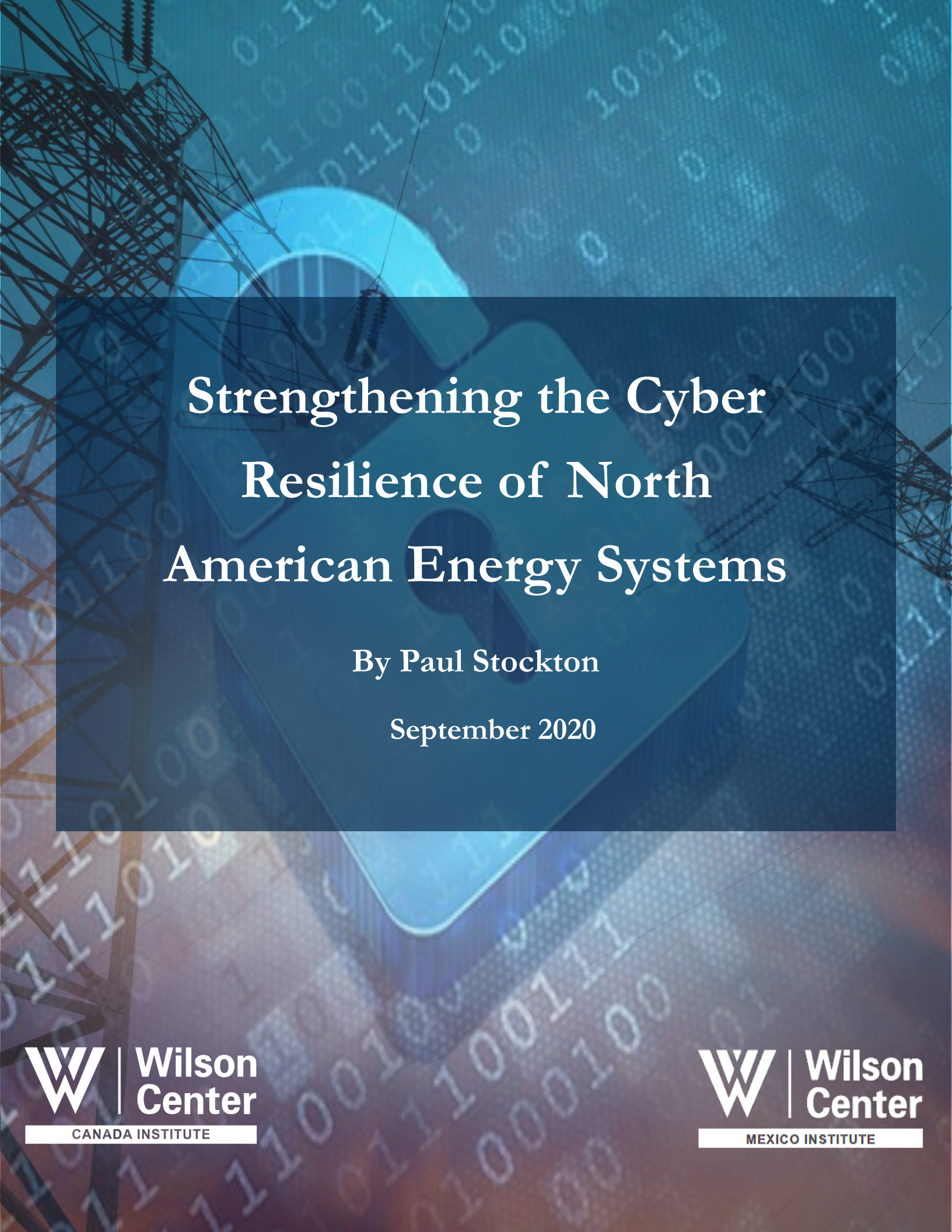


Strengthening the Cyber Resilience of North American Energy Systems

By Paul Stockton

September 2020

Wilson Center
CANADA INSTITUTE

Wilson Center
MEXICO INSTITUTE

Strengthening the Cyber Resilience of North American Energy Systems

By Paul Stockton[1]

Cyber threats to the power grid and oil and natural gas systems in North America are rapidly intensifying. System operators in Mexico, Canada, and the United States are bolstering their resilience against these threats and deepening collaboration with their respective governments. At the same time, energy infrastructure is increasingly integrated across the content. The nations of North America should not only improve infrastructure security within their own borders, but also launch new collaborative efforts to bolster their shared resilience against cyberattacks.

