's private hacking community who generally maintains a close relationship with the government—particularly the IRGC and the Ministry of Intelligence.

¹⁹¹ Cyrus Farivar, "Man Who Allegedly Gave Vault 7 Cache To Wikileaks Busted By Poor Opsec," *ARS Technica*, June 19, 2018, <https://arstechnica.com/tech-policy/2018/06/ex-cia-engineer-indicted-on-several-new-charges-connected-to-vault-7-leak/>.

¹⁹² Dean Beeby, "State-Sponsored Cyberattacks On Canada Successful About Once A Week," *BBC News*, October 30, 2017, <https://www.cbc.ca/news/politics/cyber-attacks-canada-cse-1.4378711>.

¹⁹³ Howard Solomon, "Hacktivist Group Temporarily Takes Down Canadian Federal Sites," *IT World Canada*, June 17, 2015, <https://www.itworldcanada.com/article/hacktivist-group-temporarily-takes-down-federal-sites/375450>.

¹⁹⁴ David Banisar and Patricia Melendez, "Tightening The Net Part 2: The Soft War And Cyber Tactics In Iran," *The Article 19 Center: Civic Space Unit*, March 2017, pg. 33, https://www.article19.org/data/files/medialibrary/38619/Iran_report_part_2-FINAL.pdf.

In addition to the basic malicious activity the group conducts, such as localized denial-of-service attacks or social media hijacking, they also act as one of the largest online educational and training resources for the hacking and computer security community in Iran.¹⁹⁵ For example, members of Ashiyane have taught at hackathons and security conferences in Iran as keynote speakers. During these events, members of the group review TTPs for DDoS operations, Linux server infiltration and SQL Injection attacks. As of 2017, there were allegedly 363,949 unique members participating in the group's online tutorials, which ranged from instructional videos and interactive labs focusing on Privilege Escalation, Access Control, OS Analysis and Scanning, Network Management and Infiltration, Cryptography, Email Security and Remote Access Trojan (RAT) Development.¹⁹⁶ The group has also directly provided technical know-how to regional terror groups seeking to expand their cyber capabilities, such as the closely linked Iranian affiliate Hezbollah.¹⁹⁷ These types of open-source education resources combined with the ability to buy commercial-off-the-shelf exploit kits and malware products are allowing terror groups and their domestic partners in addition to hacktivists around the world to increase their cyber proficiency.

When access to educational resources and the purchasing of exploit technology is unsuitable, as the group may not understand its code or components, an opportunity exists to pay or ideologically recruit a third-party hacker. For example, in 2015, John Riggi, a section chief at the FBI's cyber division, explained to an industry gathering of energy firms that, "The Islamic State is trying to hack U.S. power companies," however, he added that the terrorist group has,

¹⁹⁵ Dorothy Denning, "Following The Developing Iranian Cyberthreat," *Scientific American*, December 12, 2017, <https://www.scientificamerican.com/article/following-the-developing-iranian-cyberthreat/>.

¹⁹⁶ Banisar and Melendez, "Tightening The Net Part 2: The Soft War And Cyber Tactics In Iran," 34-35, 58.

¹⁹⁷ Frederick W. Kagan and Tommy Stiansen, "The Growing Cyber Threat From Iran," *American Enterprise Institute: Critical Threats Project*, April 2015, https://www.criticalthreats.org/wp-content/uploads/2016/07/imce-imagesGrowing_Cyberthreat_From_Iran_AEI_Norse_Kagan_Stiansen-1.pdf.

“Strong intent. Thankfully, low capability. But the concern is that they'll buy that capability.”¹⁹⁸ Similar remarks were made in a report written by Scott Stewart, Vice President (VP) of Tactical Analysis at Stratfor, who outlined that, “A terrorist group doesn't need to develop the malware for a hack itself. It can buy malware from a commercial hacking crew and then repurpose it for a more malicious purpose than simply stealing. State sponsorship is also a potential way for terrorist actors to gain access to malware tools for asymmetrical cyber terrorism.”¹⁹⁹ These alternative methods for terrorist and hacktivist groups to acquire the capability to conduct advanced cyber attacks is extremely difficult from a proactive mitigation standpoint since a given actor’s capability or damage potential can dramatically increase in a short period of time and with little warning. While the ideological aim of most hacktivist groups largely removes them from the discussion on strategic attacks against critical infrastructure in Canada, terror groups, particularly those who have already demonstrated intent and capability to launch or acquire complex exploit technologies, will continue to become a growing risk to industrial and non-industrial IT systems supporting Canada’s vital systems.

Insider Threats: Foreign Espionage To Accidental IT Disruptions

As outlined in the first section of this chapter where nation-state threats to Canada’s critical infrastructure were analyzed, government-linked cyber espionage is often associated with an APT-type of operation. The actor slowly scans a network, escalating privileges and locating additional vulnerabilities or vital systems to compromise in the future for strategic purposes. Governments and terror groups, and even hacktivists, can leverage an employee at an organization to facilitate their malicious objectives. For example, an individual who is recruited

¹⁹⁸ Scott Stewart, “The Coming Age Of Cyberterrorism,” *Stratfor Worldview*, October 22, 2015, <https://worldview.stratfor.com/article/coming-age-cyberterrorism>.

¹⁹⁹ Ibid.

by a foreign intelligence agency—perhaps for monetary benefits—may attach a malicious USB to an unsecure port or intentionally open a malicious file on a secure endpoint that already has authorized access to an organization’s network. Similarly, an employee or a contractor servicing an organization may have ideological beliefs that lead him/her to sympathize with an activist or terrorist group who may then use the individual as a mechanism for gaining access to a secure network or an important information system. In very dangerous scenarios, the internal employee or contractor may even be a member of the IT or cybersecurity staff, which would potentially provide the threat actor with administrative or root access and the ability to hinder incident response by masking log or security metrics. These collective security challenges are called insider threats, which the 2018 “National Cyber Security Strategy” defines as, “A malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organization’s security practices, data and computer systems.”²⁰⁰

In addition to being associated with a third party threat actor, such as a foreign government, terror group or hacktivist organization, an insider threat can also be a disgruntled skilled programmer or technician who is seeking revenge on his/her employer and has a strong understanding of the organization’s IT systems and networks. Conversely, there can also be IT accidents caused by maintenance or negligent patching mistakes, or even an unintended abuse of a system’s function. When all of these risks are aggregated, it becomes clear that insider threats have the potential to directly cause or facilitate major disruptions to the cyber assets supporting Canada’s critical infrastructure.

The 2017 Global Threat Intelligence Center (GTIC) quarterly report from NTT Security, an internationally renowned cybersecurity consultancy, reveals that, “Approximately 25% of

²⁰⁰ National Cyber Security Strategy,” *Public Safety Canada*, 34.

insider threats are hostile with the remaining 75% due to accidental or negligent activity. Even in organizations that have well-defined incident response plans, they often don't provide adequate remediation provisions for insider breaches, leaving the organization less prepared to react quickly."²⁰¹ This report highlights that the insider threat is complex and difficult to mitigate considering most of the time there is not even an actor motivation for the cybersecurity staff to take into account when tailoring detection, protection and response measures. A 2018 speech by CSIS Director David Vigneault also emphasizes the magnitude of this threat by detailing how foreign governments are increasingly targeting organizations dealing in high-tech and critical infrastructure sectors with malicious insiders. For example, nation-state actors are interested in stealing the IP from Canada's leading IT and security vendors to assist the business development of their domestic state-owned enterprises, but also to reverse engineer the stolen technology to help guide their hacking teams towards vulnerabilities in already deployed software and hardware assets servicing Canada's infrastructure.²⁰²

At the same 2018 speech, Vigneault noted that, "No matter how it's done or who's behind it, economic espionage represents a long-term threat to Canada's economy and to our prosperity. CSIS already has seen a trend emerging of state-sponsored espionage in fields like A.I., quantum technology, 5G wireless technology, biopharmaceuticals and low-carbon technology."²⁰³ While it is clear that state-linked insider threats enabling both physical and cyber espionage for commercial or intelligence purposes is a strategic concern for Canada, there are many industries and corporate sectors impacted by this threat that are out of the scope of critical infrastructure

²⁰¹ Cybersecurity Newswire Desk, "New Report Reveals How Accidental Insider Threats Put Organizations At Real Risk," *Security Magazine*, November 29, 2017, <https://www.securitymagazine.com/articles/88542-new-report-reveals-how-accidental-insider-threats-put-organizations-at-real-risk>.

²⁰² David Vigneault, "Remarks By Director David Vigneault At The Economic Club Of Canada" (speech, Canadian Security and Intelligence Service and Economic Club of Canada Conference, Toronto, ON, December 4, 2018).

²⁰³ Ibid.

security. For example, IP theft of pharmaceuticals could impact the financial and social wellbeing of Canadians and Canadian business in the long-term, but this threat is incomparable to the immediate safety and strategic consequences a cyber attack on the hospital infrastructure of the country could induce—as seen with the WannaCry ransomware virus which will be analyzed in the following chapter.

Another example of cyber and physical-enabled insider threats posing a risk to national security but having little direct impact on critical infrastructure relates to a CSE briefing in 2013. The briefing references a new training program for employees on insider threats, which was partially in response to increased foreign intelligence activity but also a countermeasure against incidents such as the 2012 Edward Snowden leaks.²⁰⁴ CSE released a comment in response to the media acquiring the briefing notes, which read, “CSE provides continuous security education and training to staff, which includes increasing staff awareness of insider threat issues.” This comment came after it was revealed that in addition to the education improvements, the agency was also implementing a five-year \$45 million USD upgrade of its Top Secret (TS) communications network—specifically as an information security control (referring to a Data Loss Prevention [DLP] program) to prevent insiders from conducting large data exfiltrations.²⁰⁵

While Vigneault’s comments and the CSE insider briefings highlight the economic and general national security consequences insider threat-related cybercrime, stolen intelligence and IP theft can cause, a 2016 Public Safety Canada report reinforces the key strategic differences insider risks pose in a critical infrastructure context. The Star media outlet, which provided the first public commentary on the report noted that, “Federal officials have quietly warned operators of electrical grids, transportation hubs and other key infrastructure of the cyber threat from

²⁰⁴ Alex Boutilier, “A Canadian Snowden? CSE Warns Of ‘Insider Threats,’” *The Star*, July 26, 2015, <https://www.thestar.com/news/canada/2015/07/26/a-canadian-snowden-cse-warns-of-insider-threats.html>.

²⁰⁵ *Ibid.*

insiders who could unleash devastating viruses and cripple systems.” The report itself states that, “Crucial networks that Canadians rely on for everyday needs face a substantial threat from rogue employees out to wreak digital havoc.” These comments emphasize the national security and public resiliency risks malicious and non-malicious insider threats continue to pose within the infrastructure environment. Protecting against IP theft and other cybersecurity issues should be a priority for the federal and provincial governments, but these risks are largely centered on individual incidents and organizations at the commercial level compared to the infrastructure risk which is often centered on a national economic and public safety level.

To demonstrate the severity of a malicious insider threat, it is worth discussing an example from a Dallas, Texas (U.S.) hospital that was the target of a cybersecurity incident in 2009.²⁰⁶ A disgruntled issue-driven security guard, who worked at the hospital and had some background in computer security, downloaded malware onto a mobile media device and brought it with him to work. Upon arrival, the employee connected the device to dozens of machines with patient records. He also attempted to upload a specialized malware program enabling remote interactive control to the IT assets connected to the hospital’s heating, ventilation, and cooling (HVAC) systems, which if compromised could have spoiled refrigerated pharmaceutical drugs and stressed many patients’ physical health.²⁰⁷ This example is an ideal demonstration of how an insider threat—regardless of motivation—can leverage his/her physical access privileges to enable a network breach and possibly cause a severe cybersecurity incident.

A different example that relates to current geopolitical and national security policy issues is the risk of a terror organization recruiting or embedding insider threats across critical

²⁰⁶ “Insider Threats: In The Healthcare Sector,” *Center for Internet Security*, accessed January 27, <https://www.cisecurity.org/blog/insider-threats-in-the-healthcare-sector/>.

²⁰⁷ Nicholas Leali, “Lessons From An Insider Attack On SCADA Systems,” *Cisco*, August 20, 2009, https://blogs.cisco.com/security/lessons_from_an_insider_attack_on_scada_systems.

infrastructure sectors in Canada. The 2012 “Assessing Cyber Threats To Canadian Infrastructure” report published by CSIS has a section dedicated to insider threats and the prospect of cyber terrorism in Canada. The section explains that, “Infrastructure sectors and institutions in various jurisdictions that are known to have experienced insider threats from international jihadist elements in recent years include airports, airlines, energy utilities, nuclear plants, petroleum companies, university laboratories, water systems, sensitive government departments and security agencies in Denmark, the Netherlands, the U.K. and the U.S.”²⁰⁸ Each of these close political and security allies of Canada has clearly experienced a terror-related insider threat scenario, indicating that the risk to infrastructure across Canada is active or simply not widely reported on due to government classifications preventing open-source exposure or the lack of information-sharing among sector stakeholders. This lack of information and reporting of insider threats throughout critical infrastructure is a serious challenge, which the report clearly outlines by stating that, “Rarely is open-source information available on manifest insider threats, since organizations tend to be reticent about any such matters for reputational reasons.”²⁰⁹

Nevertheless, certain U.S. intelligence reports for DHS provide insight into cases involving insider threats associated with terror groups targeting critical infrastructure sectors. An unclassified 2011 document titled “Insider Threat to Utilities” from the DHS Office of Intelligence and Analysis states that there have been, “Recent incidents involving physical and cyber insider attacks” across energy-based critical infrastructure and that, “Violent extremists have, in fact, obtained insider positions.”²¹⁰ The report also explains how, “Disgruntled current and former utility-sector employees have successfully used their insider knowledge to damage

²⁰⁸ Gendron and Rudner, “Assessing Cyber Threats To Canadian Infrastructure,” 35.

²⁰⁹ *Ibid.*, 21.

²¹⁰ Office of Intelligence and Analysis, “Insider Threat To Utilities,” *Department of Homeland Security*, pg. 1-2,4, July 19, 2011, <https://info.publicintelligence.net/DHS-InsiderThreat.pdf>.

facilities and disrupt site operations.”²¹¹ Not only is this example demonstrative of the ongoing risk of insiders to cybersecurity programs in Canada and in allied countries, but since the utility sector is particularly prevalent in cross-border operations, these specific incidents may have actually represented a direct threat to Canadians and Canadian businesses.

The DHS report also highlights an example in the mid-2000s where a third party vendor with political and ideological sympathies for al-Qaeda was providing engineering maintenance at five different U.S.-based nuclear power plants.²¹² The individual, who would later be arrested in 2010 by security forces in Yemen during a raid on regional al-Qaeda cell, was able to pass federal background checks and have access to IT systems at the plants from 2002 to 2008. Not only does this U.S. example among the others highlighted in this section reinforce the insider cyber threat to critical services and systems in Canada, but recent survey statistics from the private sector also reflect a growing concern of privileged insiders. A 2018 study from Cybersecurity Insiders and Crowd Research Partners titled “Insider Threat Report” asked over 450 IT security professionals working in government, private industry and critical infrastructure sectors their opinions on the growing risk of insider threats.²¹³ The survey indicates that, “90% of organizations feel vulnerable to insider attacks. The main enabling risk factors include too many users with excessive access privileges (37%), an increasing number of devices with access to sensitive data (36%), and the increasing complexity of information technology (35%).” While the vast majority of professionals recognized the threat, close to 53% actually confirmed insider attacks against their organization in the previous 12 months.

²¹¹ Ibid., 2.

²¹² Ibid., 4-5

²¹³ Holger Schulze, “Insider Threat Report 2018,” *Crowd Research Partners with Cybersecurity Insiders*, November 2018, <https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf>.

A follow-up assessment from IT World Canada on the “Insider Threat Report”, which included a discussion with Robert Marti, director of privileged access management with CA Technologies, specifically outlined that organizations in Canada have strong security measures for the network perimeter but little internal defense or response measures for insiders.²¹⁴ While commenting on the report, Marti noted that, “The findings show that an equal amount of attention is needed to deal with outside threats, malicious inside threats and accidental inside threats.”²¹⁵ These comments and the figures from the report emphasize the need for insider threats to be recognized as a strategic challenge within Canada’s critical infrastructure cybersecurity policies. Whether the threat is linked to a nation-state’s geopolitical interests, a disgruntled an employee who is fired and somehow retains his user account privileges, a hacktivist supporting a civil cause, a terror group recruiting an employee to disrupt a system or upload malware or even IT contractors who make accidental or negligent mistakes, the risk of insiders enabling or directly conducting a cyber attack on essential infrastructure operations poses an active safety and national security risk to Canadians. Consequently, the country’s future cybersecurity authorities overseeing and auditing critical infrastructure operators and owners needs to ensure adequate controls are in place to mitigate the insider threat ecosystem.

²¹⁴ Cindy Baker, “Trusted Insiders Are Now The Most Serious Security Threat,” *IT World Canada*, February 1, 2018, <https://www.itworldcanada.com/article/trusted-insiders-are-now-the-most-serious-security-threat/401284>.

²¹⁵ *Ibid.*

THE STRATEGIC IMPACT OF CYBER ATTACKS ON CRITICAL INFRASTRUCTURE

The previous chapters have highlighted how there are unique and active vulnerabilities within industrial and non-industrial critical infrastructure IT systems across Canada in addition to there being a range of threat actors seeking to exploit these vulnerabilities. However, during a 2017 cybersecurity summit in Toronto, Scott Jones, a former assistant deputy minister at CSE, reinforced the fact that Canada has, “Yet to suffer a massive critical infrastructure attack and we’ve yet to suffer a massive loss of [sector] capability.”²¹⁶ Since Canada faces vulnerabilities and threats but has not yet been the target of a successful large-scale cyber attack on critical infrastructure, this chapter will have to rely on past cyber attacks and incidents that have occurred in adversarial and allied countries around the world to highlight the consequences of failing to mitigate strategic cybersecurity risks.

Key events that this chapter will review will be the Ukraine power grid attack in 2015, the U.S.-Israeli Stuxnet computer worm targeting Iranian nuclear infrastructure in 2010 and the WannaCry impact on Britain’s National Health Service (NHS) in 2017. Although these examples are instances of successful attacks, there are numerous other examples where compromises occur but attacks were either stopped by network security teams before reaching full potential or the threat actor was simply not aiming to maximize damage in infected IT systems. For example, between 2010 and 2015, DHS’s ICS-CERT saw a 640% increase in the number of cases where industrial IT systems were in some way compromised.²¹⁷ The majority of these incidents were

²¹⁶ Sharp and Jim Finkle, “Canada Worried About Infrastructure Hacks: Intelligence Official.”

