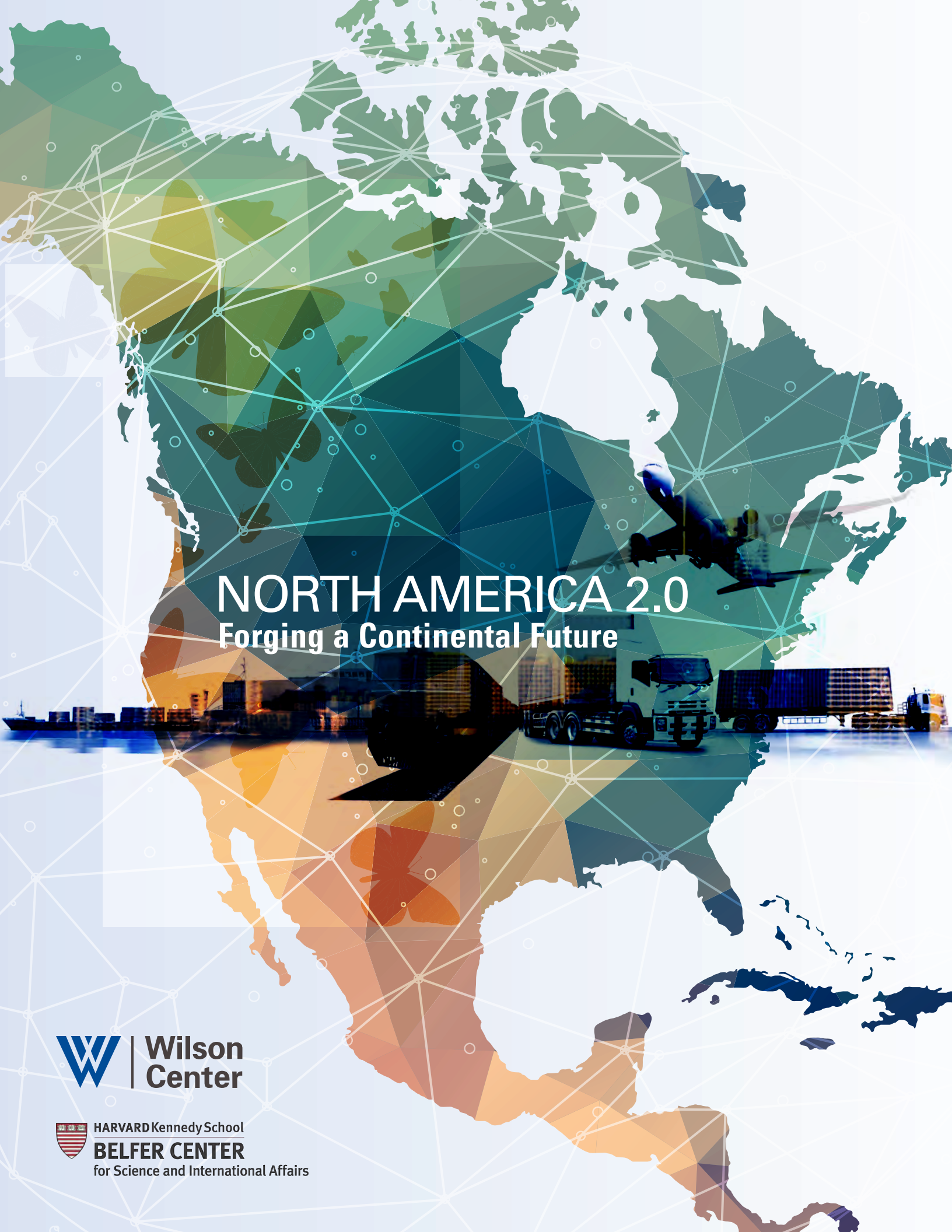

NORTH AMERICA 2.0

Forging a Continental Future

Wilson Center

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

Cybersecurity and Critical Infrastructure Resilience in North America

By Luisa Parraguez, Paul Stockton, and Gaétan Houle

May 2021
Working Paper*

This working paper will be published as a chapter in the forthcoming book, *North America 2.0: Forging a Continental Future.*

Cybersecurity and Critical Infrastructure Resilience in North America

Luisa Parraguez, Paul Stockton, and Gaétan Houle[1]

> *The terror of 9/11 and the failure of the three governments to build on the NAFTA foundation allowed old problems to fester and new problems to multiply. The fears that accompanied these problems made it hard to see that each crisis was connected, and that a solution would only become possible with a deeper level of cooperation.*
>
> – Robert A. Pastor, The North American Idea: A Vision of a Continental Future (Oxford University Press, 2011)

Introduction

The fast pace of technological advance and proliferation of malicious actors has caused cyber threats to North America to multiply. The more connected we are through digital platforms, the more vulnerable we are to criminal or unauthorized use of data. Threats to critical infrastructure have become a major concern for governments and the private sector, which constantly innovates to obtain maximum resilience and share the cost of security. Mexico, Canada, and the United States grapple with the classic security debate of how much privacy one is willing to hand over to ensure safety. If there is one clear example of a borderless North America, it is cyberspace. Across the region, interests are aligned and threats are shared, yet joint strategies are lacking, as each country does the best it can to protect itself against a constant flow of intrusions. As physical borders disappear in cyberspace, a large window of opportunity has opened for cooperative approaches to develop perimeter security for North American cyberspace. This chapter seeks to identify some of these shared challenges and opportunities, focusing on three areas where the opportunities for North American collaboration are greatest: protecting critical infrastructure, securing financial transactions, and improving public-private and regional cooperation to identify and mitigate cyberattacks.

As the world becomes more reliant on digital platforms, the volume, velocity, variety, and scale of cyber threats will only increase. Although ransomware attacks are becoming less frequent, malicious cryptomining is increasing; in 2021, illicit activity is predicted to account for over 70 percent of all cryptocurrency transactions.[2] The private and public sectors have been spending billions to defend against these threats each year; the North American cybersecurity market was estimated at US$51.6 billion in 2018 and is projected to reach US$82.5 billion by 2023.[3]

As cyber risks have increased, so too has the depth of integration across the continent. The manufacturing sectors of Mexico, Canada, and the United States have, especially in the context of NAFTA (North American Free Trade Agreement) and now the USMCA (United States-Mexico-Canada Agreement), joined together to create a single regional platform for production. Parts and materials now travel back and forth across the borders within North America during the manufacturing process, and industry in each country depends heavily on regular, on-time shipments of supplies from the others. A disruption at any node in the system, whether caused by a cyberattack or any other reason, can paralyze a production network until the issue is resolved. What is more, the energy systems powering regional production are also deeply intertwined. In 2020, Canada and Mexico were the number-one and number-two sources of oil imports for the United States, with 52 percent and 11 percent, respectively.[4] The United States and Canada have a fully integrated electric grid. Mexico shares limited integration with the North American grid,

but it has strong economic and environmental incentives to add connections in the coming decades. Migration, tourism, and trade throughout North America generate financial flows to send money to family members, pay for travel costs, and buy imported parts and materials. With so many nodes of connection across the region, each vulnerable to cyber risks in its own ways, cooperation to product regional systems is vital.