Opportunities for trilateral cooperation are especially promising – and necessary – for electric systems. Two very large and three smaller alternating current (AC) "interconnections" span the United States and much of Canada.[2] One of these systems, the Western Interconnection, includes a small portion of Mexico's Baja California. Grid transmission operators in the United States and Mexico are also exploring options to expand cross-border flows of electricity via Texas's ERCOT Interconnection.[3] Electrons flow across these interconnections without regard to (and unimpeded by) national borders.[4]

---

[1] Paul Stockton is Managing Director of Sonecon LLC, a strategic advisory firm in Washington, DC, and served as Assistant Secretary of Defense for Homeland Defense from 2009-2013. Dr. Stockton offers special thanks to Rob Denaburg, Director, Security Research & Analysis, Sonecon, LLC, for his many contributions to the study. He also thanks Alan Bersin, Stuart Brindley of J.S. Brindley Consulting, Matt Duncan, Luisa Parraguez, Pat Hoffman, Gaétan Houle, Chuck Kosak and Lt. Gen. Chris Miller, USAF (Ret). The views expressed in this article are those of the author and do not reflect the official policy or position of the Department of Defense or the US Government.

[2] "Learn More About Interconnections," U.S. Department of Energy, n.d., https://www.energy.gov/oe/services/electricity-policy-coordination-and-implementation/transmission-planning/recovery-act-0.

[3] Tom Kleckner, "FERC OKs DC Tie Operations Between Texas, Mexico," RTO Insider, July 31, 2018, https://rtoinsider.com/ferc-aep-ercot-mexico-dc-tie-connections-97152/. For the original FERC order, see: FERC, *Proposed and Final Order Directing Transmission Service*, 164 FERC ¶ 61,056 (Docket No. TX18-1-000), July 26, 2018, https://www.ferc.gov/CalendarFiles/20180726154430-TX18-1-000.pdf.

[4] For an explanation of basic grid operations and the structure of the interconnected North American electric grid, see: Federal Energy Regulatory Commission (FERC), *Reliability Primer*, 2016, https://www.ferc.gov/legal/staff-reports/2016/reliability-primer.pdf; "Learn More About Interconnections," DOE, n.d.,

The grid's integrated structure enables power companies to provide more reliable service than is possible with smaller, separated systems that cannot assist each other when instabilities emerge. The scale of the interconnected North American electric system and the high voltage transmission lines that provide its backbone help bring wind and solar-generated power from remote regions to cities where that power is needed. Grid integration also helps expand energy markets, attract private investment, lower capital costs and energy costs for consumers, and provide for a more diverse mix of energy resources to increase energy security.[5]

However, threats to North American energy systems are intensifying. On May 1, 2020, President Donald Trump declared that threats to the U.S. power grid constituted a "national emergency."[6] China and other potential adversaries are also improving their capabilities to attack the natural gas pipelines that fuel power generation across much of the continent. Cyberattacks on grid and gas systems can also have disruptive effects far beyond the energy sector. Hospitals, water systems, seaports, and other electricity-dependent facilities will be crippled if attackers can create wide area blackouts. These dependencies make the energy sector an especially lucrative target for adversaries seeking to maximize the devastation they inflict.

Each nation in North America is striving to bolster the resilience of its own infrastructure. However, the interconnected structure of the grid also creates a shared problem: cyber-induced outages in one nation can rapidly spread to its neighbors unless grid operators collaborate to avert such cascading failures. As cyber threats become more severe, the United States, Canada, and Mexico will need to ramp up plans and capabilities to coordinate cross-border response operations accordingly.

---

https://www.energy.gov/oe/services/electricity-policy-coordination-and-implementation/transmission-planning/recovery-act-0.

[5] United States Government Accountability Office (GAO), *NORTH AMERICAN ENERGY INTEGRATION: Information about Cooperation with Canada and Mexico and among U.S. Agencies* (GAO-18-575), August 2018, p. 5, https://www.gao.gov/assets/700/693644.pdf.

[6] The Executive Order cites one threat as especially dangerous: the risk that foreign adversaries will corrupt the supply chains for critical grid equipment. See: President Donald J. Trump, *Executive Order on Securing the United States Bulk-Power System*, May 1, 2020, https://www.whitehouse.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/.

A solid foundation already exists to make such improvements. The North American Electric Reliability Corporation (NERC) provides mandatory standards for physical and cybersecurity that apply to the four continental interconnections.[7] Power companies also have extensive experience in assisting each other across national, state, and provincial borders to manage disturbances to the grid caused by severe storms and other familiar hazards.[8] Now, thanks to the GridEx exercise system and other initiatives, U.S. and Canadian grid operators are also strengthening their ability to coordinate emergency response operations against cyber and physical attacks.[9]

Government-to-government collaboration is improving as well. The U.S. Department of Energy (DOE), the U.S. Department of Homeland Security (DHS), and other federal departments are strengthening coordination with their Canadian and Mexican counterparts to collaborate in the face of natural and manmade threats to electric systems and interdependent infrastructure sectors. A 2016 joint strategy between the U.S. and Canadian governments called for a collective effort 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 contingencies and enhance response and recovery efforts.[10] Including Mexico in such collaborative efforts could extend their benefits on a continent-wide scale.