²¹⁷ Mutsuo Noguchi and Hirofumi Ueda, “An Analysis Of The Actual Status Of Recent Cyber Attacks On Critical Infrastructures,” *NEC Corporation*, accessed on February 1, 2019, <https://www.nec.com/en/global/techrep/journal/g17/n02/170204.html>.

remediated with no impact on organizational or infrastructure uptime requirements, which reinforces the strategic difference between a compromise and an actual successful disruptive attack. This trend is also reflective of the attack rate in Canada, where infrastructure sectors have routinely suffered compromises—such as the North Korea incident with Ontario’s Transit Authority—but no actual disruptive activities on essential service operations ensued.

The general purpose of this chapter is to analyze a few examples of how technical vulnerabilities in industrial and non-industrial sectors combined with a motivated threat actor can result in an infrastructure cybersecurity failure that harms public interests and adversely impacts national security. Each example will draw on vulnerabilities and threat actor typologies outlined in previous chapters.

Ukraine Electrical Grid Shutdown, 2015

On December 23, 2015, temporary malfunctions throughout the electrical grids in three Ukrainian provinces resulted in power outages that lasted up to six hours and affected 225,000 customers—including government offices, businesses and private residences.²¹⁸ After extensive digital forensic investigations and root-cause analysis, asset owners and government officials recognized that the malfunctions were actually the result of a comprehensive cyber attack. Subsequent investigations would indicate that Russian intelligence groups and associated APT actors were responsible for the incident, though official attribution remains contested.²¹⁹ As many sources indicate, this attack was the first event where a successful cyber-induced operation

²¹⁸ Kevin Owens et al., “Ukraine Cyber-Induced Power Outage: Analysis And Practical Mitigation Strategies,” *Schweitzer Engineering Laboratories, Inc.* (paper presented at the Power and Energy Automation Conference, Spokane, Washington, March 21, 2017), 1-2.

https://www.eiseverywhere.com/file_uploads/aed4bc20e84d2839b83c18b_cba7e2876_Owens1.pdf.

²¹⁹ Abir Shehod, “Ukraine Power Grid Cyberattack And U.S. Susceptibility: Cybersecurity Implications Of Smart Grid Advancements In The U.S.,” *MIT Sloan School of Management* (working paper at the Cybersecurity Interdisciplinary Systems Laboratory, Cambridge, MA, December 2016), 8. <https://cams.mit.edu/wp-content/uploads/2016-22.pdf>.

disrupted a national electric power grid.²²⁰ These disruptions were financially costly for regional businesses and government offices and forced the utility companies to undergo extensive IT repairs, including the re-uploading of authentic code to compromised software systems and the physical replacement of destroyed hardware assets.²²¹ From a more strategic standpoint, the attack highlighted the consequences a cyber attack on critical infrastructure could have on a general population, as if the power had remained interrupted for longer periods of time their would have been highly damaging and cascading effects across hospitals, schools, transportation routes, communications and even the food supply chain.

Beginning in March of 2015, the attackers, imitating as the Ukrainian Energy Ministry, used spear phishing techniques to send fake attachments to many national electricity provider offices.²²² Employees at three different regional utilities opened the Microsoft attachments that were in these emails, which actually contained malicious code embedded in the macros of the files. Once the employees selected to enable the macros, the embedded code automatically executed and resulted in the installation of Black Energy 3 malware (BE3). The malware provided the attackers with a temporary remote connection to their command control (C2) infrastructure, allowing them to extract network reconnaissance data and study it for a period of at least six months.²²³ During this analysis phase, the attackers also moved laterally throughout corporate networks, where they conducted brute force password attacks to compromise domain controllers and an Active Directory (AD)—providing them with additional user credentials.²²⁴

With these credentials and with the traditionally weak authentication procedures on control

²²⁰ Ibid., 2.

²²¹ Robert M. Lee, Michael J. Assante and Tim Conway, “Analysis Of The Cyber Attack On The Ukrainian Power Grid: Defense Use Case,” *Electricity Information Sharing and Analysis Center*, March 18, 2016, pg. 3, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

²²² Owens et al., “Ukraine Cyber-Induced Power Outage: Analysis And Practical Mitigation Strategies,” 2.

²²³ Shehod, “Ukraine Power Grid Cyberattack And U.S. Susceptibility: Cybersecurity Implications Of Smart Grid Advancements In The U.S.,” 5.

²²⁴ Ibid., 5, 26.

system networks, the attackers were able to establish an encrypted tunnel via a virtual private network (VPN) directly interfacing with ICS-liked computers.²²⁵ These workstations, which managed and interacted with distributed electrical grid assets and SCADA systems, allowed the attackers to begin coordinating and planting their primary attack.

Using the stolen credentials from Domain Controllers the attackers were able to access control networks as authorized users, which made their movements and activities difficult to detect. With this advantage, the attackers first located the uninterruptible power supply (UPS) devices that would allow local computers to keep running for a short period of time even after the attackers took down the primary power source.²²⁶ Since the ICS operators and IT staff relied on the power that was produced by the grid they oversaw, the attackers wanted to ensure that once the grid was offline the operators would lose both their primary and backup electricity. This would leave them completely disconnected from their field assets, thereby protecting the attackers' ongoing operation. At one of the facilities impacted by the attack, the UPS software was reconfigured to deactivate itself after the attacker caused the wide-scale outage.²²⁷ When the UPS devices were signaled to provide the backup power, they simply deactivated. Almost all computer machines and systems in the control environment were subsequently shutdown, which included downtime for mission-critical data centers and certain back-office IT operations.

Next, the attackers leveraged their authorized presence on control center workstations to enable remote connections to serial-to-Ethernet field devices located at geographically dispersed substations.²²⁸ The attackers then pushed malicious firmware versions to these devices, which would ensure that commands from the operators travelling over Ethernet communication

²²⁵ Lee, "Analysis Of The Cyber Attack On The Ukrainian Power Grid: Defense Use Case," 2-3.

²²⁶ *Ibid.*, 7-8.

²²⁷ *Ibid.*

²²⁸ Owens et al., "Ukraine Cyber-Induced Power Outage: Analysis And Practical Mitigation Strategies," 1-2.

protocols would not be converted to the serial protocols needed to communicate with PLCs and local control technologies at the substations. Effectively, this would cut the control center and its operators off from managing the physical components of their field systems, leading to a complete disruption of the SCADA architecture.²²⁹ Since the attackers had remote interactive access to compromised control network workstations, they simply began their attack by commanding more than 50 substations to go offline.²³⁰ This was followed by the execution of the malicious firmware already uploaded to the serial-to-Ethernet convertors, which made the devices inoperable and unreachable by any employees in the control center aiming to bring the substations back online. As the primary power outages proliferated and the pre-planned UPS attack automatically commenced, backup power supply to the control centers also deactivated. This resulted in data center and corporate IT disruptions at multiple company facilities and made the operator task of gaining control of their field devices extremely challenging.

Lastly, the attackers used a customized KillDisk malware program to wipe the system files off of operator workstations, which like the serial-to-Ethernet convertor attacks, made the computers inoperable.²³¹ KillDisk is essentially a piece of malware that wipes or overwrites data in important files, which ultimately causes a computer to crash. Rebooting the computer is not an option because KillDisk also overwrites the master boot data on hard drives. General management, finance, human resources and a wide-range of ICS servers and devices were targeted with the malware.²³² Although the malware variants and the interruptions to the SCADA system were the key features of the primary power supply disruption, there were also

²²⁹ Shehod, "Ukraine Power Grid Cyberattack And U.S. Susceptibility: Cybersecurity Implications Of Smart Grid Advancements In The U.S.," 5-6.

²³⁰ Owens et al., "Ukraine Cyber-Induced Power Outage: Analysis And Practical Mitigation Strategies," 1, 3.

²³¹ Lee, "Analysis Of The Cyber Attack On The Ukrainian Power Grid: Defense Use Case," 8.

²³² Shehod, "Ukraine Power Grid Cyberattack And U.S. Susceptibility: Cybersecurity Implications Of Smart Grid Advancements In The U.S.," 7.

supplemental attacks that contributed to a slow and uncoordinated incident response. For example, the malicious actors launched a telephony-based denial of service operation targeting the impacted energy companies and government offices assisting in the response. This leveraged the same tactics of a DDoS attack on network or application servers but instead aimed to overload the phone systems to disrupt communication and emergency response efforts. Robert M. Lee, a former Cyber Warfare Operations Officer for the U.S. Air Force and the co-founder of Dragos Security, noted in 2016 that, “It was brilliant. In terms of sophistication, most people always focus on the malware that’s used in an attack. To me what makes sophistication is logistics and planning and operations...this was highly sophisticated. What sophisticated actors do is they put concerted effort into even unlikely scenarios to make sure they’re covering all aspects of what could go wrong.”²³³ Lee’s comments highlight the technical challenges such an intensive and well-planned operation can pose for even well funded and trained cybersecurity programs in Canada aiming to protect critical infrastructure systems.

Although this incident has a visceral connection to Russia due to the geopolitical conditions at the time, Lee also stated that, “This had to be a well-funded, well-trained team. But it didn’t have to be a nation-state.”²³⁴ These comments reinforce the trend highlighted in the previous chapter where APT groups are no longer only associated with governments and that exploit technology proliferation and wider access to advanced computer security education are raising the technical profiles of non-state actors. The attack not only provides insight on technical cyber risks in industrial critical infrastructure sectors but it also highlights how a potential adversary may employ cyber operations during a period of hybrid hostility or strategic

²³³ Kim Zetter, “Inside The Cunning, Unprecedented Hack Of Ukraine’s Power Grid,” *WIRED*, March 3, 2016, <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>.

²³⁴ Steven Luber, “Information War Or Cyber War? Exploring The Russo-Ukrainian Digital Conflict,” *Leksika*, December 27, 2016, <http://www.leksika.org/tacticalanalysis/2016/12/27/information-war-or-cyber-war-exploring-the-russo-ukrainian-digital-conflict>.

conflict. For example, though no official attribution was assigned to the Russian government, it is worth noting that in the year before the incident Russian paramilitary forces invaded Crimea, Ukraine and began supporting an armed rebellion in the country's Eastern provinces—which was still ongoing during the time of the cyber attack.²³⁵

During this conflict, Russian backed security forces leveraged hybrid warfare techniques to confuse Ukrainian political decision-making processes and to disturb Ukrainian allied military activities in and near the conflict zone. A report from The Henry M. Jackson School of International Relations at Washington University details how Russian forces have, “Combined cyber warfare tactics with traditional strategy to create a new type of hybrid warfare that relies on proxies and surrogates to prevent attribution and intent, and to maximize confusion and uncertainty.”²³⁶ This approach to inducing complex conflict environments is consistent with the timing and sophistication of the power grid attack, further demonstrating how Russia has leveraged cyberspace as a technical tool for achieving strategic objectives in addition to supporting geopolitical interests—with limited international legal and political liabilities.

Ukraine is an ally of Canada, and in the year following Russia's Crimea invasion, the CAF launched Operation UNIFIER.²³⁷ As described by Canada's Department of National Defense, UNIFER was created to provide military support to the Security Forces of Ukraine. This geopolitical context and Canada's distant involvement in a foreign issue at odds with Moscow's interests provides an indication of why and how Canada may be targeted by a similar

²³⁵ Shehod, “Ukraine Power Grid Cyberattack And U.S. Susceptibility: Cybersecurity Implications Of Smart Grid Advancements In The U.S.,” 8.

²³⁶ Donghui Park, Julia Summers and Michael Walstrom, “Cyberattack On Critical Infrastructure: Russia And The Ukrainian Power Grid Attacks,” *University of Washington: Henry M. Jackson School of International Relations*, October 11, 2017, <https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/>.

²³⁷ Canadian Armed Forces, “Operation UNIFIER,” *Department of National Defense: Operations and Exercises*, last modified December 3, 2018, <https://www.canada.ca/en/department-national-defence/services/operations/military-operations/current-operations/operation-unifier.html>.

strategic cyber operation in the future—not necessarily by Russian-linked actors, but by any type of APT group with intent and capability. The prospect of this type of sustained attack on the same scale of the Ukrainian cyber incident but longer in duration reflects a scenario where financial, safety, healthcare, communications, transport and numerous other critical infrastructures would face a cascading disruption impacting Canada’s economy and national security.

Stuxnet Computer Worm in Iran, 2010

In 2010, Israel and the U.S. launched a malicious computer worm targeting Iran’s nuclear infrastructure, which at the time and even today has been criticized for supporting a nuclear weapons development program.²³⁸ Although the actors behind this attack are close allies of Canada, the 2010 operation is another useful case study for understanding the physical damage that could occur as a result of industrial IT compromises. Additionally, the attack highlights how cyberspace can be used as a strategic tool for achieving geopolitical objectives when more traditional physical, military or political means are not feasible. This point is particularly important, as the Stuxnet example reflects how the U.S. and Israel leveraged cybersecurity weaknesses in Iran to specifically slow down or disable key components of the country’s nuclear development when options such as sanctions and military intervention were either ineffective or unfeasible. The geopolitical nature of the operation was also evident from Tehran’s response, which as a result of the incident began laying the foundation of the country’s Cyber Defense Command and a new cybersecurity unit under the Passive Defense Organization (PDO) to

²³⁸ Paul Mueller and Babak Yadegari, “The Stuxnet Worm,” *University of Arizona: Department of Information Sciences*, pg. 1-2, 2012, <https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/topic9-final/report.pdf>.

protect domestic networks and systems from foreign adversaries.²³⁹ ²⁴⁰ While the country's immediate reactions centered on standing up new defensive capabilities, Iran also increased its offensive cyber activity—including the use computer-based financial crime and intellectual property (IP) theft to support the country's economy and to strategically position themselves within important adversarial IT systems. Iran, in addition to other countries around the world, observed the Stuxnet operation as the introduction of a new era in geopolitical competition requiring the development of new doctrines and tools to pressure foreign competitors in the digital space.

Stuxnet's advanced payload utilized four different zero-day exploits affecting Windows OS and Siemens industrial control software.²⁴¹ The computer worm was delivered via USB directly into one of Iran's primary nuclear enrichment facilities, the Natanz site, which is located just South of the country's capital of Tehran.²⁴² The insider who initially connected the USB to a computer port at the facility is believed to have been a contractor, though it is unclear whether he/she was acting maliciously or inadvertently. Once connected to the computer, the worm was uploaded and was immediately able to begin spreading across the control network as the infected computer was situated directly at an industrial facility already integrated with ICS equipment and SCADA systems. Stuxnet's malware utilized at least two stolen digital certificates, which are traditionally used to cryptographically guarantee the trustworthiness of a piece of software.²⁴³ The certificate does this by communicating with an OS that a file has not been tampered with or

²³⁹ Banisar and Melendez, "Tightening The Net Part 2: The Soft War And Cyber Tactics In Iran," 8.

²⁴⁰ Michael Connell, "Deterring Iran's Use Of Offensive Cyber: A Case Study," *CNA Analysis and Solutions and Defense Technical Information Center (DTIC)*, pg. 4, 6-7, October 2014, <https://apps.dtic.mil/dtic/tr/fulltext/u2/a617308.pdf>.

²⁴¹ David Kushner, "The Real Story Of Stuxnet," *IEEE Spectrum*, February 26, 2013, <https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>.

²⁴² Ibid.

²⁴³ Dan Goodin, "Stuxnet-Style Code Signing Is More Widespread Than Anyone Thought," *ARS Technica*, November 3, 2017, <https://arstechnica.com/information-technology/2017/11/evasive-code-signed-malware-flourished-before-stuxnet-and-still-does/>.

corrupted after its original publisher or author completed its development. If a virus infects a file after it has been digitally signed then it breaks the digital signature, and an OS such as Windows would refrain from executing the file. However, if a file is infected and then digitally signed, the result is a piece of software with embedded malicious code that can be verified as safe for execution on a computer system. The Stuxnet worm bypassed detection tools by leveraging this masking technique, which facilitated the spread of malware on ICS devices and nuclear production equipment at nearly 14 facilities across Iran.²⁴⁴

As Stuxnet replicated itself across the control network, it was searching for Windows-based equipment that was operating Siemens Step7 industrial software.²⁴⁵ Unique rootkits allowed the attackers to gain administrator level access to multiple PLCs using these Step7 programs, which then enabled a read and modify function for all communications being sent from the control center to field equipment—and from field equipment to control center workstations.²⁴⁶ There were at least three different modules within Stuxnet’s primary attack sequence, and with the worm using rootkits to embed malicious code directly into parts of the PLC OS, security controls and detection software at the Iranian facilities were unable to recognize any abnormal activity. Stuxnet commanded these PLCs to spin the uranium centrifuges at the Natanz nuclear facility outside of its normal operating parameters, which ultimately induced catastrophic damage.²⁴⁷

Briefly, a centrifuge is a piece of equipment that increases the concentration of the active isotope of uranium, U-235, which is an essential ingredient for both nuclear reactors and nuclear weapons. By spinning the centrifuges outside of their normal parameters—both too fast and too

²⁴⁴ Kushner, “The Real Story of Stuxnet.”

²⁴⁵ Mueller and Yadegari, “The Stuxnet Worm,” 3, 5-6.

²⁴⁶ Ibid.

²⁴⁷ Kushner, “The Real Story of Stuxnet.”

slow multiple times over several months—the U.S.-Israeli worm was able to slowly destroy 984 centrifuges, which was nearly 20% of the entire processing capacity at the Natanz facility.²⁴⁸ The compromised PLCs relayed inaccurate information to the operators in the control center of the facility, which indicated normal centrifuge spinning speeds when in reality they were slowly incurring damage. This cyber attack set back the Iranian nuclear program at least two years, inducing significant financial costs for the government and creating challenges for their foreign policy and regional geopolitical objectives. Although this attack was largely a strategic success for Canada’s allies, the destructive potential that was demonstrated not only influenced Iran to accelerate their offensive cyber capability programs but also showed state and non-stat actors across the world how a cyber weapon could be used for physical effect objectives.²⁴⁹

Kaspersky Lab and Symantec investigations on Stuxnet revealed that the worm’s presence on Iranian control networks was a result of a USB being compromised at a third party vendor who provided engineering support to centrifuges across the country.²⁵⁰ Security researchers noted that the Natanz facility had no known vulnerable Internet connections, stating that, “The targeting of certain high profile companies was the solution and it was probably successful.”²⁵¹ These comments refer to the specific targeting of manufacturers and vendors who serviced the Natanz site, which included Stuxnet uploads on machines at Neda Industrial Group and Foolad Technic Engineering Company—who were both involved in industrial automation software—in addition to other Iranian-based companies such as Mobarakeh Steel Company and

²⁴⁸ Michael Holloway, “Stuxnet Worm Attack On Iranian Nuclear Facilities,” *Stanford University*, July 26, 2015, <http://large.stanford.edu/courses/2015/ph241/holloway1/>.