In response to rising cyber threats, the United States, Canada, and Mexico have all taken steps to identify critical cyber assets and prioritize cybersecurity as an issue of international importance. The U.S. Department of Homeland Security has identified 16 critical infrastructure sectors related to cybersecurity: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public sector, information technology (IT), nuclear reactors, materials and waste, transportation systems, water and wastewater systems.[5] In Canada, the Department of Public Safety has outlined 10 sectors with vital cyber assets in health, food, finance, water, information and transportation.[6] Mexico does not yet have a list of critical cyber infrastructure, but several important national strategies mention cybersecurity as a global concept.[7] Companies operating across North America also have taken significant steps to improve cybersecurity and, in some cases, to improve cooperation with one another and with all three governments.

No single actor has full awareness of or all the required tools to deal with cyber threats. As a result, it is tremendously important to create spaces and systems for the sharing of real-time information regarding the threat landscape and best practices in cybersecurity. Mechanisms for cooperation are needed among private sector actors, between businesses and government, and among governments. As proposed later in this chapter, the creation of a platform for the exchange of information among public and private actors across the North American continent would scale up the benefits of cooperation greatly.

In each country, substantial progress and innovation in cybersecurity is already underway. North America faces shared threats, especially to its critical infrastructure and financial sectors, as well as shared opportunities, such as public-private partnerships to make a more resilient cyber landscape. Sharing best practices on a trilateral basis gives each country a chance to strengthen cybersecurity at home and across the continent. This chapter reviews the approach each of the three North American governments has taken in facing cyber threats to financial transactions and critical infrastructure and identifies ways in which some of those approaches create opportunities for trilateral cooperation to strengthen continental security in this new and evolving realm.

Cyber Policy Background: United States

In 2018, former U.S. Director of National Intelligence Dan Coats warned that "the digital infrastructure that serves this country is literally under attack."[8] Since that warning, China, Russia, and other nations have intensified their efforts to implant advanced persistent threats in the systems that control essential public health and safety, economic, and national security infrastructure. The 2021 *Annual Threat Assessment of the US Intelligence Community* notes that "China can launch cyber attacks that, at a minimum, can cause localized, temporary disruptions to critical infrastructure within the United States."[9] Russia continues to target the industrial control systems critical to infrastructure operations "in the United States and in allied and partner countries, as

compromising such infrastructure improves—and in some cases can demonstrate—its ability to damage infrastructure during a crisis."[10]

Through these campaigns, potential adversaries can maintain a covert presence on infrastructure networks, install secret malware to disrupt grid operations, and conduct other malicious activities to attack critical system components.[11] *The National Counterintelligence Strategy of the United States of America, 2020–2022*, highlights both the severity of these cyber threats and the imperative to partner with Mexico, Canada, and other nations to counter them:

> Disruption of U.S. critical infrastructure could undermine our nation's security, economy, public health and safety in a variety of ways. For example, adversaries seeking to cause societal disruption in the United States could attack the electrical grid causing a large-scale power outage that affects many aspects of daily life. Additionally, foreign adversaries could disrupt the U.S. economy by interfering with the ability of individuals and businesses to conduct financial transactions. We must work with our allies and partners to identify and mitigate foreign intelligence threats to critical infrastructure upon which our collective national and economic security depends.[12]

To frame the need for North American collaboration more bluntly: adversaries are *preparing the battlefield* to create massive blackouts and other interruptions of critical services in the United States. Similar threats to Canadian and Mexican critical infrastructure and the interconnected nature of some infrastructure systems—the electric power grid in particular—make these cyber threats a truly trilateral issue.[13]

The utilities sector has extensive experience managing outages caused by natural disasters; however, adversary-induced disruptions present far more complex challenges. Unlike disruptions caused by natural hazards, adversaries can implant malware in infrastructure networks, enabling attacks and disrupting restoration efforts with limited physical strikes or operational information warfare. They also can map utilities' cyber systems, focusing their attacks on the most operationally critical assets to create widespread failures. As such, in addition to the traditional incident response roles and resources necessary in response to severe weather, infrastructure owners and operators, their government partners, and other stakeholders will need the resources to sustain and restore infrastructure in a contested environment.

Electric utilities and other energy sector companies are strengthening their coordination with federal and state governments to meet these challenges. As this chapter will discuss, equivalent improvements are underway in the financial services sector and other sectors critical to the U.S. economy. However, cyber threats to these critical systems are growing rapidly as well. Accelerated measures to strengthen the cyber resilience of U.S. infrastructure, and deepen collaboration between the United States and its neighbors, will be vital for years to come.

Cyber Policy Background: Canada

Canada has a robust critical infrastructure sector. Of the 10 critical infrastructure sectors established by the Government of Canada, the two most important are the energy sector (which includes electric utilities, nuclear energy, and oil and gas) and the financial sector. As these critical infrastructures focus on securing their networks, safeguarding citizens' personal information, and

building resilience against malicious actors, limited resources and an increasingly sophisticated threat environment pose challenges. To manage competing priorities, Canadian critical infrastructure organizations must collaborate to tackle cyber threats and address security risks.

In particular, Canadian organizations will have to address the country's lack of cybersecurity expertise. Though it is already in short supply, demand for cybersecurity talent in Canada is increasing by 7 percent annually.[14] Additionally, cybersecurity is rarely prioritized at the board level in private companies. IT or cybersecurity executives are underrepresented as board members, even at companies operating critical infrastructure in the energy and information and communications technology sectors. Moreover, in board meetings less than one hour per year is typically spent discussing cybersecurity matters, unless a security breach has occurred. Consequently, most chief information security officers have difficulty recruiting cybersecurity talent; to say the least, their cybersecurity programs are usually underfunded. Board members know cyber threats exist, and yet they do not sufficiently explore potential risks and solutions.