The ongoing development of a North American Energy Resilience Model (NAERM) provides an additional foundation for progress. The NAERM is helping DOE, its National Laboratories, and industry create a comprehensive model of North American energy sector infrastructure, including natural gas, electric, and other energy systems. The NAERM will be particularly helpful for

[7] NERC provides mandatory physical and cyber security standards for those Bulk Power system (BPS) utilities whose facilities are essential to the operation of the three main continental interconnections, versus smaller utilities that are limited to power distribution roles.

[8] Note: In the United States, these power companies are called "utilities." In Canada, "utilities" refers to the service offered by "utility providers." However, this paper uses U.S. terminology.

[9] North American Electric Reliability Corporation (NERC), *GridEx V: Lessons Learned Report*, March 2020, p. *viii*, https://www.nerc.com/pa/CI/CIPOutreach/GridEX/TLP%20WHITE%20GridEx%20V%20Lessons%20Learned%20MAR20.pdf.

[10] Governments of the United States and Canada, *Joint United States-Canada Electric Grid Security and Resilience Strategy*, December 2016, pp. 11-12, https://www.whitehouse.gov/sites/whitehouse.gov/files/images/Joint_US_Canada_Grid_Strategy_06Dec2016.pdf.

assessing potential threats to these interdependent systems and developing strategies to mitigate them.[11]

However, given the increasingly severe threats to electric and natural gas systems, existing government plans and mechanisms for cross-border coordination are inadequate. This paper analyzes improvements in adversary cyberattack capabilities that pose especially significant risks to energy infrastructure. The paper then examines opportunities to deepen collaboration between Canada, Mexico, and the United States against these threats. In particular, the paper analyzes initiatives that can help strengthen plans and capabilities for cross-border coordination in ways that respect each nation's sovereignty and that supplement the significant resilience initiatives already underway across the continent.

One opportunity for progress lies in developing a trilateral assessment of cyber threats to North American electric systems. While many emergency operations can help manage grid instability regardless of cause, improvements in cyber weapons are creating new threat vectors that require specialized plans and power restoration capabilities. U.S. and Canadian governments already engage in extensive threat information sharing. Valuable precedents exist to include Mexico in such efforts and share perspectives on emerging threats. The analysis that follows examines the benefits of establishing a trilateral threat assessment, highlights specific cyberattack vectors that the assessment should include, and identifies emerging challenges to address – including power restoration operations in future pandemics.

Another opportunity for progress lies in improving coordination of government emergency measures. While grid owners and operators are responsible for protecting and restoring the reliability of their systems in an emergency, government agencies may also seek to prioritize the restoration of power to military bases or other facilities critical for national security, the economy, and public health and safety. The November 2019 GridEx exercise highlighted the need for close industry-government coordination on issuing and implementing such emergency measures. In particular, because measures taken on one side of the border are coordinated with neighboring electric systems, close coordination between the governments of Canada, the United States, and

[11] U.S. Department of Energy, *North American Energy Resilience Model*, July 2019, p. 2, https://www.energy.gov/sites/prod/files/2019/07/f65/NAERM_Report_public_version_072219_508.pdf.

Mexico could be valuable for responding to cyberattacks. This paper proposes specific options to bolster such coordination in partnership with the electric industry.

One intriguing but problematic way to do so would be to utilize the North American Aerospace Defense Command (NORAD) for support of infrastructure protection response operations. NORAD provides a globally unique and extraordinarily effective bi-national command for aerospace warning, aerospace control, and maritime warning for North America. Canada's House of Commons Standing Committee on National Defense and other organizations have explored whether NORAD ought to include the cyber domain.[12] A range of U.S. analyses raise the same possibility.

The value proposition for extending NORAD's responsibilities to the cyber realm: just as the United States and Canada can more effectively protect themselves against Russian bombers in a bi-national command than they can individually, so too might they better defend their interconnected electric systems through collaboration within the proven NORAD framework. Along the same line of reasoning, it might also be helpful to invite Mexico to join NORAD and thereby establish a trilateral command structure to help strengthen North American grid security while respecting each nation's sovereignty.

This paper recommends against adding grid cyber defense to NORAD's duties. The Command already has its hands full meeting intensifying threats in the air and maritime domains. With global warming and increased ship travel, the Arctic region has also emerged as a broader strategic priority for NORAD.[13] Moreover, in all three nations, other government organizations already have the responsibility and expertise to help power companies prepare for and respond to attacks

[12] Standing Committee on National Defence, *Canada and the Defence of North America: NORAD and Aerial Readiness*, 42nd Parliament, 1st Session, September 2016, 23-26, https://www.ourcommons.ca/Content/Committee/421/NDDN/Reports/RP8406082/nddnrp02/nddnrp02-e.pdf.