²⁴⁹ Jo Lauder, “Stuxnet: The Real Life Sci-Fi Story Of The World's First Digital Weapon,” *ABC Net*, October 12, 2016, <https://www.abc.net.au/triplej/programs/hack/the-worlds-first-digital-weapon-stuxnet/7926298>.

²⁵⁰ Jon Fingas, “Stuxnet Worm Entered Iran's Nuclear Facilities Through Hacked Suppliers,” *Engadget*, November 13, 2014, <https://www.engadget.com/2014/11/13/stuxnet-worm-targeted-companies-first/>.

²⁵¹ Lucian Constantin, “First Stuxnet Victims Were Five Iranian Industrial Automation Companies,” *PC World*, November 12, 2014, <https://www.pcworld.com/article/2846852/first-stuxnet-victims-were-five-iranian-industrial-automation-companies.html>.

Behpajoo Electric & Engineering Company. One of the key vendors targeted was Kalaye Electric, who was the main manufacturer of the Iranian uranium enrichment centrifuges.²⁵² The Kaspersky report states that, “It appears quite reasonable that this organization of all others was chosen as the first link in the infections chain intended to bring the worm to its ultimate target.”²⁵³ This case study is a useful example of how the vast amount of vendors and third-party stakeholders supporting critical infrastructure in Canada can be used as an entry point for damaging malware to reach vital IT systems. Further, since an insider—who was either acting unknowingly or maliciously—transferred the computer worm via a USB inside the secure Natanz facility, the example also demonstrates the real impact an insider can pose.

While the threat actors in this example involve two of the most advanced allied cyber powers in the world, and two governments who pose no strategic risks to Canada, it is still important to recognize the technical and policy impact of the attack of itself. For example, Stuxnet’s highly effective code—alike the operation in Ukraine—demonstrates that vulnerable ICS equipment and control networks can allow an actor to cause significant physical disruptions. Although the Stuxnet malware was crafted and tested to ensure only certain functionality would be altered, an untested version with less control and technical specificity could have posed a much larger radiation-based health risk to nearby civilian populations in Iran.^{254 255}

As of 2017, there were five large nuclear power production facilities in Canada with a total of 19 reactors in commercial operation, which accounted for close to 20% of total electricity

²⁵² Ibid

²⁵³ Ibid.

²⁵⁴ Conor Gaffey, “Cyberattack On Nuclear Facilities Could Cause Radiation Leak: Report,” *Newsweek*, October 5, 2015, <https://www.newsweek.com/nuclear-power-stations-cyberattacknuclear-power-plants-cyberattacknuclear-599233>.

²⁵⁵ “Russia Says Stuxnet Could Have Caused New Chernobyl,” *Reuters: News Bulletin*, January 26, 2011, <https://www.reuters.com/article/us-iran-nuclear-russia/russia-says-stuxnet-could-have-caused-new-chernobyl-idUSTRE70P6WS20110126>.

demands across the country.²⁵⁶ In 2018, Canadian Nuclear Laboratories (CNL), Canada's premier nuclear science and technology organization, created the National Innovation Center for Cybersecurity with the intent of improving nuclear and other critical infrastructure cybersecurity across the country. In a statement on the new Center, CNL explained that, "While there is a large commercial industry catering to the cyber security of business and information technology systems, the cyber security of industrial control systems has been widely overlooked. Yet, this critical sector has shown vulnerabilities, with recent attacks on the Ukraine power grid in 2015 and 2016, a German steel mill in 2014, and the well-known Stuxnet attack in 2010."²⁵⁷ These comments reinforce how critical infrastructure stakeholders in Canada view the nearly decade-old Stuxnet attack as a lingering indicator of active cyber risks across industrial IT environments.

The CNL statement in 2018 also explained that, "Every year, the instruments, controls, and monitors that keep Canada's most valuable energy assets running smoothly become more automated. This transformation offers tremendous benefits to Canadians, but it also presents new risks to the country's energy grid and other major infrastructure."²⁵⁸ The Stuxnet and Ukraine power grid case study that this chapter has reviewed demonstrates the strategic consequences cybersecurity failures throughout vital industrial IT environments can induce. Not only do these incidents prove the geopolitical or security utility of infrastructure cyber attacks, but they also demonstrate the growing trend of threat actors leveraging vulnerabilities in SCADA-linked assets. Therefore, understanding that a range of different actors with varying levels of technical

²⁵⁶ Canadian Nuclear Safety Commission, "Regulatory Oversight Report For Canadian Nuclear Power Generating Sites: 2017," *Ministry of Natural Resources*, November 8, 2018, <http://www.nuclearsafety.gc.ca/eng/the-commission/meetings/cmd/pdf/CMD18/CMD18-M39.pdf>.

²⁵⁷ Patrick Quinn, "CNL Opens National Innovation Centre For Cybersecurity," *Canadian Nuclear Laboratories (CNL)*, May 16, 2018, <http://www.cnl.ca/en/home/news-and-publications/news-releases/2018/cnl-opens-national-innovation-centre-for-cybersecu.aspx>.

²⁵⁸ *Ibid.*

sophistication are actively scanning and planning cyber attacks on Canada's ICS-dependant sectors needs to be a core national security priority for the country moving forward.

From a long-term policy perspective, it is worth noting that many government and private industry cybersecurity stakeholders have disapproved of deploying such an advanced computer weapon in the wild—noting a potential blowback affect. During a 2011 Senate Committee on Homeland Security and Governmental Affairs meeting, President and CEO of the National Board of Information Security Examiners of the United States, Inc., Michael Assante, stated that, “The [Stuxnet] worm stands as not only a blueprint for entities sophisticated enough to reproduce a Stuxnet-like attack—such as Russia or China—but an attacker with less means could still use parts of the code to wreak less-controlled havoc.”²⁵⁹ A subsequent congressional report discussing the implications of the Stuxnet attack noted that, “It is widely believed that terrorist organizations do not currently possess the capability or have not made the necessary arrangements with technically savvy organizations to develop a Stuxnet-type worm. However, Stuxnet's design revelations may make it easier for terrorist organizations to develop such capabilities in the future.”²⁶⁰ The damaging impact Stuxnet had on Iranian infrastructure and the technical capabilities that the U.S and Israel demonstrated to the world not only ushered in the era of strategic cyber operations, but it also exposed advanced attack know-how for state and non-state actors to augment their indigenous cyber capabilities. Moving forward, Canada and its allies will need to be cautious with how and where their offensive cyber activity occurs as once toolkits, TTPs and code are operationalized in the wild, adversaries—both state and non-state—will have access to these exploits and may leverage them against friendly assets in the future.

²⁵⁹ Lee Ferran, “Stuxnet: Could Cyber Superweapon Be Turned On U.S.?” *ABC News*, January 28, 2011, <https://abcnews.go.com/Blotter/stuxnet-cyber-super-weapon-turned-us/story?id=12767405>.

²⁶⁰ *Ibid.*

WannaCry Ransomware Virus and Britain's Healthcare System, 2017

In May of 2017, a computer virus known as WannaCry was released worldwide impacting at least 150 countries and causing nearly \$4 billion USD in ransomware payment and IT reimaging, data retrieval and system restoration costs.²⁶¹ While the WannaCry virus was not targeted at a specific country or organization, and while its developers were certainly financially motivated, the virus had a unique strategic impact on Britain where the country's national healthcare system experienced serious disruptions. The impact of these disruptions was costly from a monetary standpoint and threatening to the health and safety of British citizens seeking treatment at medical facilities across the country. While the Iranian and Ukrainian examples focus on industrial IT vulnerabilities and cyber attacks, this example will focus on a non-industrial environment—Britain's healthcare infrastructure.

WannaCry's ransomware encrypts data on infected computers and demands a ransom payment to allow user access. WannaCry made use of an exploit tool that was first developed by the U.S. National Security Agency (NSA), which was called EternalBlue.²⁶² This exploitation tool, among many others, were publically released by a hacking and activist collective known as The Shadow Brokers on April 14, 2017—just one month before the WannaCry launch.²⁶³ EternalBlue allowed the creators of WannaCry to take advantage of vulnerabilities in the Microsoft Windows implementation of Server Message Block (SMB) protocol.²⁶⁴ SMB protocol is a standard transport protocol used by Windows machines for a wide variety of purposes such as file sharing and access to remote Windows services, in addition to generally facilitating

²⁶¹ Jonathan Berr, "WannaCry Ransomware Attack Losses Could Reach \$4 Billion," *CBC News*, May 16, 2017, <https://www.cbcnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/>.

²⁶² Technical Intelligence Group, "WannaCry Ransomware Attack," *EY*, May 2017, pg. 3-4, [https://www.ey.com/Publication/vwLUAssets/ey-wannacry-ransomware-attack/\\$File/ey-wannacry-ransomware-attack.pdf](https://www.ey.com/Publication/vwLUAssets/ey-wannacry-ransomware-attack/$File/ey-wannacry-ransomware-attack.pdf).

²⁶³ *Ibid.*

²⁶⁴ Nadav Grossman, "EternalBlue – Everything There Is To Know," *Check Point Research*, September 19, 2017, <https://research.checkpoint.com/eternalblue-everything-know/>.

communication between nodes on a network. The vulnerability in the protocol allows the virus to execute malicious code on target computers and machines after securing a connection to an exposed SMB port. Once a machine is successfully infected with the malware, the virus will scan local networks searching for additional machines with vulnerable SMB ports attempting to spread its reach.²⁶⁵ The second component of the virus is the ransomware functionality, which then begins to encrypt a wide range of important files on infected computers and machines, including Microsoft Office files, system operation files and other sensitive data. WannaCry also checks targeted computers for a DoublePulsar infection, which is a separate backdoor tool released in the April by the Shadow Brokers leak that also takes advantage of SMB port vulnerabilities.²⁶⁶

While Microsoft publically expressed their anger and dissatisfaction with the NSA for developing an exploit for one of their OS vulnerabilities without informing them of the flaw, the company had already discovered the vulnerability indigenously and released a patch in March of 2017. This patch was highly effective and most organizations implementing the patch did not have their Windows systems or machines compromised by WannaCry.²⁶⁷ A report from Britain's National Audit Office (NAO) in April 2018 notes that the National Health Service (NHS) and the Department of Health, "Had issued critical alerts warning organisations to patch their systems." The report later adds that before May 2017—which was when WannaCry launched—NHS and the Department, "Had no formal mechanism for assessing whether local NHS organisations had complied with their advice and guidance and whether they were prepared for a

²⁶⁵ Nicole Oppenheim, Ali Islam and Winny Thomas, "SMB Exploited: WannaCry Use Of EternalBlue," *FireEye*, May 26, 2017, <https://www.fireeye.com/blog/threat-research/2017/05/smb-exploited-wannacry-use-of-eternalblue.html>.

²⁶⁶ Technical Intelligence Group, "WannaCry Ransomware Attack," 1.

²⁶⁷ *Ibid.*, 16.

cyber attack.”²⁶⁸ This lack of patch management oversight was catastrophic, as many medical facilities, providers and organizations throughout the country’s healthcare infrastructure were still operating on out-dated and vulnerable Windows XP software.

Once the virus began spreading, about 34% of Britain’s regional medical districts—referred to as Trusts—experienced major disruptions. The NAO report notes that, “In total at least 81 out of 236 trusts across England were affected. A further 603 primary care and other NHS organisations were infected by WannaCry, including 595 GP practices.”²⁶⁹ Over a seven-day period, there were at least 19,000 healthcare appointments—including 139 essential cancer treatments—that were cancelled and at least seven medical districts had to divert urgent care patients away from hospital emergency departments due to vital IT system lockouts that were demanding ransom payment.²⁷⁰

Many cybersecurity firms and governments attributed the WannaCry virus to an APT actor associated with the North Korean government called the Lazarus Group.²⁷¹ While the actor was not targeting Britain or national healthcare infrastructure specifically, the virus posed a real national security risk in terms of financial damage and the possibility of physically impacting the safety of many citizens. HealthCareCAN, formerly known as the Canadian Healthcare Association, conducted a member-based survey with hospitals, medical research centers and universities in May 2017 following WannaCry’s impact on Britain’s NHS. The survey indicated that, “More than 8 in 10 health leaders said that Canada’s health sector is vulnerable to cyber attacks. Likewise, 86% of HealthCareCAN members say that their organization has detected a

²⁶⁸ “Investigation: WannaCry Cyber Attack And The NHS,” *National Audit Office (NAO)*, October 27, 2017, <https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/>.

²⁶⁹ *Ibid.*

²⁷⁰ *Ibid.*

²⁷¹ Josh Fruhlinger, “What Is WannaCry Ransomware, How Does It Infect, And Who Was Responsible?” *CSO Online*, August 30, 2018, <https://www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html>.

breach or narrowly avoided incident.”²⁷² These figures add urgency for developing a more comprehensive and resilient cybersecurity posture across the Canadian healthcare space and the non-industrial environment in general, particularly in the context of major events such as WannaCry. Atty Mashatan, a professor at Ryerson University's School of Information Technology Management, stated shortly after the launch of WannaCry that, “This time around we [Canada] were lucky,” adding that, “It was nothing more than a fluke that Canada appears to have been largely spared from Friday's ransomware attack that disrupted services in Russia, the U.K., Ukraine, Spain and India.”²⁷³

Recognizing the strategic risks associated with a cybersecurity failure in the healthcare sector demonstrates that strong security and incident response practices in non-industrial infrastructure environments are equally as important compared to the more physical industrial sectors, such as water, gas and oil, or electricity. Further, this case study also highlights a useful example regarding patch management programs across nationwide systems. Not only was a lack of patching a major cause for WannaCry’s disproportionate impact in Britain, but it was also highlighted in chapter two where difficulties patching software in the LVTS proved to be an ongoing source of systemic cyber risk for Canadian banks and the economy. Regardless of the sector—industrial or non-industrial—ensuring that key owner, operator and regulator stakeholders conform to adequate cybersecurity standards is the only verifiable approach to building a more resilient environment for the country’s most important and at risk digital systems.

²⁷² Jennifer Zelmer, “Cybersafe Healthcare: Options For Strengthening Cybersecurity In Canada’s Health Sector,” *Azimuth Health Group for HealthCareCAN*, September 2018, <http://www.healthcarecan.ca/wp-content/themes/camyno/assets/document/Cyber%20Security/Options%20Brief%20Summit%20Report.pdf>.

²⁷³ Nicole Thompson, “WannaCry Cyberattack Missed Canada On A Fluke: Professor,” *Huffington Post*, May 14, 2017, <https://www.huffingtonpost.ca/entry/16605402>.

Implications for Canada

Altogether, the three critical infrastructure cyber attacks reviewed in this chapter act as useful case studies for recognizing how Canada’s national interests could be harmed through cyber vulnerabilities—both technical and policy-based—being exploited across the country’s essential service landscape. While Canadian allies and not adversaries orchestrated the Stuxnet attack, the physical destruction that the operation induced to ICS and SCADA processes throughout Iranian nuclear infrastructure directly influenced risk perceptions associated with the integrity and availability of similar technologies and systems operating in Canada. This point was reinforced by CNL—a key nuclear science and technology organization in Canada previously referenced in this chapter—who specifically noted the Stuxnet attack as the reason for launching improved nuclear power cybersecurity initiatives across the country. Further, the same year of the Stuxnet operation, Canada’s Parliament directly prioritized remediation and protection against strategic cyber threats to critical infrastructure in a government publication that stated, “Stuxnet demonstrates the potential for well-resourced cyber-attacks to damage or destroy critical infrastructures.”²⁷⁴ Regardless of being an operation researched and executed by allied nations, the threat of Stuxnet’s code proliferation and the recognition by Canadian officials that similar TTPs could be used on infrastructure targets in Canada reinforces the point that Stuxnet directly transformed the perceived strategic risk landscape for nationally important IT systems—particularly those linked to nuclear power facilities.

Similar strategic risks to Canadian infrastructure assets were also realized after the 2015 cyber-induced Ukraine power grid failure. For example, in 2016, Prime Minister Justin Trudeau directed Public Safety Minister Ralph Goodale to assess all government operations and

²⁷⁴ Holly Porteous, “The Stuxnet Worm: Just Another Computer Attack Or A Game Changer?” *Library of Parliament: Parliamentary Information and Research Service*, pg. 3, October 7, 2010, http://publications.gc.ca/collections/collection_2010/bdp-lop/eb/2010-81-eng.pdf.

capabilities to determine whether the country could respond to a similar incident, citing that potential adversaries could exploit electrical systems in Canada. The issue was further discussed during a parliamentary committee hearing that same year where Conservative Member of Parliament (MP) Cheryl Gallant stated that, “The concern is that this type of sophisticated, planned, synchronized attack could occur in North America,” and that it is important for the government to, “Make sure that [such] a coordinated attack or perhaps a more sophisticated one does not impede our electricity system and all the items attached to the grid that we depend on.”²⁷⁵ Considering a foreign adversary was likely the source of the Ukraine attack and since the target of the attack was an official Canadian military partner, this incident directly influenced and educated Ottawa policymakers on the strategic issues surrounding critical infrastructure cybersecurity. Not only did it highlight the physical impact that a cyber operation could induce, but it also highlighted how a major event could directly deteriorate economic and security interests and require a significant amount of time, resources and technical expertise that were not necessarily available in Canada at the time to conduct a proper recovery. For certain sectors and organizations in Canada, this unpreparedness remains apparent to date. Gallant’s comments reinforce the trend of increased risk perception among Canadian officials—including the Prime Minister—who recognized the Ukraine incident and its technical complexities and geopolitical fallout as an indication of active and rapidly growing strategic cyber threats to Canadians and their infrastructure.

The WannaCry case study examined in this chapter also forced the Canadian government and its private industry partners to internalize the growing threat and likelihood of an actor exploiting vulnerabilities across the country’s most important assets. This realization was rooted

²⁷⁵ Susan Lunn, “Ralph Goodale Says Ukraine Cyberattack Caused International Anxiety,” *CBC News*, March 8, 2016, <https://www.cbc.ca/news/politics/cybersecurity-ukraine-goodale-federal-review-1.3481433>.

in WannaCry ransomware, particularly in the context of Britain’s NHS, having a direct impact on the physical safety of citizens and the potential to induce a long-term strategic crisis for the country. Tom Bossert, a Homeland Security Advisor to the White House in 2017 noted that, “It affected individuals, industry, governments and the consequences were beyond economic. The computers affected badly in the U.K. in their health care system put lives at risk, not just money.”²⁷⁶ As noted in the previous section, HealthCareCAN specifically collected industry and government survey data to reinforce the need for significant improvement of cybersecurity programs across Canada’s healthcare infrastructure in the aftermath of the virus. Further, since Canada and its closest allies attributed the WannaCry attack to North Korean security and intelligence groups—some of which have infiltrated Canadian critical infrastructure IT systems in the past—there is a clear indication that advanced threat actors interested in targeting Canada have both the technical capability and political willingness to execute a potentially catastrophic operation. When the impact of the these three case studies examined in this chapter are aggregated from a sophistication and financial/ physical damage standpoint, it becomes clear that the strategic risk facing Canadian and allied critical infrastructure has only continued to increase and become more challenging to mitigate.