Digital technologies and the Internet increasingly are important to innovation and economic growth. As such, strong cybersecurity is critical to Canada's competitiveness, economic stability, and long-term prosperity. Accordingly, Canada's National Cyber Security Strategy was first promulgated in 2010 and updated in 2018.[15] The new strategy established three goals in response to evolving threats, emerging opportunities, and the need for collaborative action on cybersecurity: (1) secure and resilient Canadian systems, (2) an innovative and adaptive cyber ecosystem; and (3) effective leadership and collaboration. This framework came at an opportune time; cybercrime in Canada causes more than CA$3 billion in economic losses each year.[16]

After the Canadian government updated the country's National Cyber Security Strategy, it then provided cybersecurity funding for the 2018 and 2019 federal budgets totaling close to CA$1 billion. The strategy is designed to be adaptable, accounting for the continuously changing cyber landscape. The 2019 budget included CA$145 million to help to protect Canada's critical cyber systems, including in the finance, telecommunications, energy, and transport sectors. It also provided CA$80 million over four years to support three or more Canadian cybersecurity networks across Canada that are affiliated with postsecondary institutions.

To support these goals, Canada created the Canadian Centre for Cyber Security.[17] The center offers a unified approach to cybersecurity that builds on Canada's cybersecurity expertise and centralizes cyber innovation and collaboration in the country, providing a place for private and public sector partners to work side-by-side to solve Canada's most complex cyber issues. The center also launched the Learning and Innovation Hub, a trusted source of learning activities and programs for cyber security and communications security professionals working within the Government of Canada or Canadian business partners.[18] The Learning and Innovation Hub provides services, guidance, and advice on cybersecurity training and education to industry, academia, and other levels of government.

Cyber Policy Background: Mexico

Despite (and in some cases because of) its technological progress, Mexico faces significant cybersecurity challenges. The introduction and expansion of digital technologies into the production processes of various economic sectors, including manufacturing, has become apparent

in the country's expanding economic performance. In particular, technological expansion and the growth of Industry 4.0 contributed to the growth of the Mexican automotive and telecommunication sectors; currently, Mexico produces 80 percent of Latin America's high-tech exports.[19] Although Mexico as a whole is not yet the target of devastating cybersecurity threats from external actors, cyberattacks on Mexican institutions and individuals have at times jeopardized financial sector functions.[20] As a result, the federal government created institutions and legal frameworks to protect the economy and its citizens.

Mexico's 2005 National Security Law (Ley de Seguridad Nacional) regulates the organization and coordination of national security, including its critical infrastructure and institutional resiliency in the event of a cyber-disaster.[21] Though this law has not been updated since President Vicente Fox's term (2000–2006), it nevertheless identifies key threats to the nation, including foreign intervention in domestic issues, attacks on military and police bases, and attacks on public services. That said, even though the government recognizes the cybersecurity threat, there is no specialized center that deals with the national protection of Mexico's critical infrastructure. The Mexican government implemented new protocols following numerous incidents with private banks, but the information that has become public varies depending on the sensitivity of the situation and the actors involved. Similarly, the 2017 Personal Data Protection Law (Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados) has been critical in establishing rules concerning the management of sensitive information in the private sector, especially banks.[22] The Mexican government has an excellent legal framework on cybersecurity in comparison to other Latin American countries, but there are concerns regarding the lack of implementation, as there is no central structure to oversee data protection issues.

In recent years, the Mexican government has implemented several initiatives to increase and improve cybersecurity. Mexico's Computer Incident Response Team (CERT-MX) is one example. The Scientific Division of the Federal Police of Mexico is responsible for investigating national cybercrimes and is the host institution of CERT-MX. CERT-MX is a member of the global Forum for Incident Response and Security Teams and it has a collaboration protocol with other government agencies. CERT-MX is also responsible for protecting critical national infrastructure. A Specialized Information Security Committee was tasked with developing a National Strategy for Information Security. Mexican government agencies adhere to the Administrative Manual of General Management of Information, Communications and Cyber Security Technologies on international standards such as ISO 27001, ITIL and Cobit.

In 2019, the Mexican National Intelligence Center hosted an official meeting where representatives of the U.S. Federal Bureau of Investigation and the U.S. Department of Justice agreed with the Mexican government on a program to coordinate information exchange efforts concerning cybersecurity, including best practices in financial, telecommunications, and health for both countries.[23] Mexico is the country in Latin America with the second-most cyberattacks. Internet access is growing; 57.4 percent of Mexico's population use the internet, and most financial institutions offer online banking applications.[24] The COVID-19 pandemic has driven Mexico to leapfrog into the digital financial services as millions of lending, exchange, payments, and banking transactions are carried out through mobile devices and digital platforms.[25] Geolocation was also brought into the process in March 2021 for additional user security. Although private sector partnerships may be occurring in different economic sectors, little has leaked out to the public.

Mexico is still working on the fundamentals of cybersecurity and defense. As such, a large push is required to generate the political willpower to actually back macro-cybersecurity projects with sufficient funding. Technological advances and interconnectivity are not going to stop anytime soon. Therefore, Mexican cybersecurity must evolve quickly and to the best of its abilities.

Defining a North American Cyber-Agenda

Trilateral cooperation is required to bring together the three North American countries. All three are already interdependent in infrastructure and supply chains. Cyberattacks could seriously compromise the well-being of the region, in particular the financial and energy sectors. China has a strategy to set the global standards in cyberspace, and North America cannot step aside. Canada, Mexico, and the United States must place cybersecurity front and center. The current state of critical infrastructure security breaches and cyberattacks may come from many adversaries. Some of the threat vectors include supply chain corruption, attacks on electric grids, distributed denial of service (DDoS) attacks, data wiping, ransomware, and Artificial Intelligence (AI).

Current state of critical infrastructure security

The critical infrastructure supporting North American economies, national security, and public health and safety is increasingly integrated across national boundaries.[26] This integration entails both risks and opportunities for each country. Adversary attacks on lifeline systems in one nation may cause disruptions, either directly or indirectly, in the others. Yet the connectivity between these systems also provides unique opportunities to strengthen the security and emergency preparedness of all three nations.

The energy sector in particular exemplifies this growing integration. Canada, the United States, and Mexico "in many ways comprise one large, integrated market for energy commodities," including oil, natural gas, petroleum products, and electricity.[27] The U.S. and Canadian power grids are closely integrated, and Mexico is considering expanding its participation in the North American grid. This deepening energy integration offers compelling economic benefits for all three nations. Yet progress towards such integration differs by commodity and country. Electric infrastructure integration between Canada and the United States serves as "a global model of highly functional, cross-border electricity coordination."[28] U.S. and Canadian grids are connected by more than three dozen major transmission lines, ranging from the Pacific Northwest to New England. The resulting power flows have created a deeply integrated network of north-south electric infrastructure and synchronized cross-border operations. Additionally, the two countries are pursuing further connectivity with several new cross-border transmission lines currently in various phases of development—though some projects face permitting and other challenges.