[13] Gen. Terrence O'Shaughnessy, Commander of NORAD and USNORTHCOM, recently told the U.S. Senate Armed Services Committee that the "the strategic value of the Arctic as our first line of defense has reemerged and USNORTHCOM and NORAD are taking active measures to ensure our ability to detect, to track, and defeat potential threats in this region." See: Charles Pope, "Heightened focus on the Arctic brings attention, challenges to the Air Force," U.S. Air Force, March 11, 2019, https://www.af.mil/News/Article-Display/Article/1781707/heightened-focus-on-the-arctic-brings-attention-challenges-to-the-air-force/.

on the grid. Leveraging these existing industry-government partnerships to strengthen North American grid resilience offers the most efficient and effective way forward.

Nevertheless, NORAD offers an unmatched and effective model of *operational unity of effort* between sovereign nations to defend their shared continent. As cyber collaboration goes forward between the grid operators and government agencies of Mexico, Canada, and the United States, NORAD'S bi-national command structure may provide valuable lessons learned to help coordinate cyber response operations across the continent.

This paper lays the foundation for analyzing these options to improve resilience by providing an overview of grid integration in North America. Subsequent sections examine emerging cyber threats and options to collaborate against them, including: 1) development of a trilateral threat assessment; 2) improved government coordination for grid security emergencies; and 3) expanding NORAD's responsibilities to include cyber defense of the grid.

A. The Integration of North American Energy Systems

Infrastructure sectors vary in the degree to which they are integrated across national borders.[14] Water and wastewater systems, for example, remain highly localized and lack the power grid's interconnected structure. But all of these systems depend on electric power to function. Given the foundational importance of grid-provided power to other critical infrastructure sectors, strengthening the cyber resilience of the grid (and of the natural gas pipelines on which power generation increasingly depends) can have far-reaching benefits across North America.

[14] This book uses the definition of "critical infrastructure" provided in *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.

1. The North American Grid: Structure and Emerging Trends[15]

The continent's interconnected electric systems already offer enormous benefits for grid reliability – that is, the sustainment of service even in the face of sudden disturbances (including cyberattacks) or the unanticipated failure of system components.[16] The emerging threat environment also makes it essential to strengthen system resilience. The United States' *National Security Strategy* (2017) defines resilience as "the ability to withstand and recover rapidly from deliberate attacks, accidents, natural disasters, as well as unconventional stresses, shocks, and threats to our economy and democratic system."[17] In the next few years, significant opportunities will emerge to leverage the North American grid's interconnected structure for resilience against such stresses.

Figure 1 depicts the major interconnections that span much of the continent. As noted in the introduction, electrons flowing within these interconnections do not recognize national borders; rather, they flow according to the laws of physics and the controls exercised by grid operators who operate under a shared set of grid reliability standards and other rules.

These interconnections provide for large "power pools" that allow for greater economies of scale. They also strengthen electric system reliability by making more power generation and transmission capabilities available so that operators can move electricity around to compensate for unexpected interruptions in power flows.[18] For example, as new transmission lines increase connectivity between the two nations, electricity exported by Canada or Mexico could help manage instabilities in the United States and mitigate sudden shortfalls in the availability of U.S.-generated power.