²⁷⁶ Howard Solomon, “Canada Helped Confirm North Korea Behind WannaCry Ransomware, Says U.S.,” *IT World Canada*, December 19, 2017, <https://www.itworldcanada.com/article/canada-helped-confirm-north-korea-behind-wannacry-ransomware-says-u-s/400152>.

POLICY-BASED SOLUTIONS, RECOMMENDATIONS AND REMEDIATIONS

As the final chapter, the following sections will outline some key technical and policy solutions that would improve the current state of critical infrastructure cybersecurity in Canada. While the federal government and private industry have made improvements to their overall cyber posture in response to the growing sophistication and motivation of threat actors, there are still security gaps in the programs defending Canada's vital systems that will need to be addressed. The general approach that will be outlined in this chapter follows a three-tiered critical infrastructure cybersecurity strategy implemented by a coordinated public-private partnership. This chapter will break the three tiers down into individual sections.

The first section will discuss the need for minimum cybersecurity standards to be implemented and enforced using a framework-based approach, which would include developing security controls for infrastructure operators, regulators, owners and third parties. The implementation of these controls would be standardized across the country by using a common purpose-built Canadian version of the U.S. NIST critical infrastructure framework. This assessment tool could be constructed and tailored for specific sector needs in Canada as opposed to simply recommending the highly generic NIST version. The second section will advocate for government and private sector infrastructure stakeholders to adopt an assumption of compromise (AoC) culture to create a more proactive and threat-conscious environment for defending networks and important IT systems. Lastly, the third section will reinforce the need for federal and provincial governments to increase their communication and interaction with private stakeholders to ensure critical infrastructure operators and vendors are receiving real-time threat data. This will not only improve defenses and tailor cybersecurity programs to defend against

active threats, but it will also ensure that classified but useful information at federal intelligence agencies gets disseminated to necessary entities in a timely and non-redacted manner. Although recent developments indicate improvement, such as the first public release of a National Cyber Threat Assessment in 2018 and the growth of participation in the Canadian Cyber Threat Exchange (CCTX), this chapter will outline how there are still lingering policy barriers and challenges that need correcting before Canada's critical infrastructure systems can become more digitally secure.

Critical Infrastructure Cybersecurity: A Framework Approach

The overall objective of implementing a minimum cybersecurity standard for all stakeholders in each of Canada's ten critical infrastructure sectors is an extremely large and financially costly objective. Not only will these standards need to be technically different across sectors, but the risk assessments for different types of IT systems and the varying levels of private involvement will make the standards incompatible. Conducting oversight of this process and auditing for compliance purposes would create new administrative difficulties that would likely hinder this approach from the start.

To counter this challenge, the minimum cybersecurity standard should be implemented in a framework format where universal policy-based controls that are technology neutral are developed to help improve posture at all levels of the critical infrastructure industry—which includes regulators, owners, operators and vendors. By leveraging a universal framework, each sector would have the opportunity to subsequently narrow the focus of each control to ensure it is suitable and compatible with industry best practices, procedures and technologies. Developing one primary framework and requiring that all stakeholders meet a certain level of the

framework's implementation could itself become the national infrastructure cybersecurity standard. For example, each organization being assessed by the framework might need to meet a certain average maturity score to be considered as compliant under the standard, and a lack of compliance can mean fines or exclusion from servicing certain vital assets. This would be a much more cost, resource and time efficient approach compared to a segmented strategy focusing on individual sectors specifically. Instead, sectors could take the primary universal framework and work with government stakeholders, such as CSE, CSIS, CAF and Public Safety Canada to tailor controls or requirements where needed.

A key benefit of developing this cyber risk management framework is that DHS and NIST in the U.S. have already produced a comprehensive internationally renowned template that Canada's federal authorities could leverage. This template is called the "Framework for Improving Critical Infrastructure Cybersecurity" with the newest version being released in April of 2018.²⁷⁷ NIST describes their publication as a framework that, "Consists of standards, guidelines, and best practices to manage cybersecurity-related risk." More specifically, the publication notes that the framework's, "Prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security."²⁷⁸ Public Safety Canada has actually endorsed this type of concept, where a universal Canadian-centric cybersecurity framework could be generally applied across multiple sectors to assess regulators, owners, operators and vendors. For example, Public Safety's 2016 "Fundamentals of Cyber Security for Canada's Critical Infrastructure Community" states that the organization officially, "Endorses the NIST Framework and acknowledges the

²⁷⁷ "Framework For Improving Critical Infrastructure Cybersecurity," *National Institute of Standards and Technology*, pg. 2-3, April 16, 2018, <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.

²⁷⁸ *Ibid.*, iv-v.

relevance and applicability of the Framework in the Canadian context.”²⁷⁹ Additionally, a January 2017 “Cyber Review Consultations Report” also from Public Safety Canada, specifically highlighted that, “There are a number of industry standards and/or guidance documents that can be leveraged to help build an appropriate program...including the NIST Cybersecurity Framework for Critical Infrastructure.”²⁸⁰ In addition to these references, numerous other Public Safety, private industry and federal government reports highlight the utility in adopting a tailored version of the NIST framework as a high-level approach to creating a national infrastructure cybersecurity standard.

There have already been instances of sectors in Canada tailoring the NIST framework for their unique technological and operational needs. For example, in 2015, the Investment Industry Regulatory Organization of Canada (IIROC) released a “Cybersecurity Best Practice Guide” that refers to NIST’s primary control functions as, “A high-level, strategic view of the lifecycle of an organization’s management of cybersecurity risk.”²⁸¹ The guide then explains that adopting these functions would provide, “A proven process upon which to establish and manage cybersecurity program development” for Canada’s FMI.²⁸² Other sectors in addition to finance have also leveraged the NIST framework as a strategic guidance tool to build-out a more tailored cybersecurity program. A direct example of this has been the province of Ontario, who in 2017 developed and implemented the “Ontario Cyber Security Framework.”²⁸³ The Ontario framework was developed and coordinated by the Ontario Energy Board (OEB), which is the

²⁷⁹ “Fundamentals Of Cyber Security For Canada's CI Community,” *Public Safety Canada*.

²⁸⁰ “Cyber Review Consultations Report,” *Public Safety Canada*, January 17, 2017, <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/2017-cybr-rvw-cnslttns-rprt/index-en.aspx>.

²⁸¹ “Cybersecurity Best Practices Guide For IIROC Dealer Members,” Investment Industry Regulatory Organization of Canada (IIROC), pg. 11, December 15, 2015, http://www.iiroc.ca/industry/Documents/CybersecurityBestPracticesGuide_en.pdf.

²⁸² *Ibid.*, 13.

²⁸³ “Ontario Cyber Security Framework,” *Ontario Energy Board*, pg. 2, December 6, 2017, <https://www.oeb.ca/sites/default/files/Ontario-Cyber-Security-Framework-20171206.pdf>.

regulator and authority responsible for provincial electricity and natural gas production, distribution, safety and usage.

The OEB launched the framework for the purpose of having a common tool to evaluate the cybersecurity posture of small gas and electric Local Distribution Companies (LDCs) who tend to have less comprehensive, structured and official reporting capabilities compared to larger organizations.²⁸⁴ Instead of requiring these smaller companies to develop their own in-house assessment capabilities or paying for an outsourced cybersecurity audit, the OEB wanted a common template that they could apply across the province to any energy distribution organization to evaluate the province's overall infrastructure cyber resilience. The OEB explains that the province's, "Cyber Security Working Group developed an Ontario distributor and non-bulk transmitter Cyber Security Framework based on the NIST Cybersecurity Framework."²⁸⁵ The OEB primarily utilized the comprehensive foundation provided in the NIST document as opposed to developing a completely new approach, which not only saved money and provincial resources, but also created standardized cybersecurity control criteria that made tracking improvements and comparing resiliency evaluations between companies easier to understand over the long-term.²⁸⁶

In addition to the generic criteria listed in the NIST framework, the OEB also combined security controls and key risk indicators (KRI) created by the U.S. Department of Energy (DoE) into the Ontario Framework to provide more technically focused controls suited for the energy sector.²⁸⁷ The IIROC and OEB examples are exactly aligned with the policy recommendation

²⁸⁴ Ibid., 3, 5-6.

²⁸⁵ Ibid., 3.

²⁸⁶ "Ontario's Cyber Security Framework Is Now In Force," *Association of Power Producers of Ontario*, June 2018, <https://magazine.appro.org/news/ontario-news/5545-1529540280-ontario's-cyber-security-framework-is-now-in-force.html>.

²⁸⁷ "Ontario Cyber Security Framework," *Ontario Energy Board*, 8.

this section is providing, as in both cases Canadian regulatory bodies leveraged the well-developed NIST framework and tailored its content to more appropriately provide cybersecurity control and maturity assessment criteria as part of a Canadian sector-specific version. Additionally, the Ontario Framework is also a useful case study in terms of enforcement. For example, the OEB created a Central Compliance Authority (CCA) to track provincial implementation of the framework and to conduct routine audits to ensure baseline controls are being met and that maturity ratings were slowly improving.²⁸⁸ Without having a common assessment tool, the duties of the CCA would be administratively and technically challenging because each organization could be using different auditing or evaluation benchmarks and metrics.

At the federal level, there are also examples of critical infrastructure stakeholders adopting the NIST framework. In 2018, Health Canada—a federal government Department—recommended the use of the risk management practices outlined in the NIST publication to offset growing cybersecurity challenges across the industry ranging from privacy considerations to major attacks. The announcement states that stakeholders in the healthcare and medical supply chain sector should leverage the framework, “As a blueprint of best practices to guide their cybersecurity activities.”²⁸⁹ ²⁹⁰ Alike the energy and finance examples highlighted in the previous paragraphs, Health Canada noted that additional controls unique to the sector should also be utilized. For example, new cybersecurity challenges arising from medical equipment being linked to IoT devices are issues not entirely covered in the generic NIST framework.

²⁸⁸ “Ontario’s Cyber Security Framework Is Now In Force,” *Association of Power Producers of Ontario*.

²⁸⁹ Health Canada, “Draft Guidance Document,” *Health Canada: Public Consultation Review*, December 2, 2018, <https://www.canada.ca/en/health-canada/services/drugs-health-products/public-involvement-consultations/medical-devices/consultation-premarket-cybersecurity-profile/draft-guidance-premarket-cybersecurity.html#a2.2.5.1>.

²⁹⁰ Stewart Eisenhart, “Health Canada Setting Pre-Market Medical Device Cybersecurity Requirements,” *Emergo*, <https://www.emergobyul.com/blog/2018/12/health-canada-setting-pre-market-medical-device-cybersecurity-requirements>.

Also at the federal level, organizations such as the Canadian Water and Wastewater Association (CWWA) have recommended national water infrastructure owners and operators to implement derivatives of the NIST framework. Public and non-profit water system regulators have all indicated that using the framework can improve sector cybersecurity and create a standardized model capable of evaluating organizations, companies and vendors across the water processing and distribution system consistently. A 2017 report from the Critical Infrastructure Protection Initiative at Dalhousie University in Halifax, Canada, which was sponsored by Defense Research and Development Canada (DRDC), called for Canadian water sector stakeholders to implement a guidance document called the “Process Control System Security for the Water Sector (PCSWS).”²⁹¹ This document was explicitly created by the American Water Works Association (AWWA) as a “Voluntary, sector-specific approach for adopting the NIST Cybersecurity Framework.”²⁹² While the AWWA is not a Canadian-based regulatory or trade body, the 2017 Halifax study outlines how the CWWA supports the PCSWS approach and believes its use of the NIST framework can be effective for Canada’s national water sector stakeholders.²⁹³

The industrial and non-industrial examples discussed in this section—including finance, health, energy and water—clearly highlight the demand for using the NIST framework as a tool to improve cybersecurity oversight, controls, standardization and common enforcement measures across individual sectors in Canada. Although there is not yet a Canadian version of the NIST framework that could be deployed as the official generic cybersecurity assessment tool for the

²⁹¹ Calvin Burns, Kevin Quigley and Gwendolyn Moncrieff-Gould, “Strengthening The Resilience Of The Canadian Water Sector,” *Critical Infrastructure Protection Initiative at Dalhousie University*, pg. 133, December 15, 2017, https://www.cwwa.ca/pdf_files/Water_sector_vulnerability_REPORT.pdf.

²⁹² American Water Works Association (AWWA), “Process Control System Security Guidance For The Water Sector,” *AWWA and Water Industry Technical Action Fund (WITAF)*, October 2014, <http://www.nawc.org/uploads/documents-and-publications/documents/AWWACybersecurityguide.pdf>.

²⁹³ Burns, “Strengthening The Resilience Of The Canadian Water Sector,” 17-18, 133.

country, Public Safety Canada offers a review service that may be useful for developing a future Canadian-based version. The Department’s Canadian Cyber Resiliency Review (CCRR) program provides onsite cybersecurity assessments for critical infrastructure organizations based on, “Scores across the 10 domains of the NIST Cyber Security Framework.”²⁹⁴ The CCRR is voluntary and only organizations that specifically seek out and ask CSE or Public Safety Canada for assistance will receive the assessment, but it is worth noting that it is entirely based on applying the NIST controls and providing maturity ratings based on the framework.²⁹⁵ During the assessment, Public Safety Canada, along with private sector IT security experts and individuals from CSE or the Canadian Cyber Incident Response Center (CCIRC), work with critical infrastructure organizations to conduct a 1-2 day audit of current cybersecurity and risk management practices. The CCRR goes through the five primary framework functions of Identify, Detect, Protect, Respond and Recover in addition to assessing the maturity of each subcategory control within those five functions—which amounts to analyzing 108 controls.²⁹⁶ These controls range from hardware and software asset management, detection processes, system development lifecycles, business continuity plans, encryption, backups, logging, root cause analysis and third party risk assessments.

The use of the voluntary CCRR NIST-based assessment tool by Public Safety Canada in addition to the general demand of NIST framework resources across the country indicates support for this section’s recommendation of creating a Canadian cybersecurity framework program to be used by all critical infrastructure stakeholders.²⁹⁷ A key reason for developing a

²⁹⁴ “The Regional Resilience Assessment Program,” *Public Safety Canada*, August 13, 2018, <https://www.publicsafety.gc.ca/cnt/ntnl-scrtr/crtcl-nfrstrctr/crtcl-nfrstrtr-rrap-en.aspx>.

²⁹⁵ *Ibid.*

²⁹⁶ “Framework For Improving Critical Infrastructure Cybersecurity,” *National Institute of Standards and Technology*, 23-24.

²⁹⁷ Scott J. Shackelford Zachery Bohm, “Securing Critical North American Infrastructure: A Comparative Case Study In Cybersecurity Regulation,” *Canada-United State Law Journal* 40, no. 1 (2016): 69.

framework unique to the Canadian context as opposed to continuing to informally rely on the U.S. NIST version is that regulatory, legal and reporting structures in Canada are different than in the U.S. While the NIST framework was intentionally built to be generic enough for wide consumption across multiple sectors and even countries, a Canadian-based high-level framework would take into account operational, composition and regulatory features that only exist in Canada's critical infrastructure environments. These features can include the distinction of federal and provincial regulatory duties, data privacy and intelligence sharing laws, or even cross-sector resiliency collaboration requirements. Although each sector will need to tailor the framework's implementation to adjust for different technologies and processes, there are common issues that every stakeholder will need to address—such as how to formally report cyber incidents to federal intelligence agencies like the CCIRC—who is Canada's computer security incident response team and the main point of contact for critical infrastructure organizations when they need to report a cyber incident.²⁹⁸ Outlining these types of specific controls and contexts within the tailored Canadian framework would create less implementation ambiguity that may be associated with the generic NIST version, which is still being used in federal tools as pointed out in the CCRR.

The federal government does not need to provide direct oversight of each individual sector, but instead can delegate framework oversight responsibilities to regional or sector-specific organizations who can use the Canadian purpose-built framework to consistently, evenly and accurately measure security capabilities of owners, operators and vendors—just as the OEB and IIROC continue to do for their industries. For example, a regulator conducting a sector wide resiliency review can aggregate maturity scores collected during a framework compliance audit to determine the level of cyber risk in the sector from an objective perspective, as opposed to

²⁹⁸ “Fundamentals Of Cyber Security For Canada's CI Community,” *Public Safety Canada*.

relying on a wide range of reports from operators that have different control and assessment criteria. This first tier of the proposed critical infrastructure cybersecurity strategy would create a high-level framework tool that would provide policy makers, key sector stakeholders and regulators with more accurate, consistent and tailored information on the current state of cyber resilience at a given organization, the vendors in a sector and the sector as a whole.

Fostering an Assumption of Compromise (AoC) Culture

As outlined in chapter four, the threat actors interested in targeting Canada’s vital systems are continuing to increase their technical sophistication at a rapid rate. This is occurring while new ICT processes and systems, such as IoT, 5G and cloud computing are transforming how traditional IT environments across Canada’s critical infrastructure are operated. The combination of these trends and the persistence of vulnerable legacy hardware and software in both industrial and non-industrial sectors require Canadian owners, operators and vendors to change their cultural approach to cybersecurity. The second tier of a proposed critical infrastructure cybersecurity strategy is to foster an Assumption of Compromise (AoC) culture among all stakeholders across every sector. An AoC approach essentially moves enterprise security strategy away from the notion that sophisticated threats—such as APTs—can be prevented from accessing protected networks, meaning cybersecurity programs need to recognize that breaches or compromises will and are actively occurring.²⁹⁹ An AoC approach not only places an emphasis on detection and response functions, which includes appropriate tooling ranging from Intrusion Detection and Prevention Systems (IDS/IPS) to insider threat behaviour software, but it also aims to implement a new foundational approach to security. A key

²⁹⁹ Becky Metivier, “Assume Compromise: Protect, Detect and Respond,” *Sage Data Security*, January 8, 2018, <https://www.sagedatasecurity.com/blog/assume-compromise-protect-detect-and-respond>.

component of this culture shift relies on adapting the idea that malicious actors are not just individuals or groups outside the enterprise's perimeter defenses trying to break in but are already active inside the network. These actors are always seeking access to important systems, conducting reconnaissance, escalating privileges and moving laterally across local and wide area networks. Cybersecurity then, is no longer responsive but proactive.