The connectivity of North American infrastructure also creates risks of cross-border failures, as exemplified by the 2003 blackout, which started in Ohio and resulted in power outages for millions of customers in the U.S. and Canada.[44] Interconnections between U.S. and Canadian power systems have only increased since then. U.S. and Canadian officials warn that given this growing connectivity, "Isolated or complex events with cascading effects that can take place in either country can have major consequences for both the United States' and Canada's electric grids and adversely affect national security, economic, and public health and safety."[45] As Mexico and the

United States develop more synchronous ties between utilities on both sides of the border, they will face similar risks.

The U.S. and Canadian governments developed the Joint United States–Canada Electric Grid Security and Resilience Strategy in December 2016 to strengthen the security and resilience of the U.S. and Canadian electric grid from all adversarial threats and natural hazards. The strategy provides a policy framework for further improving integration and building coordination and information sharing mechanisms. It calls for collaboration to protect system assets and critical functions in both nations so that the North American grid can "withstand and recover rapidly from disruptions," and emphasizes the need for collaboration to manage contingences and enhance response and recovery efforts.

The integration of electric infrastructure between the United States and Mexico is much less mature. Even though the two countries have engaged in the electricity trade since 1905, there are few transmission connections between them. Indeed, the only synchronous connections exist at the border between Mexico and the state of California. Limited electricity trade also occurs across asynchronous interconnections between the Electric Reliability Council of Texas (ERCOT) and Mexican utilities. This case provides a key example of the benefits of integration: these interconnections are primarily used to supplement constrained electricity supplies and maintain reliability in emergencies. Nevertheless, the February 2021 blackouts that started in Texas and spread across the border into northern Mexico demonstrated the risks and potential benefits of electric grid integration between the United States and Mexico. Mexican president Andrés Manuel López Obrador was quick to blame the power shortage on grid interconnection and promote the benefits of Mexican energy independence.[29] However, Texas is susceptible to blackouts in the first place because its own grid is not connected to other major grids in the United States.[30] Greater grid integration would protect Texas and northern Mexico from future disruptive events.

Bilateral coordination to deepen integration between the United States and Mexico, as well as trilateral coordination that includes Canada, is underway. In 2017, former Secretaries of Energy Ernest Moniz (United States) and Pedro Joaquin Coldwell (Mexico) agreed to nonbinding pledges to increase this connectivity to strengthen reliability on both sides of the border. Later that year, NERC signed a Memorandum of Understanding (MOU) with the Mexico Comisión Reguladora de Energía (CRE) and the Centro Nacional de Control de Energía (CENACE) to formalize collaboration on several regulatory, technical, and operational challenges, including critical infrastructure protection. The MOU does not propose integrating regulatory schemes, but does recognize "the benefits of mutual collaboration to enhance reliability of electric power systems in Mexico and the United States of America."[31] Moreover, the U.S. Department of Energy's Quadrennial Energy Review specifically recommends increasing U.S.-Mexico bilateral cooperation on electric reliability as the latter expands its domestic and international electricity transmission systems, in addition to broader North American efforts.[32]

Although electric utilities and their government partners have taken major strides since the 2003 Ohio blackout to mitigate the risks of cross-border outages, that progress must accelerate. As energy sector integration across North America is deepening, potential adversaries are strengthening their abilities to attack that infrastructure, transforming the interconnected structure of the grid from a bulwark of reliability into a critical vulnerability. Developing a shared trilateral

understanding of emerging threats is a prerequisite for adopting new, collaborative approaches to improve continental grid resilience.

Cyberattacks and risks to critical infrastructure

The electricity subsector plays a unique role in enabling critical infrastructure sectors. Adversaries recognize the foundational importance of grid-provided power for societal continuity and will target electric infrastructure accordingly. Cyberattacks on the grid in Ukraine that caused widespread blackouts in 2015 and 2016 demonstrate potential threats to utilities in North America. In 2015, attackers hijacked the grid's operating systems to disconnect critical substations, creating brief but wide outages. Attackers were also able to "brick" operating system components and communications devices.[23] The 2016 cyberattack displayed more sophistication. After mapping the grid's operating systems, attackers used the system's internal control system (ICS) protocols to open circuit breakers, creating blackouts.[24] The malware was unusually difficult to detect, and included a wiper module that could brick grid control system components on a large scale.[25] Attackers also had the ability to deny or corrupt situational awareness data, making the grid extremely prone to cascading failures.[26] These cyberattacks moved cyberwarfare against electric systems from theory to limited (but unprecedented) practice.

Potential adversaries have conducted "test drives" of additional ways to attack the grid and other critical infrastructure. The ongoing Dragonfly campaign, conducted by cyberattackers within the Russian government, enables them to use utility vendors and other trusted third parties to conduct attacks on targeted systems.[27] Triton malware, in use since at least September 2017, poses another threat, enabling adversaries to corrupt safety systems that monitor and protect the performance of key system components, creating new pathways for adversaries to sabotage and intentionally incorrectly operate critical infrastructure.[28] The XENOTIME hacking group responsible for these attacks continues to target U.S. electric and oil and natural gas networks, and is considered the "most dangerous threat to ICS" owing to their proven ability to carry out destructive attacks.[29]

Yet these attacks do not reflect the true scale and severity of the cyber threat confronting the North American grid. Russia, China, North Korea, and other potential adversaries have powerful incentives to hold their most destructive cyberweapons in reserve; doing so helps hobble efforts at building protections against such weapons. Recent studies by the Department of Energy, other government departments, and cyber experts in both academia and the private sector highlight a range of potential cyber threats which these adversaries might use to cause outages far more severe than in Ukraine:

- *Supply chain corruption*. Infrastructure owners and operators often find it difficult to ensure the integrity of their supply chain.[30] As such, adversaries could disrupt the grid by corrupting widely used grid components, exploiting those common vulnerabilities to cause massive breakdowns.[31] Software, firmware, hardware, or network services are all vulnerable to supply chain compromise, potentially enabling adversaries to inject destructive malware or gain access to sensitive components and data in utility systems. This issue is particularly concerning for industry-standard grid components used by many utilities across the United States, creating the potential for threat actors to trigger widespread failures.