---

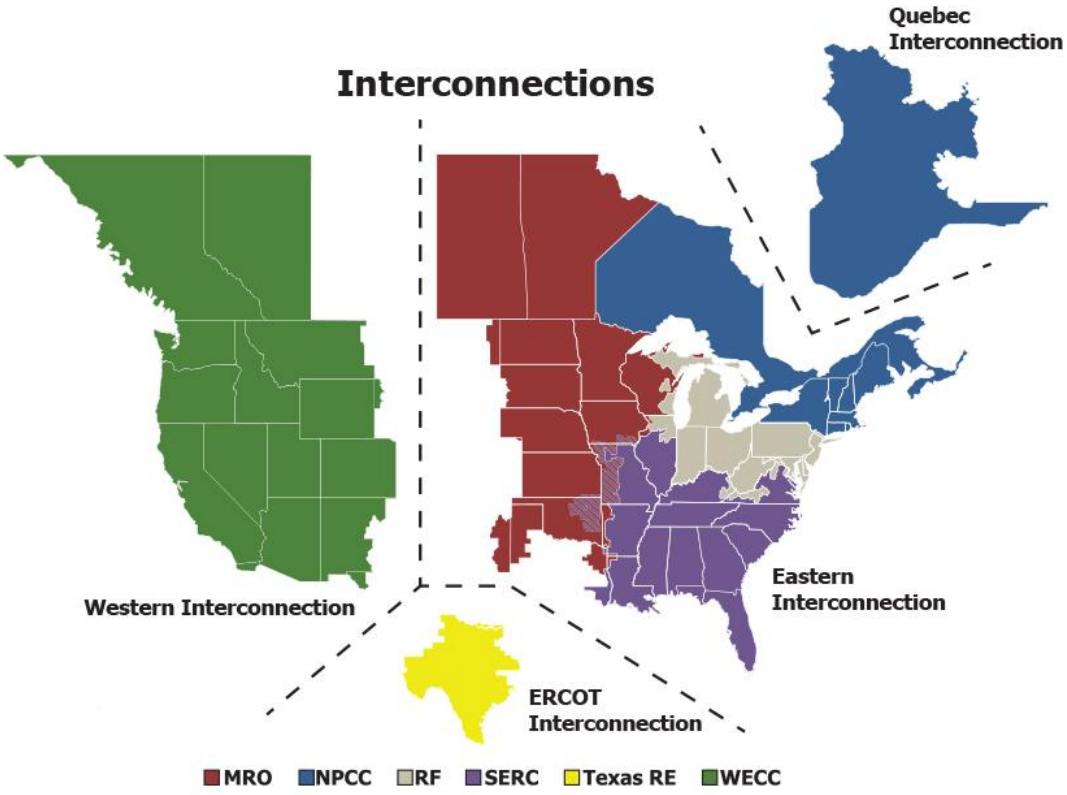
[15] I am extraordinarily grateful for the insights and improvements to this section (and the chapter as a whole) offered by Stuart Brindley and other Canadian and U.S. grid experts.

[16] NERC's official definition of reliable grid operations is "Operating the elements of the [Bulk-Power System] within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements." See: NERC, *Glossary of Terms Used in NERC Reliability Standards*, last updated May 13, 2019, p. 26, https://www.nerc.com/files/glossary_of_terms.pdf.

[17] The U.S. Department of Homeland Security also adopts the *National Security Strategy* definition of resilience See: Donald J. Trump, *National Security Strategy of the United States of America*, December 2017, p. 14, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf; "Resilience," Department of Homeland Security (DHS), last updated February 25, 2019, https://www.dhs.gov/topic/resilience.

[18] FERC, *Reliability Primer*, p. 10.

Figure 1. North American Interconnections[19]



The U.S. and Canadian grids are linked by over 35 major transmission lines from the Pacific to the Atlantic Ocean.[20] The resulting power flows have created a deeply integrated network of north-south electric infrastructure and synchronized cross-border operations.[21] The two countries are also pursuing further connectivity. New York and Massachusetts are seeking significant increases

[19] Source: "Interconnections," NERC, July 2019, https://www.nerc.com/AboutNERC/keyplayers/PublishingImages/NERC_Interconnections_01JUL19.jpg. While not depicted in the image, Southern California and a portion of Mexico's Baja California have synchronous interconnections. Along the Mexico–Texas border, asynchronous interconnections also exist between the Electric Reliability Council of Texas (ERCOT) and Mexican utilities. See: "Increasing Electricity Cooperation in North America," Department of Energy, January 11, 2017, https://www.energy.gov/policy/articles/increasing-electricity-cooperation-north-america.

[20] Doug Vine (Center for Climate and Energy Solutions), *Interconnected: Canadian and U.S. Electricity*, March 2017, p. 1, https://www.c2es.org/site/assets/uploads/2017/05/canada-interconnected.pdf.

[21] Department of Energy (DOE), *Quadrennial Energy Review – Transforming the Nation's Electricity System: Second Installment of the QER*, January 2017, p. 6-6, https://www.energy.gov/sites/prod/files/2017/02/f34/Quadrennial%20Energy%20Review--Second%20Installment%20%28Full%20Report%29.pdf.

in Canadian hydropower to help achieve their clean energy goals.[22] Several new cross-border transmission lines are also under development, though many of them face permitting challenges. The Lake Erie Connector is a one-thousand-megawatt high-voltage, direct current line expected to link Ontario's Independent Electricity System Operator with PJM in 2024.[23] The Champlain Hudson Power Express from Quebec to New York City is expected to go into service in 2025, with still other projects in various phases of development in New England and the Midwest.[24]

Coordination between the Canadian and U.S. governments on energy resilience initiatives has been advancing as well. The *Joint United States-Canada Electric Grid Security and Resilience Strategy* (December 2016) is designed to help strengthen the security and resilience of the U.S. and Canadian grids from cyberattacks and other hazards.[25] In particular, the *Strategy* provides a policy framework for further improving integration and building coordination and information sharing mechanisms.