A 2016 EY report outlining their Cybersecurity Compromise Diagnostic service offerings, which provide technical and policy solutions as part of an AoC strategy, highlights that, "Organizations recognize that stopping sophisticated cyber attackers is unrealistic. It's no longer a matter of if or when you will be breached, it has probably already happened. The quickest way to identify and eject an intruder is to assume that they're already in your environment and to proactively assess your systems and networks for evidence of compromise."³⁰⁰ As previous chapters have noted, the threat landscape Canada's critical infrastructure community must mitigate includes APT groups that conduct prolonged attacks with TTPs that intentionally implement anti-detection tools to sustain long-term intelligence operations on their targets. These types of groups were responsible for the damaging attacks on Ukraine's power grid, Britain's NHS and Bangladesh's central bank in addition to thousands of other infrastructure compromises with less of a large-scale strategic or physical impact.³⁰¹

Although Canada's infrastructure sectors need to ensure their defenses are well implemented to deter low-cost opportunistic offensive cyber activity, organizations and regulators need to also ensure that proper human capital, financial and technical resources are

³⁰⁰ EY Threat Intelligence Services, "Cybersecurity Compromise Diagnostic: Hunting For Evidence Of Cyber Attackers," *Ernst & Young*, pg. 1-2, Accessed February 5, 2019, [https://www.ey.com/Publication/vwLUAssets/EY_-_Cybersecurity_Compromise_Diagnostic_SCORED/\\$FILE/EY-cybersecurity-compromise-diagnostic-scored.pdf](https://www.ey.com/Publication/vwLUAssets/EY_-_Cybersecurity_Compromise_Diagnostic_SCORED/$FILE/EY-cybersecurity-compromise-diagnostic-scored.pdf).

³⁰¹ Noguchi and Ueda, "An Analysis Of The Actual Status Of Recent Cyber Attacks On Critical Infrastructures."

being directed towards the APT-type actor who may be operating on behalf of a government for strategic and geopolitical objectives. For example, while Canadian banks have a range of daily cybersecurity challenges to mitigate, ranging from data privacy breaches to the hacking of online bank accounts, there must also be initiatives aiming to mitigate the low-probability high-impact risk of an actor targeting an essential service such as the LVTS.

This approach moves organizations away from a preventative or outward-centric cybersecurity strategy, as protection tools and policies do not directly address issues such as zero-day vulnerabilities or the likelihood that state-driven APTs have already or will in the future find a vector to compromise a targeted network. If organizations dedicate more budget and human talent towards detection and response functions, the potential damage that a breach can induce significantly declines.³⁰² For example, stronger detection programs may have allowed Ukraine's IT security staff to detect a malicious presence that was actively uploading malware and arbitrary code to machines connected to corporate and control networks for nearly 180 days. Even though Canadian infrastructure providers and vendors have heavily invested in improving their cybersecurity operations, chapter four's breakdown of the nation-state presence in vital networks reinforces how detection and response capabilities are likely to yield more of a return-on-investment than funding more external protection capabilities.³⁰³ Considering an AoC approach works on the premise that infiltration has already occurred, a company, regulator or vendor can spend more of their internal cybersecurity budget and technical staff hours tailoring controls to make it financially costly and timely for the adversary to locate a vulnerable asset that provides any type of strategic value. The aim of this inward focus is to change the calculus of the attacker's return on investment (ROI).

³⁰² EY Threat Intelligence Services, "Cybersecurity Compromise Diagnostic: Hunting For Evidence Of Cyber Attackers," 9-10.

³⁰³ Metivier, "Assume Compromise: Protect, Detect And Respond."

In 2015, Ashok Sankar, the Senior Director of Cyber Product Strategy and Management for Raytheon, state that, “Operating an enterprise under the assumption that your systems will never be compromised is akin to believing that because you take vitamins every day, eat right and exercise regularly, you’re not going to buy health insurance until after you’re already ill.”³⁰⁴ He elaborated on this comment by noting that industries, such as the critical infrastructure community, who are routinely targeted by advance threat actors, need to invest in the technologies, people and processes that can identify and locate indicators of compromise (IOC) as soon as possible. In doing so, organizations can seek out assistance from federal agencies—a process that would be outlined in the Canadian-tailored cybersecurity framework—and initiate their internal response plans to begin isolating and eradicating the threat and restoring systems with backups if necessary. Canadian critical infrastructure organizations need to assume that they are always being targeted by a highly capable attacker who is well funded, patient and dedicated to a long-term operation aiming to reach mission critical systems. Therefore, to mitigate this risk, it would be prudent to detect such an event as soon as possible and respond in a timely manner, which is the overall objective of an AoC strategy.

A March 2018 NSA cybersecurity bulletin offering key mitigation techniques for APT actors noted that their recommendations were primarily based, “Upon the NIST Cybersecurity Framework functions to manage cybersecurity risk and to promote a defense-in-depth security posture.”³⁰⁵ Defense-in-depth architecture is a cybersecurity concept that is closely aligned with both the NIST framework and an AoC culture, as it calls for redundant defensive measures that

³⁰⁴ Ashok Sankar, “To Effectively Protect Against Threats, Cyber Professionals Should Design Their Defenses Around An Assumption Of Compromise,” *Raytheon*, July 2015, <https://www.raytheon.com/cyber/news/feature/blog-sankar-compromise>.

³⁰⁵ Cybersecurity Requirements Center (CRC), “NSA’S Top Ten Cybersecurity Mitigation Strategies,” *National Security Agency*, March 2018, <https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-nsas-top10-cybersecurity-mitigation-strategies.pdf>.

aim to block threats in addition to finding them and eradicating their activities. Layering defensive solutions draws on a range of tools and processes, including centralized patching software, IDS/IPS, network access controls, physical access controls, firewalls, sandboxing environments for malware analysis, host antivirus software, data encryption and routine backup schedules. Using these components of a defense-in-depth strategy indirectly outlined in the NIST framework, combined with an AoC culture where employees, executives and IT security staff are constantly vigilant and searching for threats already in the network, critical infrastructure enterprises will create a significantly more robust cybersecurity posture for the country's vital services and systems.

Discussing the commercial perspective of AoC approaches, a 2018 article from Krebs On Security, noted that, "The companies run by leaders and corporate board members with advanced security maturity are investing in ways to attract and retain more cybersecurity talent, and arranging those defenders in a posture that assumes the bad guys will get in."³⁰⁶ Private industry outside of the critical infrastructure community is responding to the growing sophistication of the common hacker by ensuring incident response and detection capabilities are equally if not more capable than perimeter security measures. Not only will Canadian infrastructure owners, operators, and vendors fall behind the general cybersecurity trends by not shifting to AoC tactics, but they will also be providing attackers with a strategic advantage. Therefore, it is clear that leveraging an AoC approach combined with the technical and policy guidelines outlined in a national cybersecurity framework will ensure the country's critical systems are prepared to mitigate the increasingly capable state and non-state threat landscape.

³⁰⁶ Brian Krebs, "What The Marriott Breach Says About Security," *Krebs on Security*, December 2018, <https://krebsonsecurity.com/2018/12/what-the-marriott-breach-says-about-security/>.

Improving Cyber Threat Information-Sharing

The 2016 Public Safety Canada report titled “Security and Prosperity in the Digital Age” notes that, “Most of Canada’s critical infrastructure is owned by the private sector. Canada will need to find ways to bring together governments at all levels as well as owners and operators of critical infrastructure to truly address cyber threats to essential services.”³⁰⁷ While several chapters have outlined the private sectors prominent role in Canadian critical infrastructure, in addition to highlighting the complex cross-sector and cross-government interactions that occur on a daily basis, there still remains communication challenges between private and public stakeholders when it comes to relaying cyber incidents to the government or passing down threat data from federal bodies to operators and owners. Addressing these communication and information-sharing weaknesses is a national security concern, which was reinforced in the private-public collaboration objectives outlined in Public Safety Canada’s 2018 National Cyber Security Strategy.³⁰⁸

The Canadian government and its intelligence agencies have a unique capability to collect, analyze, and disseminate important threat information to owners, operators and vendors supporting critical infrastructure. The 2012 “Assessing Cyber Threats To Canadian Infrastructure” report published by CSIS notes that, “Critical infrastructure stakeholders in the Energy and Utilities, Finance, ICT, and Transportation sectors in Canada have been accustomed to managing the risks to their facilities at a local level. Nevertheless, it is widely acknowledged by stakeholders in these key sectors that there are weaknesses and gaps in their cyber defences

³⁰⁷ “Security And Prosperity In The Digital Age: Consulting On Canada's Approach To Cyber Security,” *Public Safety Canada*, last modified January 24, 2018, <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/2016-scerty-prsprty/index-en.aspx>.

³⁰⁸ “National Cyber Security Strategy,” *Public Safety Canada*, 31.

against current threats.”³⁰⁹ When discussing how government stakeholders can address these challenges, the report argues that, “A more holistic, finely-tuned partnership approach between the private sector and the security and intelligence community is warranted to help stakeholders—as well as local authorities—offset these vulnerabilities, mitigate any potential damage and pre-plan resilience.”³¹⁰ While this proposal was outlined in nearly seven years ago, there have been several impediments to implementing such a seamless information-sharing program. This has curbed the development of a widely used and trusted threat data exchange network where public and private infrastructure stakeholders could communicate. However, several agencies and federal Departments have launched initiatives to address this problem, with some being successful and others facing additional roadblocks.

In 2012, the “Report of the Auditor General of Canada,” which was delivered to the national Parliament, noted that, “As CCIRC is not operating around the clock, there is a risk that there will be a delay in the sharing of critical information linked to newly discovered vulnerabilities or active cyber events reported to CCIRC after operating hours. A restriction on operating hours means that CCIRC is not able to monitor the cyber threat environment 24 hours a day, as was envisioned in its mandate.”³¹¹ This was clearly a gap in the country’s cybersecurity incident response capability, in addition to being a major barrier for establishing real-time monitoring and information-sharing standards to link private stakeholders with government agencies. As of 2016, these issues had largely been addressed, with CCIRC operating 24 hours a day and seven days week, while also expanding and updating its intelligence dissemination

³⁰⁹ Gendron and Rudner, “Assessing Cyber Threats To Canadian Infrastructure,” 47.

³¹⁰ *Ibid.*

³¹¹ Office of the Auditor General of Canada, “Fall Report Of The Auditor General Of Canada 2012: Chapter 3—Protecting Canadian Critical Infrastructure Against Cyber Threats,” *OAG Reports to Parliament*, July 17, 2012, http://www.oag-bvg.gc.ca/internet/English/parl_oag_201210_03_e_37347.html.

programs.³¹² For example, by 2016 the organization had grown its Community Portal, which was a forum for private and public sector stakeholders to report incidents and gain access to CCIRC's world-class malware analysis laboratory and a range of vulnerability assessment tools. CCIRC also increased private and government participation in the Critical Infrastructure Gateway project, which is a web-based information-sharing platform that allows critical infrastructure community members to report incidents, share assessments, notify of cyber alerts all while retaining highly secured communication protocols to prevent any inappropriate disclosures to the public.³¹³

Although these advancements indicate that information-sharing programs and processes were improving for the critical infrastructure community, serious challenges still persisted. For example, nearly five years after the Auditor General report, Public Safety Canada published its 2017 "Horizontal Evaluation of Canada's Cyber Security Strategy," which noted that, "Despite improvements made, for the most part information-sharing among participating organizations was done on an ad hoc and selective basis. There was no clear policy as to what should be shared, with whom and when. It was mostly the individual organizations that decide on their own terms what to share with others."³¹⁴ This lack of coordination and oversight demonstrates that program development efforts initiated after the 2012 audit review were either not well enforced or were not implemented with the proper rigor and urgency. Since threat data and information-sharing between government and private critical infrastructure stakeholders is essential for ensuring high-risk vulnerabilities and advanced attacker TTPs are widely defended against across sectors, the findings of the 2017 Horizontal Evaluation highlight the need for ongoing policy reform.

³¹² "Fundamentals Of Cyber Security For Canada's CI Community," *Public Safety Canada*.

³¹³ *Ibid.*

³¹⁴ "Horizontal Evaluation Of Canada's Cyber Security Strategy," *Public Safety Canada*, 10.

Another impediment to improved cyber threat-information sharing are the classification restrictions that prevent certain intelligence at the government level being disseminated to private sector infrastructure owners and operators who do not maintain active government clearances. The 2017 Horizontal Evaluation document explains that, “Currently, there is no efficient mechanism for sharing classified information, particularly in real time.”³¹⁵ Not only is this an operational challenge for stopping an active malicious cyber campaign, but it also provides more evidence of a lack of remediation activities following the recommendations outlined in the 2012 federal audit. A 2018 Senate Standing Committee on Banking, Trade and Commerce report discussing cyber threats to Canadian interests also reaffirmed the classification issues that are limiting threat information-sharing between public and private entities. The report notes that, “There is a need for the government and the private sector to coordinate their efforts to rapidly respond to cyber attacks, which could involve sharing sensitive and confidential information. However, information sharing can be difficult since government information may be classified and companies can only share limited or very general information.”³¹⁶

David Swan, the director of cyber intelligence at the Centre for Strategic Cyberspace and Security Science in Alberta, reinforced this point during an interview with IT World Canada where he explained that, “Canadian companies are very conservative on what they let out about cyber attacks, and that’s a problem because if you don’t share information on who’s attacking then the bad guys get to run around the neighbourhood and keep doing it.”³¹⁷ Not only are government policy limitations creating threat information-sharing barriers, but corporate competition, IP considerations and a general lack of interest in sending sensitive company data to

³¹⁵ Ibid., 1-2.

³¹⁶ Doug Black (Senator, Hon.) and Carolyn Stewart Olsen (Senator, Hon.), “Cyber Security And Cyber Fraud,” *Report of the Standing Senate Committee on Banking, Trade and Commerce*, pg. 22, October 2018, https://sencanada.ca/content/sen/committee/421/BANC/reports/BANC_Report_FINAL_e.pdf.

³¹⁷ Solomon, “Ontario Transit Agency Extremely Confident Cyber Attack Came From North Korea.”

government networks are also curbing reform efforts. It is worth noting that in 2017, a spokeswoman with CSE announced that the agency officially maintained a software zero-day vulnerability stockpile, where certain vulnerabilities would be released to vendors and the public while others would be retained for national security purposes.³¹⁸ Considering the impact of the WannaCry virus and its roots in an NSA zero-day exploit, there is a significant precedent for ensuring that CSE and other federal agencies have the administrative procedures and technical capacity to rapidly distribute patch advice or communicate exploit TTPs that an adversary may leverage in a future infrastructure attack. However, the current state of the information-sharing apparatus indicates that this would be a challenge, which only reinforces the need to implement this policy tier as part of a new national infrastructure cybersecurity plan.

In addition to private-to-private and government-to-private threat sharing limitations, multiple reports indicate that federal agencies and Departments have internal challenges that are impacting infrastructure cybersecurity operations. An example of this government-to-government information-sharing weakness was highlighted in the 2012 federal audit, where the Office of the Auditor General explained that, “We found that CSE has not been consistently providing CCIRC with timely and complete information gained from its monitoring of government systems. We asked officials from the two agencies what kept CSE from sharing this information. CSE told us it was concerned about sharing information because of the sensitive nature of the information it collects, such as classification levels or the sensitivities of client departments.”³¹⁹ While the report notes that these intergovernmental and interagency issues were addressed the following year of the audit, the 2017 Horizontal Strategy indicates otherwise. For

³¹⁸ Matthew Braga, “When Do Canadian Spies Disclose The Software Flaws They Find? There's A Policy, But Few Details,” *CBC News*, September 6, 2017, <https://www.cbc.ca/news/technology/canada-cse-spies-zero-day-software-vulnerabilities-1.4276007>.

³¹⁹ Office of the Auditor General of Canada, “Fall Report Of The Auditor General Of Canada 2012.”

example, the 2017 document states that, “There is a lack of appropriate tools and infrastructure for sharing classified information. Currently, several classified networks across government lack interoperability. In addition, only a limited number of employees have access to these networks.”³²⁰ While classification challenges are clear barriers for implementing improved threat data distribution for regulators, operators and owners to utilize in their local or national cybersecurity programs, there have also been difficulties in assigning roles and responsibilities. This has directly impacted the event response quality of past critical infrastructure cyber incidents, where private stakeholders were unclear about who to contact in the Canadian government.

The 2017 Horizontal Strategy also discovered that, “Critical infrastructure owners and operators were particularly unclear about the roles and responsibilities of these two organizations [CCIRC and CSE].”³²¹ This lack of clarity existed despite of the policy and administrative remediation activities federal authorities undertook in the years following the 2012 audit. The report plainly adds in its recommendation section that, “Roles and responsibilities need to be clearer, particularly those of CSE and the Canadian Cyber Incident Response Centre. Specifically, there is a need to clarify which organization should serve as the first point of contact for the private sector in the event of a cyber-incident.”³²² While further remediation efforts on this issue have been launched since 2017, over a year later the 2018 cyber threat report from the Senate warned that, “There is a clear need for public/private coordination in responding to attacks against critical infrastructure and a single clear point of contact in the public sector for chief information security officers in the private sector. These improvements will help us better

³²⁰ “Horizontal Evaluation Of Canada's Cyber Security Strategy,” *Public Safety Canada*, 10.

³²¹ *Ibid.*, 8.

³²² *Ibid.*, 19.

share information in a protected fashion and will help us manage and prevent future attacks.”³²³ These ongoing roles and responsibility challenges across the critical infrastructure environment and the confusion among sector stakeholders regarding public-private and government-to-government information-sharing procedures reinforces the need to create new incentives, structures and exercises to improve communication.

While the government is launching new initiatives to improve the Critical Infrastructure Gateway project and to reduce classification barriers, CSE and CCIRC along with private sector operators and vendors should increase their interaction with the Canadian Cyber Threat Exchange (CCTX).³²⁴ This independent, not-for-profit organization has a rapidly growing membership—including critical infrastructure stakeholders and ordinary corporate entities—interested in leveraging their threat information, cyber analysis and risk mitigation services. Not only does CCTX gather threat data from its members, but it also correlates and analyzes this data to create actionable cyber threat intelligence that directly feeds into member cybersecurity programs and dashboards.³²⁵ Working with non-governmental partners, such as CCTX, is a cost-effective and quick solution for increasing the country’s threat information-sharing capacity. However, as previously noted, these types of public-private partnerships will only reach their full potential if classification, administrative and protocol communication barriers are resolved first.

Implementing the three strategy tiers recommended in this chapter would significantly increase the cyber resilience of the country’s critical infrastructure. The framework would provide a high-level guidance tool for all industrial and non-industrial sector stakeholders to build-out their cybersecurity programs in addition to providing regulators with a reliable,

³²³ Black and Olsen, “Cyber Security And Cyber Fraud,” 23.

³²⁴ “National Cross Sector Forum 2018-2020 Action Plan For Critical Infrastructure,” *Public Safety Canada*, 10.