- *Attacks on electric grids*. Adversaries can cause outages using a variety of techniques. Protective relays that isolate faults to protect equipment and stem cascading power failures are prime targets. These relays were once electromechanical; now, much of the grid relies on microprocessor-based relays that are vulnerable to cyberattacks.[32] Adversaries can also use communication controls designed decades ago without any considerations for cybersecurity, to embed the protocol language into the malware to cause "cascading failures and . . . serious damage to equipment."[33] A new threat vector has emerged in part as a result of grid modernization. A drastic change in load could lead to instability and power swings, causing outages and equipment damage. For example, if adversaries gain access to large numbers of these smart meters, they could cause "a widespread blackout by switching smart meters on and off repeatedly."[34]
- *Distributed Denial of Service (DDoS) attacks*. Adversaries could also target critical infrastructure components with DDoS attacks to exacerbate the effects of a cyberattack and amplify restoration challenges. The proliferation of the Internet of Things (IoT) has expanded network connectivity to traditionally offline objects and devices, many of which are insufficiently secured. Adversaries have demonstrated their ability to compromise many of these new IoT devices and harness them in a botnet to overwhelm Internet-connected targets with web traffic.[35] As such, networked system control components may be vulnerable to DDoS attacks, and botnets pose a direct threat to grid instability. An adversary could also use a DDoS attack to disable key components in other critical infrastructure sectors, including communications systems vital to power restoration, as part of a larger cyber campaign against the grid.
- *Data wiping*. Adversaries will likely attempt to debilitate electric utilities by using data wiper modules to destroy large amounts of data or brick targeted systems.[36] Historically, wiper module attacks have been limited to wiping computers themselves, without targeting system networks themselves. The 2012 attack on Saudi Aramco, for example, wiped 30,000 Windows-based computers but did not affect industrial control systems.[37] More recent attacks, however, have included wiper modules that target control systems and networks. Future attacks may infect and effectively brick thousands of control system components. Disabling supervisory control and data acquisition (SCADA) systems adds risk and complicates grid operations, but will not interrupt power flows without some external form of disruption.[38] Moreover, because electric utility providers anticipate threats to SCADA systems, they have made plans to cope with the loss of SCADA functionality and have upgraded manual grid operation capabilities in the event of control systems degradation or failure.[39] Still, advanced adversaries could deploy wiper modules to compound and exacerbate the effects of a more complex cyberattack, delaying electric restoration by forcing infrastructure operators to manually operate portions of the grid.
- *Ransomware*. Ransomware attacks are a concerning threat to critical infrastructure information systems. Much like data-wiping malware, ransomware renders computers inoperable. Ransomware infects a computer system and restricts users' access to or encrypts the computer's content.[40] This malware often exploits network vulnerabilities and moves laterally, infecting as many endpoints as possible.[41] Once infected, the only way to restore functionality is to pay a ransom for each individual machine to the attacker or the actor launching the attack on their behalf. Otherwise, all infected endpoints must be replaced. Although recent attacks (including WannaCry and Petya/NotPetya) have been expansive, they did not present a particularly disruptive threat to the electric grid. However,

more advanced ransomware attacks have the potential to infect—and potentially act as a method to intentionally misoperate—industrial control systems. In a mock attack at the Georgia Institute of Technology, researchers were able to gain access and then send commands to programmable logic controllers in a simulated water plant. The researchers warned that these tactics are the "next logical step" for ransomware attacks.[42] Such an advanced form of ransomware attack has yet to occur, or at least be acknowledged publicly. However, as adversaries continue to improve their offensive capabilities, the use of ransomware to disrupt utility operations and restoration efforts present a growing threat.

- *Artificial Intelligence.* Over the longer term, adversaries may use AI to assist their attacks, making real-time defense against them much more difficult. AI may enable adversaries to design sophisticated and comprehensive cyberattacks against the electric grid by automating labor-intensive functions currently performed by high-skilled cyber personnel, thus lowering the human effort required to map U.S. utility infrastructure and control systems. Once attacks are underway, adversaries may also be able to use AI to help detect and maneuver around U.S. defensive measures, and do so at a "machine-speed" that overwhelms human decision-making.[43] China in particular has declared its intention to become the world leader in AI, and is committed to applying its expertise to "leapfrog" U.S. defense capabilities.[44] Russia is also ramping up its AI research and development efforts. U.S. power companies and their government partners will need to respond accordingly, and accelerate the implementation of grid protection measures to prevent AI-enabled attacks.

Taken together, these threat vectors pose a growing challenge for protecting the North American electrical grid, as well as the flow of natural gas on which power generation depends, from continent-scale attacks. Adversaries will likely use supply chain corruption, AI, and other means of attack create and exploit common grid system failures and vulnerabilities across North America. The United States, Mexico, and Canada must defend against these advanced cyber threats in a coordinated approach that accounts for deepening energy sector integration across the continent.

The NERC and Collaboration in Critical Infrastructure

Mandatory reliability standards between utility companies and public sector collaboration form the basis of continental cooperation to ensure electric grid resiliency throughout North America. The United States and Canada have especially strong mandatory reliability standards between their utilities to help reduce the risks of outages across the two countries. The North American Electric Reliability Council (NERC) began issuing standards applicable to both Canadian and U.S. utilities in the aftermath of the 2003 blackout.[79] These shared standards help power companies in both countries maintain the reliability of their systems, and will help them prevent instabilities from spreading during grid security emergencies. Currently, NERC reliability standards are mandatory and enforceable in the provinces of Alberta, British Columbia, Manitoba, New Brunswick, Nova Scotia, and Ontario, and are in the process of being adopted in Quebec.[80] Although NERC's jurisdiction does not include most of Mexico, NERC reliability standards are enforceable in interconnected jurisdictions of Baja California Norte.[81] Moreover, grid cooperation between the United States and Mexico has been deepening. The 2017 MOU between NERC, Mexico's federal energy regulator, and the independent system operator for Mexico's grid can and should lead to a similarly effective regulatory scheme as between the United States and Canada, and full electricity subsector coordination across North America.