The integration of electric infrastructure between the United States and Mexico is much less extensive. Despite electricity trade between the two countries that dates back to 1905, there are few transmission connections between them. Indeed, the only synchronous connections exist at the border between Mexico and the state of California.[26] Limited electricity trade also occurs across asynchronous interconnections between the Electric Reliability Council of Texas (ERCOT) and Mexican utilities, which provides a prime example of the benefits of integration: these

[22] New York City Mayor Bill de Blasio's long-term strategic plan, released in April 2019, proposes that the city, in partnership with New York State "will pursue an investment in new transmission to access large-scale Canadian hydropower." See: Government of New York City, *OneNYC 2050: Building a Strong and Fair City*, A Livable Climate (Volume 7 of 9), April 2019, p. 14, https://onenyc.cityofnewyork.us/wp-content/uploads/2019/05/OneNYC-2050-A-Livable-Climate.pdf. See also: Geoffrey Morgan, "How Canada's other major energy export could light up New England states," *Financial Post*, April 16, 2019, https://business.financialpost.com/commodities/energy/how-canadas-other-major-energy-export-could-light-up-new-england-states.

[23] "ITC Lake Erie Connection Project," ITC, 2020, https://www.itclakeerieconnector.com.

[24] Danielle Muoio and Joe Anuta, "New York City may finance power line in push for Quebec hydro," Politico, October 25, 2019, https://www.politico.com/states/new-york/city-hall/story/2019/10/24/new-york-city-may-finance-power-line-in-push-for-quebec-hydro-1225983; "About the Project," New England Clean Energy Connect, n.d., https://www.necleanenergyconnect.org/project-overview; "Atlantic Link," Emera, 2020, https://www.atlanticlink.com/; and "Delivering Clean Energy to Minnesota," Great Northern Transmission Line, 2020, https://greatnortherntransmissionline.com/index.html.

[25] Governments of the United States and Canada, *Joint United States-Canada Electric Grid Security and Resilience Strategy*, December 2016, p. 1.

[26] GAO, *NORTH AMERICAN ENERGY INTEGRATION*, p. 5.

interconnections are primarily used to supplement constrained electricity supplies and maintain reliability in emergencies.[27]

Nevertheless, agreements are in place that could facilitate greater integration in the future. In 2017, former Secretaries of Energy Ernest Moniz (U.S.) and Pedro Joaquin Coldwell (Mexico) agreed to non-binding pledges to increase this connectivity in ways that would strengthen reliability on both sides of the border.[28] 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) in 2017 to formalize collaboration on a number of 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."[29] Moreover, DOE's *Quadrennial Energy Review* (QER) specifically recommends increasing bilateral cooperation between the United States and Mexico on electric reliability as the latter expands their domestic and international electricity transmission systems, in addition to broader North American efforts.[30]

Since the 2018 election of President Andrés Manuel López Obrador, Mexican grid policy initiatives have focused more on internal issues (including energy markets) than on integration with systems in the United States.[31] However, structural challenges could slow efforts to increase

[27] Paul W. Parfomak et al., (Congressional Research Service (CRS)), *Cross-Border Energy Trade in North America: Present and Potential*, January 24, 2017, p. 33, https://fas.org/sgp/crs/misc/R44747.pdf. There is also a proposed transmission project that would create an asynchronous tie between grid infrastructure in Arizona and in Sonora, Mexico. See: FERC, *Proposed and Final Order*, 164 FERC ¶ 61,056 (Docket No. TX18-1-000), p. 2.

[28] "Increasing Electricity Cooperation in North America," *DOE*, January 11, 2017, https://www.energy.gov/policy/articles/increasing-electricity-cooperation-north-america; "U.S. Energy Secretary and Mexico Energy Minister Sign Bilateral Principles to Promote Electricity Reliability of Interconnected Power Systems," *DOE*, January 9, 2017, https://www.energy.gov/articles/us-energy-secretary-and-mexico-energy-minister-sign-bilateral-principles-promote.

[29] *Memorandum of Understanding between CRE, CENACE and NERC*, March 8, 2017, https://www.nerc.com/AboutNERC/keyplayers/Documents/MOU%20Clean%20NERC_CRE_CENACE_EN%20FINAL.pdf.

[30] DOE, *QER*, p. 7-28.

[31] On recent changes to the structure of Mexican electricity markets, see: Anthony Harrup and Robbie Whelan, "Mexican Government Moves to Tighten Grip on Electricity Market," Wall Street Journal, May 17, 2020, https://www.wsj.com/articles/mexican-government-moves-to-tighten-grip-on-electricity-market-11589752754.

U.S.-Mexico grid integration, including repeated power shortages and major shortfalls in the functionality of the Mexican grid.[32] The prospect for future electric integration and trade with Mexico will depend on Mexico's ability to expand domestic transmission systems, in line with their overall economic growth and energy demand, and synchronize them with neighboring U.S. interconnections.[33] But these potential constraints should not prevent consensus-building on opportunities to strengthen cross-border resilience. On the contrary: addressing security issues now can help facilitate wider system integration if the Mexican government decides to seek expanded links to ERCOT and the Western Interconnection.