³²⁵ “CCTX Data Exchange And Collaboration Center,” *Canadian Cyber Threat Exchange (CCTX)*, accessed on February 9, 2019, <https://cctx.ca/about-cctx/>.

consistent and thorough auditing tool. Further, by combining the technical and policy controls outlined in a national framework with the organizational culture shift to AoC, foreign and domestic threat actors—even the most sophisticated APT groups—would have a difficult time overcoming cybersecurity programs purpose-built for detection, eradication and response. Lastly, leveraging the advanced intelligence, computer engineering and cybersecurity analysis capabilities of Canada’s security community, namely the CSE, CSIS and CCIRC, to provide real-time threat feeds directly into the security architecture of critical infrastructure enterprises will ensure that Canada remains well prepared to defend the nation’s essential services from strategic attacks and incidents in cyberspace.

Areas of Future Research

Three primary areas of research that are important to add to the discussion of protecting Canada’s critical infrastructure from cyber threats relate to retaliation policy, attribution of attacks and international legal models for managing offensive cyber activities. First, it is important to recognize that the policies surrounding how Canada would retaliate to an attack and with what means that retaliation would leverage remains unclear. This is an area of research that is essential for future critical infrastructure protection as these policies can communicate consequences to adversaries that may deter their computer network exploitation and attack activities. Part of this research would need to expand the defensive orientated framework approach provided in this chapter to also include an offensively orientated framework for whether Canada would leverage digital or physical means to target an attacker and under what circumstances escalation would occur. Additionally, further outlining the relationship between civilian signals and cybersecurity agencies, such as CSE, and their offensive cyber partners

embedded across the CAF would strengthen the understanding of offensive authorities in Canada and who would be responsible for carrying out an attack.

The topic of escalation and retaliation becomes complicated when assessing the possible response options for different types of threat actors. For example, it is difficult to determine which authorities should respond to a cyber attack that caused significant physical or financial damage when the actor is an international terrorist group leveraging digital infrastructure across multiple countries. Under these circumstances, it could be politically and legally challenging for the government of Canada to conduct any activity as the targeted IT systems could belong to the hosting government or international companies who were not necessarily the perpetrator of the attack. Research is needed to clarify how these issues would be resolved and what legal requirements would need to be settled to ensure a retaliation could occur promptly against foreign and domestic threats.

An additional area of future research that should be examined includes the requirements and prospect of establishing international norms and legal models for offensive activities in cyberspace. Part of this research area needs to address attribution challenges from a technical and policy standpoint. On the technical side, it would be beneficial to create identification thresholds and burden-of-proof standards for claiming a certain actor, group, or government was responsible for an operation. For example, Canada's national security would benefit if there were predetermined guidelines for assessing when an attack or infiltration attempt could be attributed to a government when the actor directly responsible was a private group who received certain assistance from official state institutions—though the affiliation or involvement of these institutions is difficult to precisely establish. As highlighted in chapter four, many different APT groups and private threat actors have close relationships with governments but are not always

ordered, controlled or augmented by official employees, leaders or military authorities.

Understanding how to manage these types of attribution issues should be an essential component of future analysis associated with responding to and deterring cyber attacks on Canadian critical infrastructure.

Lastly, an important aspect of future research that should be undertaken relates to the challenges associated with government based computer network defense and its operational integration with the majority of Canada's privately owned and controlled critical infrastructure IT networks. Since this was not a technical issue specifically analyzed in this thesis, future discussions on critical infrastructure cybersecurity across the country should review the costs, legal challenges and resource requirements for leveraging real-time CAF and CSE attack prevention within the IT systems for the thousands of private sector stakeholders supporting essential services. This research would directly support and add new context to the third policy recommendation provided in this chapter, which relates to cyber threat information-sharing, as it would take the recommendation one step further by allowing hands-on government network intervention on privately owned systems. Additional analysis would need to occur to understand the feasibility of private industry allowing this type of remote interactive government access to important proprietary digital assets often housing or overseeing intellectual property and proprietary technology.

CONCLUSION

Failures within the provision of essential services provided by private industry or public entities can result in major safety risks and financial loss for Canadians and Canadian businesses. Historically, events or actors that were capable of inducing this type of failure were associated with physical disturbances, such as environmental disasters or equipment malfunctions and even acts of material terrorism. While these threats are still ongoing challenges for ensuring the integrity and availability of critical infrastructure, new risks in cyberspace have rapidly transformed the requirements for securing vital assets and achieving a high level of resiliency across national systems. Federal government initiatives and policy reform, particularly from organizations such as Public Safety Canada and CSE, have aimed to meet these evolving requirements but this has been paralleled by an increasingly dedicated and technically proficient threat landscape. Consequently, significant cyber risks still persist across the country's critical industrial and non-industrial infrastructures, posing an active national security challenge for the government and an operational issue for sector stakeholders.

As this thesis has outlined, the breadth and complexity of critical infrastructure sectors makes oversight and enforcement of cybersecurity policies a challenging objective. This is in addition to the highly technical issues that were identified in ICS and SCADA systems throughout the industrial environment and the unique IT security challenges facing stakeholders in the non-industrial environment, such as banks servicing the national FMI. Combining these policy and technical challenges reinforces the idea that cybersecurity for critical infrastructure must be a collaborative effort, where there is strong public-private coordination and recognition of the unique threat environment that is actively seeking to compromise key assets. This

environment includes nation-state governments with significant technical, financial and personnel resources, and their sophisticated affiliates such as Iran's APT33 or China's APT10 hacking groups. The thesis also detailed how less advanced but increasingly resourceful non-state actors are beginning to become direct threats, such as international terrorist groups who are not only trying to develop indigenous capabilities but are looking to ideologically recruit computer security experts or pay them for hacking-as-a-service. Further, as highlighted during the assessment of insider threats, the growing digital connections throughout critical infrastructure are opening up new avenues for malicious and negligent employees, contractors and business partners to conduct attacks directly or enable others to do so.

The key vulnerabilities that were identified for industrial infrastructure sectors largely stemmed from the convergence of corporate and control networks, where the linkage of control technologies with Internet-facing systems has introduced new strategic risks for Canada. Some of the country's most fundamental systems, such as electricity, water distribution and natural gas delivery, can be disrupted, disabled and even destroyed by well-crafted and executed malicious cyber operations. This was highlighted in the examples of the Ukrainian power grid attack and Stuxnet's impact on Iranian nuclear infrastructure, in addition to smaller less impactful incidents such as the North Korean hack against Metrolinx. As stakeholders in the control environment continue to integrate legacy IT systems with emerging technologies such as cloud computing, SDN and IoT devices, the attack surface will increase and advanced threat actors will have more opportunities to position themselves within networks servicing Canadians, businesses and government offices on a daily basis.

The thesis also explained the unique risks in the non-industrial environment using the FMI as a case study. While the example demonstrated the direct risks to the national economy

specifically, such as patch management issues and software vulnerabilities associated with the LVTS or SWIFT network, it also referenced more general challenges such as the rising prospect of extremely large DDoS attacks. The strategic consequences of major incidents in the non-industrial environment were highlighted in the WannaCry ransomware virus example, which analyzed the technical cybersecurity failures that crippled key British healthcare organizations and their operations for several days in 2017—including some medical emergency providers. Subsequent chapters discussed how legacy IT systems in these non-industrial environments are now integrating with emerging technologies such as 5G networks to create new national security policy issues for Canadian infrastructure stakeholders, such foreign adversaries leveraging their position in the hardware and software supply chain to maliciously alter components of important IT assets before deployment in Canadian networks.

To address the increasingly complicated threat landscape targeting critical infrastructure and the rapidly growing number of vulnerabilities across legacy and emerging IT systems in industrial and non-industrial sectors, this thesis constructed and recommended a three-tiered national infrastructure cybersecurity strategy. This approach suggests that federal authorities leverage a tailored NIST assessment framework unique to the Canadian legal, regulatory, political and threat landscape; incentivize and implement an AoC culture among all sector stakeholders to improve detection and response capabilities as opposed to focusing on external protection priorities; and lastly, increase cyber threat-information sharing to promote peer-to-peer and government-to-industry threat intelligence and data exchanges. This strategy drew support and evidence from the recommendations and findings of publications outlined in Canadian sources such as Public Safety Canada, CSIS, CSE, and from U.S. sources such as the DHS, FBI, NIST and the NSA.

As Ottawa and its foreign partners continue to commit more resources to leverage cyberspace as a tool for geopolitical competition, Canada's competitors and adversaries—state and non-state alike—will continue to do the same. These trends indicate that the strategic and commercial importance of the cyber domain is rising just as new technologies and associated vulnerabilities are being introduced into the nation's critical infrastructure. Ensuring that private industry and public infrastructure stakeholders can defend against a range of threat actors 365 days a year and 24 hours a day will continue to grow as a key requirement for supporting the country's national security. If this challenge cannot be adequately addressed with the assistance of technical and policy-based cybersecurity reform, Canada will face a systemic security risk that may hinder the economic and safety interests of the country moving into the future.

BIBLIOGRAPHY

- Abrams, Marshall, Keith Stouffer, Victoria Pillitteri, Suzanne Lightman, and Adam Hahn. "Guide To Industrial Control Systems (ICS) Security: NIST Special Publication 800-82." *National Institute of Standards and Technology*. 2015. <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf>.
- American Water Works Association (AWWA). "Process Control System Security Guidance For The Water Sector." *AWWA and Water Industry Technical Action Fund (WITAF)*. October 2014. <http://www.nawc.org/uploads/documents-and-publications/documents/AWWACybersecurityguide.pdf>.
- Arjani, Neville, and Darcey McVanel. "A Primer On Canada's Large Value Transfer System." *Bank of Canada*. March 1, 2006. https://www.bankofcanada.ca/wp-content/uploads/2010/05/lvts_neville.pdf.
- Association of Power Producers of Ontario. "Ontario's Cyber Security Framework Is Now In Force." June 2018. <https://magazine.appro.org/news/ontario-news/5545-1529540280-ontario's-cyber-security-framework-is-now-in-force.html>.
- Baker, Cindy. "Trusted Insiders Are Now The Most Serious Security Threat," *IT World Canada*. February 1, 2018. <https://www.itworldcanada.com/article/trusted-insiders-are-now-the-most-serious-security-threat/401284>.
- Banisar, David and Patricia Melendez. "Tightening The Net Part 2: The Soft War And Cyber Tactics In Iran." *The Article 19 Center: Civic Space Unit*. March 2017. https://www.article19.org/data/files/medialibrary/38619/Iran_report_part_2-FINAL.pdf.
- Banking and Capital Markets Division. "Supporting The Entire Payments Value Chain." *CGI Group Inc*. Last modified January 2019. <https://www.cgi.com/en/banking-capital-markets/cross-banking-capabilities/payments>.
- Bank of Canada. "Regulatory Oversight Of Designated Clearing And Settlement Systems." *BoC Press and Market Notices*. Last modified April 2017. <https://www.bankofcanada.ca/2017/04/release-2016-bank-canada-fmi-oversight-activities-annual-report/>.
- Beeby, Dean. "State-Sponsored Cyberattacks On Canada Successful About Once A Week." *BBC News*. October 30, 2017. <https://www.cbc.ca/news/politics/cyber-attacks-canada-cse-1.4378711>.
- Berr, Jonathan. "WannaCry Ransomware Attack Losses Could Reach \$4 Billion." *CBC News*. May 16, 2017. <https://www.cbcnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/>.

- Beyond Security. "Understanding And Defending Against SQL Injection Attacks." Last modified January 2019. <https://www.beyondsecurity.com/about-sql-injection.html>.
- Bisson, David. "ICS Security: What It Is And Why It's A Challenge For Organizations." *Tripwire Cyber Security Solutions*. August 20, 2018. <https://www.tripwire.com/state-of-security/ics-security/ics-security-challenge-organizations/>.
- Black, Doug (The Honourable Senator) and The Honourable Senator Carolyn Stewart Olsen. "Cyber Security And Cyber Fraud." *Report of the Standing Senate Committee on Banking, Trade and Commerce*. October 2018. https://sencanada.ca/content/sen/committee/421/BANC/reports/BANC_Report_FINAL_e.pdf.
- Boutilier, Alex. "A Canadian Snowden? CSE Warns Of 'Insider Threats.'" *The Star*. July 26, 2015. <https://www.thestar.com/news/canada/2015/07/26/a-canadian-snowden-cse-warns-of-insider-threats.html>.
- Braga, Matthew. "When Do Canadian Spies Disclose The Software Flaws They Find? There's A Policy, But Few Details." *CBC News*. September 6, 2017. <https://www.cbc.ca/news/technology/canada-cse-spies-zero-day-software-vulnerabilities-1.4276007>.
- Brewster, Thomas. "Meet APT33: A Gnarly Iranian Hacker Crew Threatening Destruction." *Forbes*. September 20, 2017. <https://www.forbes.com/sites/thomasbrewster/2017/09/20/iran-hacker-crew-apt33-heading-for-destructive-cyberattacks/#5b5693174a48>.
- Bright, Peter. "\$1B Bangladesh Heist: Officials Say SWIFT Technicians Left Bank Vulnerable." *ARS Technica*. May 10, 2016. <https://arstechnica.com/information-technology/2016/05/1b-bangladesh-heist-officials-say-swift-technicians-left-bank-vulnerable/>.
- Buckley, Sean. "2018 Preview: Network Automation Will Take Hold In Operator Networks." *Fierce Telecom*. December 29, 2017. <https://www.fiercetelecom.com/telecom/2018-preview-network-automation-takes-hold-operator-networks>.
- Burns, Calvin, Kevin Quigley and Gwendolyn Moncrieff-Gould. "Strengthening The Resilience Of The Canadian Water Sector." *Critical Infrastructure Protection Initiative at Dalhousie University*. December 15, 2017. https://www.cwwa.ca/pdf_files/Water_sector_vulnerability_REPORT.pdf.
- Cameron, Dell. "FBI Put Anonymous Hacker Jeremy Hammond On A Terrorist Watch List." *The Daily Dot*. February 24, 2017. <https://www.dailydot.com/layer8/jeremy-hammond-terrorist-watchlist-fbi/>.

- Canadian Armed Forces. "Operation UNIFIER." *Department of National Defense: Operations and Exercises*. Last modified December 3, 2018. <https://www.canada.ca/en/department-national-defence/services/operations/military-operations/current-operations/operation-unifier.html>.
- Canadian Center for Cyber Security. "National Cyber Threat Assessment 2018." *Communications Security Establishment (CSE)*. December 6, 2018. <https://cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2018>.
- Canadian Cyber Threat Exchange (CCTX). "CCTX Data Exchange And Collaboration Center." Accessed on February 9, 2019. <https://cctx.ca/about-cctx/>.
- Canadian Payments Association. "LVTS Rule 12: Emergency Conditions." *Payments Canada*. April 24, 2017. https://www.payments.ca/sites/default/files/lvts_rule_12_eng.pdf.
- Canadian Payments Association. "LVTS Rules Overview." *Payments Canada*. August 21, 2017. https://www.payments.ca/sites/default/files/21-Aug-17/lvts_overview_eng.pdf.
- Canadian Nuclear Safety Commission "Regulatory Oversight Report For Canadian Nuclear Power Generating Sites: 2017." *Ministry of Natural Resources*. November 8, 2018. <http://www.nuclearsafety.gc.ca/eng/the-commission/meetings/cmd/pdf/CMD18/CMD18-M39.pdf>.
- Capitella, Donato. "Defending SWIFT Payment Systems From Attack." *MWR Security*. May 5, 2017. <https://www.mwrinfosecurity.com/our-thinking/defending-swift-payment-systems-from-attack/>.
- CBC News. "Virus Affecting IT System At Health Sciences North Impacting Health Care Across The Region." *CBC*. January 17, 2019. <https://www.cbc.ca/news/canada/sudbury/hsn-it-virus-update-1.4982267>.
- Center for Internet Security. "Insider Threats: In The Healthcare Sector." Accessed January 27. <https://www.cisecurity.org/blog/insider-threats-in-the-healthcare-sector/>.
- CGI Group Inc. "CGI HotScan Watch List Filtering." February 2016. https://www.cginederland.nl/sites/default/files/files_nl/brochures/cgi-nl_brochure_hotscan-watch-list-filtering_2017-04-11.pdf.
- CloudFlare. "What Is A DDoS Attack?" *CloudFlare: Learning Solutions*. Accessed January 7, 2019. <https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/>.
- Coats, Daniel R. "2018 Worldwide Threat Assessment Of The U.S. Intelligence Community." *Office of the Director of National Intelligence*. February 13, 2018. <https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf>.

- Coats, Daniel R. "2019 Worldwide Threat Assessment Of The U.S. Intelligence Community." *Office of the Director of National Intelligence*. January 29, 2019. <https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf>.
- Connell, Michael. "Deterring Iran's Use Of Offensive Cyber: A Case Study." *CNA Analysis and Solutions and Defense Technical Information Center (DTIC)*. October 2014. <https://apps.dtic.mil/dtic/tr/fulltext/u2/a617308.pdf>.
- Constantin, Lucian. "DDoS Attacks Against U.S. Banks Peaked At 60 Gbps." *CIO Insider*. December 13, 2012. <https://www.cio.com/article/2389721/security0/ddos-attacks-against-us-banks-peaked-at-60-gbps.html>.
- Constantin, Lucian. "First Stuxnet Victims Were Five Iranian Industrial Automation Companies." *PC World*. November 12, 2014. <https://www.pcworld.com/article/2846852/first-stuxnet-victims-were-five-iranian-industrial-automation-companies.html>.
- Consulting Canada News Desk. "CGI Announces Blockchain And Cybercrime Solutions For Banks." *Consulting Canada*. November 22, 2018. <https://www.consulting.ca/news/683/cgi-announces-blockchain-and-cybercrime-solutions-for-banks>.
- Cosoleto, Tara. "Australia Joins Global Condemnation Of Serious China Cyber Hacking." *SBS News*. December 21, 2018. <https://www.sbs.com.au/news/australia-joins-global-condemnation-of-serious-china-cyber-hacking>.
- Cybersecurity and Infrastructure Security Agency. "Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy And Other Critical Infrastructure Sectors." *Department of Homeland Security*. March 15, 2018. <https://www.us-cert.gov/ncas/alerts/TA18-074A>.
- Cybersecurity and Infrastructure Security Agency. "Overview Of Cyber Vulnerabilities." *Department of Homeland Security*. Accessed January 12, 2019. <https://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities#poor>.
- Cybersecurity Newswire Desk. "New Report Reveals How Accidental Insider Threats Put Organizations At Real Risk." *Security Magazine*. November 29, 2017. <https://www.securitymagazine.com/articles/88542-new-report-reveals-how-accidental-insider-threats-put-organizations-at-real-risk>.
- Cybersecurity Requirements Center (CRC). "NSA'S Top Ten Cybersecurity Mitigation Strategies." *National Security Agency*. March 2018. <https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-nsas-top10-cybersecurity-mitigation-strategies.pdf>.