NERC's role and structure as the Electric Reliability Organization for North America provides an additional bulwark for trinational grid resilience. Three of NERC's regional entities include power companies that extend across U.S. northern and southern borders: the Northeast Power Coordinating Council, the Midwest Reliability Organization, and the Western Electricity Coordinating Council. These entities help monitor and enforce compliance with reliability standards across borders, reinforcing NERC's integrated approach to risk reduction.[82]

In the face of rapidly intensifying threats, utilities and government partners also need to be able to share critical information. The NERC's Electricity Information Sharing and Analysis Center (E-ISAC) serves as an information sharing conduit both within the North American electric industry and between the electric industry and relevant government stakeholders for cyber and physical security threats. The E-ISAC facilitates communication of important or actionable information, and strives to determine and maintain "ground truth" during rapidly evolving security events. The E-ISAC also plays an essential role in cross-sector coordination, focusing on key interdependencies between electric and other sectors, such as natural gas, water, and other critical infrastructure.[83]

Grid security coordination is expanding across the public sector as well. As the Department of Energy's Quadrennial Energy Review notes, "coordination of grid security efforts can lead to a more proactive approach to addressing emerging threats across North America," and the countries have "much to gain from collaborative planning, strategy, and cooperation" regarding the power sector.[84] Capitalizing on these opportunities, the U.S. Department of Energy is collaborating with Canadian and Mexican government agencies to improve trilateral coordination concerning grid security and resilience. The department's analysis also emphasizes that changes in the electricity subsector, along with growing integration of the U.S. and Mexican power systems, provides both an opportunity for significant mutual benefit and a substantial need for "technology, policy and regulatory solutions to reliability and security challenges."[85]

Together with the voluntary grid defense measures taken by utility providers beyond those required by NERC standards, these ongoing initiatives provide a strong basis for progress. Yet amid intensifying cyber threats and deepening energy infrastructure integration across the continent, government agencies and utility providers in Canada, Mexico, and the United States should consider adopting further mechanisms for and methods of collaboration.

Strengthening the Cyber Resilience of the Financial Services Sector and Other Critical Infrastructure

Potential adversaries have an array of targets beyond the energy sector to hold at risk of disruption in future crises. The financial services sector is especially significant in this regard because of its foundation importance to the economies of Mexico, Canada, and the United States. Some recent attacks on the financial system, including those perpetrated by Russia and North Korea, were simply efforts to steal money.[33] Others, including Iran's DDoS attacks against nearly 50 major financial institutions between 2011 and 2012, sought to achieve broader systemic effects as a likely response to U.S. attacks on Iranian systems.[34] U.S. officials also found malware reportedly developed by Russia's Federal Security Service (the successor to the KGB) on Nasdaq servers in 2010.[35] The U.S. Department of the Treasury has warned that future attacks could create much

more disruptive effects, and in January 2020 called for banks and financial markets to provide additional details about the cybersecurity risks they face.[36]

Already, however, the Treasury Department and analysts such as Jason Healey have identified specific "channels" by which cyber events could create a financial crisis. Cyberattacks that corrupt or deny access to financial data could create of loss of confidence in the system and other far-reaching effects.[37] Cyberattacks on critical sector hubs and functions could also inflict systemic disruption. For example, the Federal Reserve Bank of New York has identified the wholesale payment network as constituting a "natural candidate for a malicious attacker intent on inflicting the largest possible damage to the financial system and the broader economy." In addition to disrupting critical functions, the bank emphasizes that such attacks could also trigger panic-based runs on banks and spillovers into the financial sector as a whole.[38]

Significant efforts to meet these challenges are underway. The Financial Systemic Risk Analysis & Resilience Center is addressing the systemic dangers posed by current and emerging cyber threats to the U.S. financial system.[39] Financial institutions, the Treasury Department, and academic researchers have been developing options to help defend financial systems.[40] The Hamilton exercise series conducted by the financial services sector and the Treasury Department represents additional progress for strengthening industry-government coordination against cyberattacks.[41] Going forward, U.S. sector leaders and their government partners should consider additional ways to collaborate with their counterparts in Mexico and Canada (and globally) to bolster financial sector resilience on a continent-wide basis.

The Canadian Cyber Threat Exchange and Collaboration in the Financial Sector

Cybersecurity success or failure hinges on the ability of individuals, government, and industry to share information. Information sharing challenges are not new. Successful information sharing requires trust, a solid policy framework, and commitment from all parties to solve specific cybersecurity problems.

Today, neither the private nor public sectors have a complete picture of Canada's cybersecurity posture or a consolidated view of cyber threats that impact the nation. To facilitate cyber threat information sharing and threat awareness across critical infrastructure sectors, the Canadian Cyber Threat Exchange (CCTX) was created in 2013.The CCTX acts as a hub where Canadian businesses and government agencies can share timely cyber threat information. It also provides cyber threat analysis and risk mitigation recommendations. Working closely with Canadian government and law enforcement agencies, the CCTX consolidates the cyber threats to Canada's private sector and serves as a point of contact for cyber information sharing organizations in other countries. It cross-sectoral approach engages companies of all sizes—as well as their supply chain partners and suppliers, vendors, and customers—to advance the cyber resiliency of all elements of the economy.

Participation in cyber threat information sharing networks and collaboration forums will strengthen and better prepare to mitigate or eliminate new and evolving cyber threats, both as individual organizations and collectively.[57] Another example of an initiative to bring together private-public partnerships is the CyberPeace Institute (CPI), an international nongovernmental organization that seeks accountability in cyberspace and provides assistance to victims of attacks by increasing their digital resilience and capacity to respond and recover. The CPI launched an initiative to deal with

healthcare hacks and stop cyber operations against medical facilities during the COVID-19 pandemic.[42]

Notably, although the CCTX is a nonprofit organization, its services are not free. Yet the CCTX is still in its infancy, and the quality and value of its services will increase proportionally with the membership. Ultimately, the CCTX could serve as a model for other countries, including the United States and Mexico, to follow; an extension of the CCTX framework would allow further information sharing between the countries' threat exchange centers.

Conclusion

The emergence of cybersecurity issues as a major security concern in the first decades of the 21st century has left many countries and sectors vulnerable. Canada, Mexico, and the United States all need to take steps to protect the privacy, finances, and safety of their own citizens. Collaboration between the three countries is not only the most effective way to do this, but, in sectors such as energy and supply chain protection, the integrated nature of North America makes collaboration a necessity. However, the North American community currently lacks the mechanisms to facilitate such international collaboration between their private and public sectors. To further improve cybersecurity in the region, the United States, Mexico, and Canada should develop a North American network for private-public cooperation and information exchange. As a model, it is helpful to consider the example of Canada's CCTX.

As previously stated about Canada, neither the North American public nor the private sector has a complete understanding of the cyber threats the continent faces. Businesses must consider how threats to government-run utilities can impact their business models. The 2021 SolarWinds hack, in which hackers who gained access at least nine government agencies and nearly 100 private organizations across the continent, is evidence of the danger that software vulnerabilities can cause both the private and the public sector.[43] Furthermore, no one country can be aware of threats it faces without eyes on the other two. Supply chain disruption in Mexico could impact production of medical or military equipment in Canada or the United States, and damage to electrical or water infrastructure in the United States could impact either one of its neighbors. As a result, there is a need to reach beyond the scope of the CCTX and present a united front against cybercrime.