Trilateral initiatives provide a broader framework to support such consensus-building. At the North American Leaders Summit in June 2016, the heads of Mexico, Canada and the United States committed to "deepened electric reliability cooperation to strengthen the security and resilience of an increasingly integrated North American electricity grid."[34] In November 2017, then-Secretary of Energy Rick Perry and his Canadian and Mexican counterparts also held a trilateral meeting in which they discussed a range of topics, including "the security, affordability, resiliency, and reliability of our shared energy systems, and collaboration in areas such as critical infrastructure protection, cyber security, [and] system modernization."[35] DOE and its Mexican and Canadian counterparts have also resumed efforts to develop a North American Energy Strategy, after disagreements on potential scope derailed discussions in 2017.[36]

DOE has proposed multiple lines of effort to advance North American energy integration: (1) high-level engagement through bilateral and trilateral coordination; (2) both cooperative and independent analysis of challenges and opportunities for integration, including system modeling, by working groups and project teams; and (3) policy-level actions, primarily executed

[32] DOE, *QER*, p. 6-13.

[33] CRS), *Cross-Border Energy Trade in North America*, p. 36.

[34] DOE, *QER*, p. 7-28.

[35] *North American Energy Ministerial Joint Summary*, November 15, 2017, p. 1, https://www.energy.gov/sites/prod/files/2017/11/f46/North%20American%20Energy%20Ministerial%20Joint%20Summary.pdf,

[36] GAO, *NORTH AMERICAN ENERGY INTEGRATION*, p. 10.

domestically, to support international initiatives.[37] A number of new cross-border infrastructure projects – including transmission lines and oil and natural gas (ONG) pipelines – are also either proposed or underway, paving the way for increased trade and integration, though their completion may face regulatory, political, and legal challenges.[38] In addition, the U.S. Department of State, the U.S. Agency for International Development, and other U.S. agencies have been assisting Mexico on energy integration and related issues.[39]

2. Gas-Electric System Interdependencies and Integration Trends

In many portions of North America, power generation is increasingly fueled by natural gas. To assess the overall resilience of the continent's electric interconnections against emerging threats, it is therefore also necessary to account for the structure of the natural gas systems on which the grid heavily relies. Indeed, significant interruptions to the flow of natural gas could jeopardize electric reliability.[40]

Natural gas flows between the United States and Canada and the United States and Mexico are trending in different directions. Cross-border natural gas pipeline capacity between the United States and Canada has remained fairly stagnant in recent years, though U.S. shale gas production has begun to increase U.S. gas exports to Canada while reducing imports.[41] Conversely, cross-border natural gas pipeline capacity between the United States and Mexico has grown at an increasing rate since 2011.[42] Moreover, Mexico is building a significant amount of pipelines domestically to transport natural gas to electric generators, which accounts for 60 percent of the country's electricity.[43]

---

[37] DOE, *QER*, p. 6-16.

[38] CRS, *Cross-Border Energy Trade in North America*, p. *i*.

[39] GAO, *NORTH AMERICAN ENERGY INTEGRATION*, p. 16.

[40] NERC, *Special Reliability Assessment: Potential Bulk Power System Impacts Due to Severe Disruptions on the Natural Gas System*, November 2017, p. *vii*.

[41] CRS, *Cross-Border Energy Trade in North America*, p. 22.

[42] CRS, *Cross-Border Energy Trade in North America*, p. 21.

[43] Jude Clemente, "NAFTA Deal To Bolster U.S.-Mexican Natural Gas Trade," *Forbes*, August 17, 2018, https://www.forbes.com/sites/judeclemente/2018/08/17/nafta-deal-to-bolster-u-s-mexican-natural-gas-trade/#2957679963fa.

Some utilities hedge against risks of natural gas disruption by installing "dual-fuel" generators, which have the ability to operate on secondary fuels if natural gas is not available. These dual-fuel generators can operate on diesel, no. 2 fuel oil, or other secondary sources of fuel to sustain their generating capacity.[44] However, dual-fuel generators cannot fully insulate electric systems from the effects of natural gas disruptions. On-site storage capacity for secondary fuel is limited, few dual-fuel generating units will have sufficient on-site storage of secondary fuels to continue operations until normal gas service is restored, and major outages would create enormous demand for resupplying these secondary fuels that outweigh the available supply.

As with electric systems, substantial cooperation exists between Mexico, Canada, and the United States on natural gas pipeline issues. For example, the U.S. Department of Transportation has been collaborating with Mexican and Canadian agencies on strategies to improve the safety of cross-border pipelines. [45] NERC and its North American members have has also developed recommendations to mitigate the risks posed by gas-electric interdependencies.[46] As cyber threats to both the electricity and ONG subsectors intensify, such collaborative efforts will need to grow as well.