- Defense Research and Development Canada. "National Critical Infrastructure Interdependency Model: Way Ahead." April 26, 2016. http://cradpdf.drdc-rddc.gc.ca/PDFS/unc225/p803698_A1b.pdf.
- Delui, Anon. "Man In The Middle Attacks Explained Through ARP Cache Poisoning." *Cybrary*. October 1, 2015. <https://www.cybrary.it/0p3n/man-in-the-middle-attack-explained/>.
- Denning, Dorothy. "Following The Developing Iranian Cyberthreat." *Scientific American*. December 12, 2017. <https://www.scientificamerican.com/article/following-the-developing-iranian-cyberthreat/>.
- Department of National Defense. "DND/CAF Welcomes First Cyber Operators." *The Maple Leaf: Defense News*. Last modified January 8, 2018. <https://ml-fd.caf-fac.ca/en/2018/01/9092>.
- Department of National Defense. "Operating Context And Key Risks." *DND Departmental Plans: Reports and Publications*. April 16, 2018. <https://www.canada.ca/en/department-national-defence/corporate/reports-publications/plans-priorities/2018-19/supplementary-information/operating-context-and-key-risks.html>.
- Dinis, Filipe. "Strengthening Our Cyber Defences." *Payments Canada*. May 9, 2018. <https://www.bankofcanada.ca/2018/05/strengthening-cyber-defences/>.
- Dorfman, Avi. "Four Cyber Security Threats On NFV Networks." *Telco Systems*. August 10, 2016. <http://www.telco.com/blog/four-cyber-security-threats-on-nfv-networks/>.
- Dostri, Omer. " Hamas' Cyber Activity Against Israel." *The Jerusalem Institute for Strategy and Security*. October 15, 2018. <https://jiss.org.il/en/dostri-hamas-cyber-activity-against-israel/>.
- Eigner, Oliver, Philipp Kreimel and Paul Tavorato. "Detection Of Man-In-The-Middle Attacks On Industrial Control Systems." *St. Polten University of Applied Sciences: Information and Security Department*. May 11, 2016. https://itsecx.fhstp.ac.at/wp-content/uploads/2016/11/04_PaulTavorato_ITSecX16.pdf.
- Eisenhart, Stewart. "Health Canada Setting Pre-Market Medical Device Cybersecurity Requirements." *Emergo*. <https://www.emergobyul.com/blog/2018/12/health-canada-setting-pre-market-medical-device-cybersecurity-requirements>.
- EY Threat Intelligence Services. "Cybersecurity Compromise Diagnostic: Hunting For Evidence Of Cyber Attackers." *Ernst & Young*. Accessed February 5, 2019. [https://www.ey.com/Publication/vwLUAssets/EY_-_Cybersecurity_Compromise_Diagnostic_SCORED/\\$FILE/EY-cybersecurity-compromise-diagnostic-scored.pdf](https://www.ey.com/Publication/vwLUAssets/EY_-_Cybersecurity_Compromise_Diagnostic_SCORED/$FILE/EY-cybersecurity-compromise-diagnostic-scored.pdf).

- Farivar, Cyrus. "Man Who Allegedly Gave Vault 7 Cache To Wikileaks Busted By Poor Opsec." *ARS Technica*. June 19, 2018. <https://arstechnica.com/tech-policy/2018/06/ex-cia-engineer-indicted-on-several-new-charges-connected-to-vault-7-leak/>.
- Fazio, Antonino, and Fabio Zuffranieri. "Interbank Payment System Architecture From A Cyber Security Perspective." *Bank of Italy: Questions of Economics and Finance Occasional Papers Series* no. 418 (2018): 1-19.
- Financial Sector Assessment Team. "Oversight And Supervision Of Financial Market Infrastructures, And Selected Issues In The Payment System." *International Monetary Fund (IMF) Country Report* 15 no. 254 (2015): 1-27.
- Fingas, Jon. "Stuxnet Worm Entered Iran's Nuclear Facilities Through Hacked Suppliers." *Engadget*. November 13, 2014. <https://www.engadget.com/2014/11/13/stuxnet-worm-targeted-companies-first/>.
- Freeze, Colin. "Ottawa's 2016 Memo On Cyber Threats Points Finger At Russia, China." *The Globe and Mail*. May 4, 2018. <https://www.theglobeandmail.com/canada/article-ottawas-2016-memo-on-cyberthreats-points-finger-at-russia-china/>.
- Fruhlinger, Josh. "What Is WannaCry Ransomware, How Does It Infect, And Who Was Responsible?" *CSO Online*. August 30, 2018. <https://www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html>.
- Gaffey, Conor. "Cyberattack On Nuclear Facilities Could Cause Radiation Leak: Report." *Newsweek*. October 5, 2015. <https://www.newsweek.com/nuclear-power-stations-cyberattacknuclear-power-plants-cyberattacknuclear-599233>.
- Gallagher, Harold, Wade McMahon and Ron Morrow. "Cyber Security: Protecting The Resilience Of Canada's Financial System." *Bank of Canada* 7 no. 14 (2014): 47-53.
- Garber, Roman. "What Makes IoT Security So Tough?" *DZone*. June 11, 2018. <https://dzone.com/articles/what-makes-iot-security-so-tough>.
- Gendron, Angela and Martin Rudner. "Assessing Cyber Threats To Canadian Infrastructure." *Canadian Security Intelligence Service*. March 2012. https://www.canada.ca/content/dam/csisscrs/documents/publications/CyberTrheats_AO_Booklet_ENG.pdf.
- Genik, Lynne. "Operations Research Support For Critical Infrastructure Resilience In The Province Of British Columbia." *Defense Research and Development Canada: Center for Security Science*. October 16, 2012. <https://apps.dtic.mil/dtic/tr/fulltext/u2/a568449.pdf>.

- Ginter, Andrew. "The Top 20 Cyber Attacks Against Industrial Control Systems." *Waterfall Security Solutions*. December 2017. https://ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/QNL_DEC_17/Waterfall_top-20-attacks-article-d2%20-%20Article_S508NC.pdf.
- Global Affairs Canada. "Co-Chairs' Summary Of The Vancouver Foreign Ministers' Meeting On Security And Stability On The Korean Peninsula." January 16, 2018. https://www.canada.ca/en/global-affairs/news/2018/01/co-chair_s_summaryofthevancouverforeignministersmeetingonsecurit.html?_ga=2.150039222.1285958903.1516771858-817845510.1516771858.
- Goodin, Dan. "Stuxnet-Style Code Signing Is More Widespread Than Anyone Thought." *ARS Technica*. November 3, 2017. <https://arstechnica.com/information-technology/2017/11/evasive-code-signed-malware-flourished-before-stuxnet-and-still-does/>.
- Government of the United States and Government of Canada. "Joint United States-Canada Electric Grid Security And Resilience Strategy." *Government of Canada: Public Joint-release Statements*. December 2016. https://www.nrcan.gc.ca/sites/www.nrcan.gc.ca/files/energy/pdf/JOINT%20GRID%20SECURITY%20AND%20RESILIENCE-Strategy_en.pdf.
- Grim, Ryan. "Why I Knocked Boston Children's Hospital Off The Internet: A Statement From Martin Gottesfeld." *Huffington Post*. September 18, 2016. https://www.huffingtonpost.com/entry/why-i-knocked-boston-childrens-hospital-off-the-internet-a-statement-from-martin-gottesfeld_us_57df4995e4b08cb140966cd3.
- Grossman, Nadav. "EternalBlue – Everything There Is To Know." *Check Point Research*. September 19, 2017. <https://research.checkpoint.com/eternalblue-everything-know/>.
- Gunderman, Dan. "Incident Of The Week: DDoS Attack Hits 3 Banks Simultaneously." *Cyber Security Hub*. February 2, 2018. <https://www.cshub.com/attacks/news/incident-of-the-week-ddos-attack-hits-3-banks>.
- Gundert, Levi, Sanil Chohan, and Greg Lesnewich. "Iran's Hacker Hierarchy Exposed." *Recorded Future*. Accessed on November 25, 2018. <https://go.recordedfuture.com/hubfs/reports/cta-2018-0509.pdf>.
- Hajdarbegovic, Nermin. "Are We Creating An Insecure Internet of Things (IoT)?" Security Challenges and Concerns." *Top Tal*. February 2016. <https://www.toptal.com/it/are-we-creating-an-insecure-internet-of-things>.
- Hales, John. "Comparing SDN, NFV And Cloud Computing." *Global Knowledge*. August 14, 2014. <https://www.globalknowledge.com/blog/2014/08/14/comparing-sdn-nfv-and-cloud-computing/>.

- Health Canada. "Draft Guidance Document." *Health Canada: Public Consultation Review*. December 2, 2018. <https://www.canada.ca/en/health-canada/services/drugs-health-products/public-involvement-consultations/medical-devices/consultation-premarket-cybersecurity-profile/draft-guidance-premarket-cybersecurity.html#a2.2.5.1>.
- Hildenbrand, Jerry. "What is 5G Technology?" *Android Central*. Last modified February 9, 2019. <https://www.androidcentral.com/what-5g>.
- Holloway, Michael. "Stuxnet Worm Attack On Iranian Nuclear Facilities." *Stanford University*. July 26, 2015. <http://large.stanford.edu/courses/2015/ph241/holloway1/>.
- Horwitz, Jeremy. "U.S. Lobbies Germany, Italy, And Japan To Ban Huawei 5G Equipment." *Venture Beat*. November 23, 2018. <https://venturebeat.com/2018/11/23/u-s-lobbies-germany-italy-and-japan-to-ban-huawei-5g-equipment/>.
- Hughes, Owen. "WannaCry Impact On NHS Considerably Larger Than Previously Suggested." *Digital Health: News, Networks and Intelligence*. October 21, 2017. https://www.chicagomanualofstyle.org/tools_citationguide/citation-guide-1.html.
- Humphreys, Adrian. "Toronto-Born Canadian Is Mystery Man Behind ISIL's High-Profile Cyber Attacks." *The National Post*. November 7, 2018. <https://nationalpost.com/news/canada/toronto-born-canadian-is-mystery-man-behind-isils-high-profile-cyber-attacks>.
- Independent Electricity System Operator (IESO). "Ontario's Electricity System: Generation And Transmission System Maps." *IESO Organization*. Last modified December 3, 2018. <http://www.ieso.ca/localContent/ontarioenergymap/index.html>.
- Independent Electricity System Operator (IESO). "Standing Committee Cyber Security Forum." *IESO Organization*. Last modified January 2019. <http://www.ieso.ca/en/Sector-Participants/Engagement-Initiatives/Standing-Committees/Cyber-Security-Forum>.
- Industrial Control Systems Cyber Emergency Response Team. "Recommended Practice: Improving Industrial Control System Cybersecurity With Defense-in-Depth Strategies." *Department of Homeland Security*. September 2016. https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICSCERT_Defense_in_Depth_2016_S508C.pdf.
- Investment Industry Regulatory Organization of Canada (IIROC). "Cybersecurity Best Practices Guide For IIROC Dealer Members." December 15, 2015. http://www.iiroc.ca/industry/Documents/CybersecurityBestPracticesGuide_en.pdf.
- Jeremy, Yonah. "Exclusive: Islamic Cyber Terrorists Trying To Target Infrastructure." *The Jerusalem Post*. July 9, 2018. <https://www.jpost.com/Arab-Israeli-Conflict/Exclusive-Islamic-cyber-terrorists-trying-to-target-infrastructure-562052>.

- Kagan, Frederick W. and Tommy Stiansen. "The Growing Cyber Threat From Iran." *American Enterprise Institute: Critical Threats Project*. April 2015.
https://www.criticalthreats.org/wp-content/uploads/2016/07/imce-imagesGrowing_Cyberthreat_From_Iran_AEI_Norse_Kagan_Stiansen-1.pdf.
- Khosravi, Bijan. "Autonomous Cars Won't Work - Until We Have 5G." *Forbes*. March 26, 2018.
<https://www.forbes.com/sites/bijankhosravi/2018/03/25/autonomous-cars-wont-work-until-we-have-5g/#7f0ab85b437e>.
- Kimble, Josiah, Jacqueline O'Leary and Kelli Vanderlee. "Insights Into Iranian Cyber Espionage: APT33 Targets Aerospace And Energy Sectors And Has Ties To Destructive Malware." *FireEye: Threat Research Team*. September 20, 2017.
<https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html>.
- Krebs, Brian. "What The Marriott Breach Says About Security." *Krebs on Security*. December 2018. <https://krebsonsecurity.com/2018/12/what-the-marriott-breach-says-about-security/>.
- Kuipers, David, and Mark Fabro. "Control Systems Cyber Security: Defense In Depth Strategies." *Idaho National Laboratories and Department of Homeland Security*. May 2006. <https://inldigitallibrary.inl.gov/sites/sti/sti/3375141.pdf>.
- Kushner, David. "The Real Story Of Stuxnet." *IEEE Spectrum*. February 26, 2013.
<https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>.
- Larson, Dave. "SDN And NVF: Blessing Or A Curse For DDoS Security?" *Corero: Network Security Trends*. September 20, 2016. <https://www.corero.com/blog/761-sdn-and-nvf-blessing-or-a-curse-for-ddos-security.html>.
- Lauder, Jo. "Stuxnet: The Real Life Sci-Fi Story Of The World's First Digital Weapon." *ABC Net*. October 12, 2016. <https://www.abc.net.au/triplej/programs/hack/the-worlds-first-digital-weapon-stuxnet/7926298>.
- Leali, Nicholas. "Lessons From An Insider Attack On SCADA Systems." *Cisco*. August 20, 2009. https://blogs.cisco.com/security/lessons_from_an_insider_attack_on_scada_systems.
- Lee, Robert M., Michael J. Assante and Tim Conway. "Analysis Of The Cyber Attack On The Ukrainian Power Grid: Defense Use Case." *Electricity Information Sharing and Analysis Center*. March 18, 2016. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.
- Lewis, Michael. "TD Bank Hit By Cyber Attack." *The Star*. March 21, 2013.
https://www.thestar.com/business/2013/03/21/td_bank_hit_by_cyber_attack.html.
- Littlefield, Ryan. "Cyber Terrorism: Understanding And Preventing Acts Of Terror Within Our Cyber Space." *Medium*. June 7, 2017. <https://littlefield.co/cyber-terrorism-understanding-and-preventing-acts-of-terror-within-our-cyber-space-26ae6d53cfbb>.

- Lohrman, Dan. "Understanding New Hactivism: Where Next For Hackers With A Cause?" *Government Technology*. July 31, 2016. <http://www.govtech.com/blogs/lohrmann-on-cybersecurity/understanding-new-hactivism-where-next-for-hackers-with-a-cause.html>.
- Luber, Steven. "Information War Or Cyber War? Exploring The Russo-Ukrainian Digital Conflict." *Leksika*. December 27, 2016. <http://www.leksika.org/tacticalanalysis/2016/12/27/information-war-or-cyber-war-exploring-the-russo-ukrainian-digital-conflict>.
- Lunn, Susan. "Ralph Goodale Says Ukraine Cyberattack Caused International Anxiety." *CBC News*. March 8, 2016. <https://www.cbc.ca/news/politics/cybersecurity-ukraine-goodale-federal-review-1.3481433>.
- Makuch, Ben. "Ottawa Confirms Iranian Hackers Targeted Canadian Systems." *Vice News*. March 23, 2018. https://news.vice.com/en_ca/article/paxpy7/ottawas-cyberspies-confirm-iranian-hackers-targeted-canadian-systems.
- Makuch, Ben and Justin Ling. "Iranian Hackers Infiltrated A Canadian Government System." *Vice News*. July 9, 2015. https://news.vice.com/en_us/article/pa4dxm/iranian-hackers-infiltrated-a-canadian-government-system.
- McDonald, Natalie H. "Are Our Nation's Oil And Gas Pipelines Safe From Cyber-Attack?" *ComptIA*. October 24, 2018. <https://www.comptia.org/about-us/newsroom/blog/comptia-blog/2018/10/24/are-our-nation-s-oil-and-gas-pipelines-safe-from-cyber-attack>.
- McGuirk, Rod. "Spy Chief Wanted Ban On China Telecoms From Australian 5G." *AP News*. October 30, 2018. <https://www.apnews.com/91700da1a9ce43fda41def9d2a3a996d>.
- McKay, Dimitri. "A Deep Dive Into Hyperjacking." *Security Weekly*. February 3, 2011. <https://www.securityweek.com/deep-dive-hyperjacking>.
- Metivier, Becky. "Assume Compromise: Protect, Detect and Respond." *Sage Data Security*. January 8, 2018. <https://www.sagedatasecurity.com/blog/assume-compromise-protect-detect-and-respond>.
- MITRE Corporation. "CVE-2012-2624." *Common Vulnerabilities and Exposure Database*. May 11, 2012. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2012-2624>.
- Mueller, Paul and Babak Yadegari. "The Stuxnet Worm." *University of Arizona: Department of Information Sciences*. 2012. <https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/topic9-final/report.pdf>.
- National Audit Office (NAO). "Investigation: WannaCry Cyber Attack And The NHS." October 27, 2017. <https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/>.

- National Committee on PKI. "Preliminary PKI Study On Requirements And Comparable Initiatives In Other Countries." Government of Iceland. May 2001. https://www.government.is/media/fjarmalaraduneyti-media/media/Utgefin_rit/KPMG-report.pdf.
- National Institute of Standards and Technology. "Framework For Improving Critical Infrastructure Cybersecurity." April 16, 2018, <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.
- National Protection and Programs Directorate. "DHS And Private Sector Partners Establish Information And Communications Technology Supply Chain Risk Management Task Force." *Department of Homeland Security*. October 30, 2018. <https://www.dhs.gov/news/2018/10/30/dhs-and-private-sector-partners-establish-information-and-communications-technology>.
- National Protection and Programs Directorate. "DHS Announces ICT Supply Chain Risk Management Task Force Members." *Department of Homeland Security*. November 15, 2018. <https://www.dhs.gov/news/2018/11/15/dhs-announces-ict-supply-chain-risk-management-task-force-members>.
- National Security Telecommunications Advisory Committee. "NSTAC Report To The President On Emerging Technologies Strategic Vision." *Department of Homeland Security*. July 14, 2017. <https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Emerging%20Technologies%20Strategic%20Vision.pdf>.
- Neitzel, Lee and Bob Huba, "Top Ten Differences Between ICS And IT Cybersecurity." *The International Society of Automation*. June 2014. <https://www.isa.org/standards-and-publications/isa-publications/intech-magazine/2014/may-jun/features/cover-story-top-ten-differences-between-ics-and-it-cybersecurity/>.
- NexiiLabs. "When Hackers Target Your Hypervisor." April 16, 2017. <http://nexiilabs.com/blog/when-hackers-target-your-hypervisor/>.
- Noguchi, Mutsuo and Hirofumi Ueda. "An Analysis Of The Actual Status Of Recent Cyberattacks On Critical Infrastructures." *NEC Corporation*. Accessed on February 1, 2019. <https://www.nec.com/en/global/techrep/journal/g17/n02/170204.html>.
- Novkovic, Goran. "Cloud Computing For Utilities In Canada – Present And Future." *LinkedIn Publications*. August 22, 2018. <https://www.linkedin.com/pulse/cloud-computing-utilities-canada-present-future-peng-pmp>.
- NPCC, Inc. "Northeast Power Coordinating Council: About." Last modified July 5, 2017. <https://www.npcc.org/About/default.aspx>.