The development of a CCTX-style North American network to combat cybersecurity challenges is a solution distinctly North American in character. A network that serves to enable cooperation and information exchange will address the blind spots that each country has in the other and allow best practices to spread across the continent, in turn making each country more resilient. In addition, the existence of such an institution will be a resource for governments and organizations that inevitably will face cybersecurity concerns in the future. However, the network avoids the added bureaucracy of more formal institutional solutions, reflecting a North American culture of pragmatism. Rather than relying on European-style political institutions, a North American cybersecurity network could give participants the advantage of communicating across national boundaries while maintaining the freedom to find solutions for themselves.

Using the CCTX as a model, Canada, Mexico, and the United States should build an adaptable organization that unites the private and public sectors around cyber defense. Cyberspace is now a

vital component across social, political, environmental, and economic sectors. To build a stronger future across each sector in North America, protecting cyberspace will have to be a priority.

---

[1] Luisa Parraguez offers many thanks to those who were interviewed at SEMAR (Secretaría de Marina), SEDENA (Secretaría de la Defensa Nacional), SRE (Secretaría de Relaciones Exteriores), SEGOB (Secretaría de Gobernación), INAI (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales), INEGI (Instituto Nacional de Estadística y Geografía), the financial sector and banks, programmers, engineers and security experts. Paul Stockton offers special thanks to Rob Denaburg, director of security research and analysis at Sonecon, LLC, for his many contributions to the chapter. Gaétan Houle offers special thanks to Alan Jones, former deputy director at the Canadian Security and Intelligence Services, and Robert Gordon, executive director at the Canadian Cyber Threat Exchange, for their valuable contributions to the chapter. The authors would like to thank James Chabin, research assistant at the Wilson Center, for his excellent support in preparing this chapter.

[2] CISCO, "Cryptomining: A Wolf in Sheep's Clothing Is Still a Wolf," in *Defending Against Today's Critical Threats: February 2019 Threat Report* (San Jose, CA: CISCO, February 2019), https://www.cisco.com/c/dam/global/en_uk/assets/pdfs/en_cybersecurityseries_thrt_01_0219_r2.pdf; and Cybersecurity Ventures. "2019 Cybersecurity Statistics," 2019, https://cybersecurityventures.com/research/.

[3] BCC Research, *Cyber Security: North American Markets* (Wellesley, MA: BCC Research, December 2018), https://www.bccresearch.com/market-research/information-technology/cyber-security-north-american-markets.html.

[4] U.S. Energy Information Administration, "Oil and Petroleum Products Explained," April 13, 2021, https://www.eia.gov/energyexplained/oil-and-petroleum-products/imports-and-exports.php.

[5] Department of Homeland Security, "Critical Infrastructure Sectors," accessed on April 28, 2021, https://www.dhs.gov/cisa/critical-infrastructure-sectors.

[6] Public Safety Canada, "Critical Infrastructure," accessed on April 28, 2021, https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-en.aspx.

[7] The Mexican strategic documents that mention cybersecurity include the following: Sistema Nacional de Información Estadística y Geográfica, *Plan Nacional de Desarrollo, 2013–2018* (2013), 107, https://www.snieg.mx/contenidos/espanol/normatividad/MarcoJuridico/PND_2013-2018.pdf; Consejo Nacional de Seguridad Pública, *Programa para la Seguridad Nacional 2014–2018* (2014), 64, https://www.casede.org/BibliotecaCasede/Programa_SeguridadNacional.pdf; Government of Mexico, *Estrategia Nacional de Ciberseguridad* (2017), https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf; Secretaría de Gobernación, *Plan Nacional de Desarrollo 2019–2024* (2019), 173, http://gaceta.diputados.gob.mx/PDF/64/2019/abr/20190430-XVIII-1.pdf

[8] Julian Barnes, "'Warning Lights Are Blinking Red,' Top Intelligence Officer Says of Russian Attack," *New York Times*, July 13, 2018, https://www.nytimes.com/2018/07/13/us/politics/dan-coats-intelligence-russia-cyber-warning.html.

[9] Office of the Director of National Intelligence (ODNI), *Annual Threat Assessment of the US Intelligence Community* (April 2021), 8, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf.

[10] ODNI, *Annual Threat Assessment*, 10

[11] "Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," U.S. Computer Emergency Readiness Team (US-CERT), March 15, 2018, https://www.us-cert.gov/ncas/alerts/TA18-074A; Defense Science Board, *Task Force on Cyber Deterrence* (Washington, DC: Department of Defense, February 2017), 4, https://www.acq.osd.mil/dsb/reports/2010s/DSB-cyberDeterrenceReport_02-28-17_Final.pdf; ICF International, *Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats* (Fairfax, VA: ICF International, June 2016), 19, https://www.energy.gov/sites/prod/files/2017/01/f34/Electric%20Grid%20Security%20and%20Resilience--Establishing%20a%20Baseline%20for%20Adversarial%20Threats.pdf.

[12] U.S. National Counterintelligence Center, *National Counterintelligence Strategy of the United States of America, 2020–2022*, (Washington, DC: ODNI, January 7, 2020), 6, https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf.

[13] "Protecting the Power Grid," Canadian Electricity Association, n.d., https://electricity.ca/lead/powering-canadas-economy/protecting-power-grid/; and Luisa Parraguez Kobek, *The State of Cybersecurity in Mexico: An Overview* (Washington, DC: Mexico Institute, Wilson Center, January 2017), 14, https://www.wilsoncenter.org/sites/default/files/cybersecurity_in_mexico_an_overview.pdf.

[14] Deloitte, "The Changing Faces of Cybersecurity: Closing the Cyber Risk Gap," last modified June 10, 2018, https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-cyber-talent-campaign-report-pov-aoda-en.PDF.

[15] Public Safety Canada, "National Cyber Security Strategy," last modified May 28, 2019, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx.

[16] Public Safety Canada, "National Cyber Security Action Plan (2019–2024)," last modified April 15, 2020, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/index-en.aspx.

[17] Canadian Centre for Cyber Security, "Cyber Centre Expertise," last modified June 12, 2018, https://www.cyber.gc.ca/en/.

[18] Canadian Centre for Cyber Security, "Cyber Centre Learning Hub," last modified June 24, 2019, https://www.cyber.gc.ca/en/learning-hub.

[19] The definition of Industry 4.0 was taken from the *EU Parliament 2016 Report on Industry 4.0* (European Parliament 2016), 20, http://www.europarl.europa.eu/RegData/etudes/STUD/2016/570007/IPOL_STU(2016)570007_EN.pdf. On Mexico's high-tech exports, see Promexico, "Crafting the Future: A Roadmap of the Industry 4.0 in Mexico", 11, http://mim.promexico.gob.mx/work/models/mim/templates-new/Publicaciones/Routemap/RM-I4CF.pdf**.**

[20] Interviews with financial and banking sector specialists in Mexico provide information on a wide spectrum of attacks that are nor publicized for fear of creating a customer whiplash and lack of trust in the institutions.