- Office of Cyber and Infrastructure Analysis. “DHS Guide: Risks To Critical Infrastructure Using Cloud Services.” *Department of Homeland Security*. March 2017. <https://info.publicintelligence.net/DHS-OCIA-InfrastructureCloudRisks.pdf>.
- Office of Intelligence and Analysis. “Insider Threat To Utilities.” *Department of Homeland Security*. July 19, 2011. <https://info.publicintelligence.net/DHS-InsiderThreat.pdf>.
- Office of the Auditor General of Canada. “Fall Report Of The Auditor General Of Canada 2012: Chapter 3—Protecting Canadian Critical Infrastructure Against Cyber Threats.” *OAG Reports to Parliament*. July 17, 2012. http://www.oag-bvg.gc.ca/internet/English/parl_oag_201210_03_e_37347.html.
- Olson, Parmy. “Inside Lulzsec: How The Superstar Hackers Met Wikileaks.” *Gawker*. May 30, 2012. <https://gawker.com/5914045/inside-lulzsec-how-the-superstar-hackers-met-wikileaks>.
- Ontario Emergency Management (OEM). “Critical Infrastructure: Provincial Programs.” *Ontario Ministry of the Solicitor General*. Last modified April 19, 2017. <https://www.emergencymanagementontario.ca/english/emcommunity/ProvincialPrograms/ci/ci.html>.
- Ontario Energy Board. “Ontario Cyber Security Framework v. 1.0.” December 6, 2017. <https://www.oeb.ca/sites/default/files/Ontario-Cyber-Security-Framework-20171206.pdf>.
- Ontario Energy Board. “Ontario’s Energy Sector: Mission And Mandate.” Accessed on December 23, 2018. <https://www.oeb.ca/about-us/mission-and-mandate/ontarios-energy-sector>.
- Oppenheim, Nicole, Ali Islam and Winny Thomas. “SMB Exploited: WannaCry Use Of EternalBlue.” *FireEye*. May 26, 2017. <https://www.fireeye.com/blog/threat-research/2017/05/smb-exploited-wannacry-use-of-eternalblue.html>.
- Owens, Kevin, David E. Whitehead, Dennis Gammel, and Jess Smith. “Ukraine Cyber-Induced Power Outage: Analysis And Practical Mitigation Strategies.” *Schweitzer Engineering Laboratories, Inc*. Paper presented at the Power and Energy Automation Conference, Spokane, Washington, March 21, 2017. https://www.eiseverywhere.com/file_uploads/aed4bc20e84d2839b83c18bcba7e2876_Owens1.pdf.
- Park, Donghui, Julia Summers and Michael Walstrom. “Cyberattack On Critical Infrastructure: Russia And The Ukrainian Power Grid Attacks.” *University of Washington: Henry M. Jackson School of International Relations*. October 11, 2017. <https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/>.

- Payments Canada. “Essential Payments Infrastructure: All Our Systems.” Last modified November 2017. <https://www.payments.ca/about-us/what-we-do>.
- Payments Canada. “High-Value System (LVTS) Participants.” Accessed on January 15, 2019. <https://www.payments.ca/our-directories/high-value-system-lvts-participants>.
- Payments Canada. “Payments Canada Initiates Procurement Of Canada’s New Core Clearing And Settlement System—Lynx.” April 26, 2017. <https://www.payments.ca/about-us/news/payments-canada-initiates-procurement-canada’s-new-core-clearing-and-settlement-system>.
- Payments Canada. “Retail System: Rules, Standards And Statistics.” Accessed December 17, 2018. <https://www.payments.ca/about-us/our-systems-and-rules/retail-system>.
- Pazvant, Anil. “Buffer Overflow Vulnerability On Logica HotScan SWIFT Alliance Access Interface.” *SecLists: Vendor Patches*. October 9, 2012. <https://seclists.org/bugtraq/2012/Oct/50>.
- Porteous, Holly. “The Stuxnet Worm: Just Another Computer Attack Or A Game Changer?” *Library of Parliament: Parliamentary Information and Research Service*. October 7, 2010. http://publications.gc.ca/collections/collection_2010/bdp-lop/eb/2010-81-eng.pdf.
- Powers, Ed, Sean Peasley, Rene Waslo, Byron Fletcher and David Dinh. “Examining the Industrial Control System Cyber Risk Gap.” *Deloitte LLP*. 2015. <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-ics-white-paper.pdf>.
- Press, Jordan. “Anonymous A Threat To Critical Infrastructure? Expert Says No.” *News National*. December 20, 2012. <https://o.canada.com/news/anonymous-a-threat-to-critical-infrastructure-expert-says-no>.
- Public Safety Canada. “Building Resilience Against Terrorism: Canada's Counter-Terrorism Strategy.” January 31, 2018. <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/rsln-c-gnst-trrrsm/index-en.aspx>.
- Public Safety Canada. “Cyber Review Consultations Report.” January 17, 2017. <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/2017-cybr-rvw-cnslttns-rprt/index-en.aspx>.
- Public Safety Canada. “Cyber Security: Publications and Reports.” Last modified November 19, 2018. <https://www.publicsafety.gc.ca/cnt/ntnl-scrct/cbr-scrct/index-en.aspx>.
- Public Safety Canada. “Forging A Common Understanding For Critical Infrastructure.” March 19, 2014. <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/2016-frngng-cmmn-ndrstndng-crtcalnfrstrctr/index-en.aspx>.

- Public Safety Canada. "Fundamentals Of Cyber Security For Canada's CI Community." June 24, 2016. <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/2016-fndmntls-cybr-scrty-cmmnty/index-en.aspx>.
- Public Safety Canada. "Horizontal Evaluation Of Canada's Cyber Security Strategy." September 29, 2017. <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/vltm-cnd-scrty-strtg/index-en.aspx>.
- Public Safety Canada. "ICS Security Symposium 2019." Last modified January 31, 2019. <https://www.publicsafety.gc.ca/cnt/ntnl-scrty/cbr-scrty/ndstrl-cntrl-sstms/vnts-en.aspx#smptm1>.
- Public Safety Canada. "National Cross Sector Forum 2018-2020 Action Plan For Critical Infrastructure." May 11, 2015. <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/pln-crtcl-nfrstrctr-2018-20/index-en.aspx>.
- Public Safety Canada. "National Cyber Security Strategy." June 12, 2018. <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/ntnl-cbr-scrty-strtg/index-en.aspx>.
- Public Safety Canada. "National Strategy For Critical Infrastructure." November 11, 2011. <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx>.
- Public Safety Canada. "Public Report On The Terrorism Threat To Canada." December 14, 2018. <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/pblc-rprt-trrrsm-thrt-cnd-2018/index-en.aspx>.
- Public Safety Canada. "Security And Prosperity In The Digital Age: Consulting On Canada's Approach To Cyber Security." Last modified January 24, 2018. <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/2016-scrty-prsprty/index-en.aspx>.
- Public Safety Canada. "The Regional Resilience Assessment Program." August 13, 2018. <https://www.publicsafety.gc.ca/cnt/ntnl-scrty/crtcl-nfrstrctr/crtcl-nfrstrtr-rrap-en.aspx>.
- Quinn, Patrick. "CNL Opens National Innovation Centre For Cybersecurity." *Canadian Nuclear Laboratories (CNL)*. May 16, 2018. <http://www.cnl.ca/en/home/news-and-publications/news-releases/2018/cnl-opens-national-innovation-centre-for-cybersecu.aspx>.
- QuoteColo. "What's The Difference Between Cloud Computing And Software Defined Networks (SDN)?" December 8, 2015. <https://www.quotecolo.com/whats-the-difference-between-cloud-computing-and-software-defined-networks-sdn/>.
- Rambus Public Press Team. "An Introduction To Side-Channel Attacks." *Rambus*. May 24, 2018. <https://www.rambus.com/blogs/an-introduction-to-side-channel-attacks/>.

- Reuters. "Russia Says Stuxnet Could Have Caused New Chernobyl." *Reuters: News Bulletin*. January 26, 2011. <https://www.reuters.com/article/us-iran-nuclear-russia/russia-says-stuxnet-could-have-caused-new-chernobyl-idUSTRE70P6WS20110126>.
- Roberts, Tom. "The Impact Of Operational Events On The Network Structure Of The LVTS." *Bank of Canada: Discussion Paper*. August 2011. <https://www.bankofcanada.ca/wp-content/uploads/2011/08/dp2011-07.pdf>.
- Rockwell, Mark. "SDN Looms Large In NSTAC Report." *FCW: Cybersecurity Desk*. March 3, 2017. <https://fcw.com/articles/2017/03/03/sdn-nstac.aspx>.
- Rogge, Eric. "Why IoT And Not SCADA?" *Eckerson Group*. September 23, 2015. <https://www.eckerson.com/articles/why-iot-and-not-scada>.
- Rouse, Maragaret, and Michael Cobb. "Buffer Overflow." *TeachTarget: Search Security*. Last modified September 2016. <https://searchsecurity.techtarget.com/definition/buffer-overflow>.
- Royal Canadian Navy. "Exercise Cyber Challenge 2018." *RCN News and Operations*. May 7, 2018. <http://www.navy-marine.forces.gc.ca/en/news-operations/news-view.page?doc=exercise-cyber-challenge-2018/jgb8kpna>.
- Ruson, Marry-Ann. "Will 5G Be Necessary For Self-Driving Cars?" *BBC*. September 27, 2018. <https://www.bbc.com/news/business-45048264>.
- Sankar, Ashok. "To Effectively Protect Against Threats, Cyber Professionals Should Design Their Defenses Around An Assumption Of Compromise." *Raytheon*. July 2015. <https://www.raytheon.com/cyber/news/feature/blog-sankar-compromise>.
- Schulze, Holger. "Insider Threat Report 2018." *Crowd Research Partners with Cybersecurity Insiders*. November 2018. <https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf>.
- Shackelford, Scott J. and Zachery Bohm. "Securing Critical North American Infrastructure: A Comparative Case Study In Cybersecurity Regulation." *Canada-United State Law Journal* 40, no. 1 (2016): 61-70.
- Shaikh, Rafia. "Australia Wants To Make Cybersecurity Relevant." *WCCF Tech*. October 9, 2017. <https://wccftech.com/australia-cybersecurity-relevant-mums-dads/>.
- Sharp, Alastair and Jim Finkle. "Canada Worried About Infrastructure Hacks: Intelligence Official." *Reuters*. October 23, 2017. <https://www.reuters.com/article/us-cyber-summit-canada-infrastructure/canada-worried-about-infrastructure-hacks-intelligence-official-idUSKBN1CS2EZ>.

- Shaw, William. "SCADA System Vulnerabilities To Cyber Attack." *Electric Energy Online*. October 2004. <https://electricenergyonline.com/energy/magazine/181/article/SCADA-System-Vulnerabilities-to-Cyber-Attack.htm>.
- Shehod, Abir. "Ukraine Power Grid Cyberattack And U.S. Susceptibility: Cybersecurity Implications Of Smart Grid Advancements In The U.S." *MIT Sloan School of Management*. Working paper at the Cybersecurity Interdisciplinary Systems Laboratory, Cambridge, MA, December 2016. <https://cams.mit.edu/wp-content/uploads/2016-22.pdf>.
- Singh, Kanishka and Jack Stubbs. "Britain Does Not Support Total Huawei Network Ban: Sources." *Reuters*. February 17, 2019. https://www.reuters.com/article/us-britain-huawei-tech-idUSKCN1Q60NR?utm_campaign=trueAnthem:+Trending+Content&utm_content=5c6a2c9d3ed3f000010aa5de&utm_medium=trueAnthem&utm_source=twitter.
- Sobczak, Blake. "Canadian Utilities Got Head Start Against Russian Grid Threat." *E&E News*. July 26, 2018. <https://www.eenews.net/stories/1060091227>.
- Solomon, Howard. "Canada Helped Confirm North Korea Behind WannaCry Ransomware, Says U.S." *IT World Canada*. December 19, 2017. <https://www.itworldcanada.com/article/canada-helped-confirm-north-korea-behind-wannacry-ransomware-says-u-s/400152>.
- Solomon, Howard. "Hacktivist Group Temporarily Takes Down Canadian Federal Sites." *IT World Canada*. June 17, 2015. <https://www.itworldcanada.com/article/hacktivist-group-temporarily-takes-down-federal-sites/375450>.
- Solomon, Howard. "Ontario Electric Utilities To Report Soon On Their On Cyber Security Maturity." *IT world Canada*. January 18, 2019. <https://www.itworldcanada.com/article/ontario-electric-utilities-to-report-soon-on-their-on-cyber-security-maturity/414233>.
- Solomon, Howard. "Ontario Transit Agency Extremely Confident Cyber Attack Came From North Korea." *IT World Canada*. January 24, 2018. <https://www.itworldcanada.com/article/ontario-transit-agency-extremely-confident-cyber-attack-came-from-north-korea/401047>.
- Stewart, Scott. "The Coming Age of Cyberterrorism." *Stratfor Worldview*. October 22, 2015. <https://worldview.stratfor.com/article/coming-age-cyberterrorism>.
- Stubbs, Jack. "UK Government Officials Identify Security Risks With Huawei's Telecom Equipment." *Insurance Journal*. July 20, 2018. <https://www.insurancejournal.com/news/international/2018/07/20/495718.htm>.

- Technical Intelligence Group. “WannaCry Ransomware Attack.” *EY*. May 2017. [https://www.ey.com/Publication/vwLUAssets/ey-wannacry-ransomware-attack/\\$File/ey-wannacry-ransomware-attack.pdf](https://www.ey.com/Publication/vwLUAssets/ey-wannacry-ransomware-attack/$File/ey-wannacry-ransomware-attack.pdf).
- Technology Policy Program. “Global Cyber Strategies Index.” *Center for Strategic and International Studies*. Last modified 2019. <https://www.csis.org/programs/technology-policy-program/cybersecurity-and-governance/global-cyber-strategies-index>.
- The Japan Times. “Cyberattacks Targeting Japan Networks Hit A Record 128.1 Billion In 2016.” February 8, 2017. <https://www.japantimes.co.jp/news/2017/02/08/national/crime-legal/cyberattacks-targeting-japan-networks-hit-record-128-1-billion-2016/#.XHMfQy3MxsN>.
- Thompson, Nicole. “WannaCry Cyberattack Missed Canada On A Fluke: Professor.” *Huffington Post*. May 14, 2017. <https://www.huffingtonpost.ca/entry/16605402>.
- Threat and Analytics Team. “Hactivism: A Defenders Playbook.” *Deloitte LLP*. August 12, 2016. <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-hactivism.pdf>.
- Thurman, Mathias. “The WannaCry Scramble.” *Computer World*. May 25, 2017. <https://www.computerworld.com/article/3198473/malware-vulnerabilities/the-wannacry-scramble.html>.
- Threat Analysis Team. “SWIFT Systems And The SWIFT Customer Security Program.” *MWR Security*. Accessed on January 3, 2019. <https://www.mwrinfosecurity.com/assets/swift-whitepaper/mwr-swift-payment-systems-v2.pdf>.
- Tomas, Juan P. “U.S. Senator Warns About The Use Of Huawei Gear In Canada’s 5G Networks.” *RCR Wireless News*. January 7, 2019. <https://www.rcrwireless.com/20190107/5g/us-senator-warns-about-use-huawei-gear-canada-5g-network>.
- Underwood, Kimberly. “ISIS Takes Fight To Cyber Battlefield.” *SIGNAL Magazine*. November 1, 2017. <https://www.afcea.org/content/isis-takes-fight-cyber-battlefield>.
- Vigneault, David. “Remarks By Director David Vigneault At The Economic Club Of Canada.” Speech presented at Canadian Security and Intelligence Service and Economic Club of Canada Conference, Toronto, ON, December 2018.
- Vine, Doug. “Interconnected: Canadian And U.S. Electricity.” *Center for Climate Change and Energy Solutions*. March 2017. <https://www.c2es.org/site/assets/uploads/2017/05/canada-interconnected.pdf>.

- Volz, Dustin. "U.S. Government Concludes Cyber Attack Caused Ukraine Power Outage." *Reuters*. February 25, 2016. <https://www.reuters.com/article/us-ukraine-cybersecurity/u-s-government-concludes-cyber-attack-caused-ukraine-power-outage-idUSKCN0VY30K>.
- Wall, Matthew. "A Cyber-Attack Could Stop The Country." *BBC*. October 25, 2018. <https://www.bbc.com/news/business-45952693>.
- Weeks, Carly. "Computer Virus Causes Delays At Dozens Of Northern Ontario Hospitals." *The Globe and Mail*. January 18, 2019. <https://www.theglobeandmail.com/canada/article-computer-virus-causes-delays-at-dozens-of-northern-ontario-hospitals/>.
- Wood, Eric E. "Rogers To Support IoT Networks, Oil And Gas, Food Industries With New Services." *IT World Canada*. April 6, 2016. <https://www.itworldcanada.com/article/rogers-to-support-iot-networks-oil-and-gas-food-industries-with-new-services/382129>.
- Younis A., Younis. "Securing Access To Cloud Computing For Critical Infrastructure." PhD thesis, Liverpool John Moores University, 2015.
- Zelmer, Jennifer. "Cybersafe Healthcare: Options For Strengthening Cybersecurity In Canada's Health Sector." *Azimuth Health Group for HealthCareCAN*. September 2018. <http://www.healthcarecan.ca/wp-content/themes/camyno/assets/document/Cyber%20Security/Options%20Brief%20Summit%20Report.pdf>.
- Zetter, Kim. "Inside The Cunning, Unprecedented Hack Of Ukraine's Power Grid." *WIRED*. March 3, 2016. <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>.
- Zou, Xu. "IoT Devices Are Hard To Patch: Here's Why—And How To Deal With Security." *Tech Beacon*. Accessed on January 19, 2019. <https://techbeacon.com/security/iot-devices-are-hard-patch-heres-why-how-deal-security>.