[21] Ley de Seguridad Nacional, Cámara de Diputados, Mexican Government, December 26, 2005, http://www.diputados.gob.mx/LeyesBiblio/pdf/LSegNac.pdf.

[22] "Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados," Cámara de Diputados, Mexican Government, January 26, 2017, http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf.

[23] Benjamin A. Powel & Jason C. Chipman, *Cybersecurity 2021* (London: Law Business Research Ltd., February 2021), 2021_cybersecurity_Mexico.pdf (creel.mx).

[24] GPHadmin, "Cybersecurity Regulations for Financial Institutions," February 24, 2021, https://www.gphlegal.mx/2021/02/24/cybersecurity-regulations-for-financial-institutions/.

[25] Fernando Gutierrez, "Banca debe de estar a la altura de la digitalización," *El Economista*, March 11, 2021, https://www.eleconomista.com.mx/sectorfinanciero/Banca-debe-de-estar-a-la-altura-de-la-digitalizacion-Mastercard-20210311-0116.html.

[26] This book uses the definition of "critical infrastructure" provided in the 2013 Presidential Policy Directive (PPD)-21: "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." See White House, "PPD-21 – Critical Infrastructure Security and Resilience," February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[27] Paul W. Parfomak et al. *Cross-Border Energy Trade in North America: Present and Potential*, R44747 (Washington, DC: Congressional Research Service, January 24, 2017), 1, https://fas.org/sgp/crs/misc/R44747.pdf.

[28] "Enhancing Electricity Integration in North America," in *QER Report: An Integrated Study of the U.S. Electricity System* (Department of Energy, January 2017), https://www.energy.gov/sites/prod/files/2017/01/f34/Chapter%20VI%20Enhancing%20Electricity%20Integration%20in%20North%20America_0.pdf.

[29] Amy Stillman, "Mexico Blames U.S. as Energy Crisis Spills Across the Border," Bloomberg, February 15, 2021, https://www.bloomberg.com/news/articles/2021-02-15/mexico-blames-u-s-as-energy-crisis-spills-across-the-border.

[30] Benji Jones, "Texas Blackouts Explained: Arctic Weather Shut Down Power Plants as Demand for Heat Surged, and the State's Grid Is on Its Own," Business Insider, February 18, 2021, https://www.businessinsider.com/texas-blackouts-millions-lost-power-in-storm-went-wrong-2021-2.

[31] For the final text of the MOU, see https://www.nerc.com/AboutNERC/keyplayers/Documents/MOU%20Clean%20NERC_CRE_CENACE_EN%20FINAL.pdf.

[32] U.S. Department of Energy, "North American Energy Cooperation," Office of International Affairs, n.d., https://www.energy.gov/ia/international-affairs-initiatives/north-american-energy-cooperation.

[33] Kate Fazzini, "'Evil Corp': Feds Charge Russians in Massive $100 Million Bank Hacking Scheme," CNBC, December 5, 2019, https://www.cnbc.com/2019/12/05/russian-malware-hackers-charged-in-massive-100-million-bank-scheme.html; and Evan Perez and David Shortell, "North Korean-backed Bank Hacking on the Rise, US

Officials Say," CNN, March 1, 2019, https://www.cnn.com/2019/03/01/politics/north-korea-cyberattacks-cash-bank-heists/index.html.

[34] "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector," U.S. Department of Justice, March 24, 2016, https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged.

[35] Benjamin Brake, *Strategic Risks of Ambiguity in Cyberspace*, Contingency Planning Memorandum No. 24 (Washington, DC: Council on Foreign Relations, May 14, 2015), 3, https://cdn.cfr.org/sites/default/files/pdf/2015/05/CPA_ContingencyPlanningMemo_24.pdf. The National Security Agency reportedly concluded it was possible that the malware—similar but not identical to a strain created by Russian security services—was used by a different government actor such as China. See Adi Robertson, "Russian Malware Infiltrated the Nasdaq Servers, Says Businessweek," The Verge, July 17, 2014, https://www.theverge.com/2014/7/17/5912159/russian-malware-infiltrated-the-nasdaq-stock-exchange-says-businessweek.

[36] Office of Financial Research, *2016 Financial Stability Report* (Washington, DC: Department of the Treasury, December 2016), 38–48, https://www.financialresearch.gov/financial-stability-reports/2016-financial-stability-report/. The Federal Reserve Bank of New York also recently released a report that examines potential cascading effects of attacks on large U.S. banks: Thomas M. Eisenbach, Anna Kovner, and Michael Junho Lee, *Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis*, Staff Report 909 (New York: Federal Reserve Bank of New York, January 2020), https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr909.pdf. For the Treasury Department's call for additional cyber data, see Department of the Treasury, "Agency Information Collection Activities; Proposed Collection; Comment Request; Financial Sector Critical Infrastructure Cybersecurity Survey," *Federal Register* 85, no. 14 (2020): 3761–62, https://www.govinfo.gov/content/pkg/FR-2020-01-22/pdf/2020-00898.pdf.

[37] Office of Financial Research, *Cybersecurity and Financial Stability: Risks and Resilience* (Washington, DC: Department of the Treasury, February 2017), https://www.financialresearch.gov/viewpoint-papers/files/OFRvp_17-01_Cybersecurity.pdf; Jason Healey et al., *The Future of Financial Stability and Cyber Risk* (Washington, DC: Brookings Institution, October 2018), 3–6, https://www.brookings.edu/wp-content/uploads/2018/10/Healey-et-al_Financial-Stability-and-Cyber-Risk.pdf. The study also provides a useful bibliography of research on cyber risks to the sector on page 6.

[38] Eisenbach, Kovner, and Lee, *Cyber Risk and the U.S. Financial System*, 1, 2.

[39] Healey et al., *The Future of Financial Stability and Cyber Risk* , 1.

[40] Healey et al., *The Future of Financial Stability and Cyber Risk*, 1, 8.

[41] Financial Services Information Sharing and Analysis Center, "Exercises," n.d., https://www.fsisac.com/hubfs/Resources/FS-ISAC_ExercisesOverview.pdf.

[42] For more on the CyberPeace Institute see https://cyberpeaceinstitute.org/.

[43] Douglas MacMillan and Aaron Schaffer, "Breached Software Firm SolarWinds Faces SEC Inquiry after Insider Stock Sales," *Washington Post*, March 1, 2021, https://www.washingtonpost.com/business/2021/03/01/solarwinds-sec-inquiry/.