3. Managing the Risks of Expanding Integration

Energy sector integration across North America benefits all three countries by expanding energy markets, attracting private investment, lowering capital costs and energy costs for consumers, and ultimately allowing for a more diverse mix of energy resources that increases energy security.[47]

However, the connectivity of North American infrastructure also creates risks of cross-border failures. A prime example is the 2003 blackout which started in Ohio and resulted in power outages

---

[44] Electric Infrastructure Security (EIS) Council, *E-PRO Handbook II: Volume 1 – Fuel* (Washington, D.C.: EIS Council, 2016), p. 24, https://www.eiscouncil.org/App_Data/Upload/149e7a61-5d8e-4af3-bdbf-68dce1b832b0.pdf.

[45] GAO, *NORTH AMERICAN ENERGY INTEGRATION*, p. 17.

[46] NERC, *Special Reliability Assessment*, p. *ix-x*.

[47] GAO, *NORTH AMERICAN ENERGY INTEGRATION*, p. 5; Andrew Stanley (Center for Strategic and International Studies), *Mapping the U.S.-Canada Energy Relationship*, May 2018, p. 1, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180507_Stanley_U.S.CanadaEnergy.pdf?fBwWhKl0BBuNMOeIRSolkNQ89Iij7iaz.

for millions of customers in the United States and Canada.[48] As outlined above, interconnections between U.S. and Canadian power systems have 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."[49]

NERC and its partners have made enormous progress in understanding and mitigating the risks of such cascading failures. Increased interconnectivity provides greater flexibility and capacity to respond to and support emergency situations. But cyberattacks can increase the risk of cross-border effects far beyond those created by natural hazards. In contrast to Mother Nature, we should expect adversaries to strategically target grid infrastructure and control systems to inflict blackouts of the greatest possible geographic scope and maximize disruption of electricity-dependent ports, military bases, and other critical facilities across the four interconnections.

B. Emerging Cyber Threats to the Grid and Natural Gas Systems

When President Trump declared in May 2020 that the threat to the U.S. grid constitutes a national emergency, his declaration focused on only one of many security challenges confronting energy infrastructure. The President warned that that grid equipment produced by foreign adversaries might help them create and exploit vulnerabilities in the U.S. electric system, "with potentially catastrophic effects."[50] That threat is indeed severe. However, potential adversaries are also developing other means to attack North America's electric interconnections and the natural gas pipelines that fuel power generation. These threats require accelerated efforts to strengthen energy infrastructure resilience within and between Mexico, Canada, and the United States.

Countering these threats will also require new forms of collaboration beyond those already established to deal with the cross-border effects of hurricanes and other natural hazards. Protecting

[48] North American Electric Reliability Council, *Technical Analysis of the August 14, 2003, Blackout: What Happened, Why, and What Did We Learn?*, July 13, 2004, p. 1.

[49] Governments of the U.S. and Canada, *Joint Electric Grid Security and Resilience Strategy*, December 2016, p. 10.

[50] Trump, *Executive Order on Securing the United States Bulk-Power System*.

grid networks and equipment against sophisticated malware will require very different investments than, for example, placing power lines underground or resilience measures against storm effects. Cyber resilience also requires intensive, carefully-secured information sharing on malware signatures, emerging attack vectors, and other threat data between industry and government agencies – potentially on a continent-wide basis.

In addition, emergency response and power restoration operations will require cyber-specific plans and capabilities. In contrast to hazards from Mother Nature, adversaries can implant difficult-to-detect malware in energy system networks and equipment. Advanced persistent threats (APTs) can also enable follow-on attacks and sustained campaigns to lengthen the duration of blackouts. Moreover, unlike natural disasters, adversaries can target especially critical assets to magnify the effects of their attacks and disrupt power restoration operations to lengthen outages. Most importantly, while system managers have frequent opportunities to employ their emergency response capabilities and coordination mechanisms against storm or wildfire-induced blackouts, they have no equivalent experience against cyber-induced outages. Instead, system operators and their government partners must draw lessons learned from attacks on other countries and prepare against attack vectors that are just now emerging. Those industry-government efforts should include measures to account for the risk that post-cyberattack restoration operations would need to go forward in a pandemic environment.

1. Ukraine and Beyond: Implications for North American Electric Systems

Cyberattacks on the Ukrainian power grid that caused widespread blackouts in 2015 and 2016 provide a "real world" starting point to anticipate how adversaries might strike the North American grid. In 2015, Russian hackers hijacked the grid's operating systems to disconnect critical substations, creating brief but very wide outages. Attackers were also able to permanently disable (or "brick") operating system components and communications devices.[51] The 2016 cyberattack

[51] "Bricking" a piece of equipment means rendering it unusable, often due to firmware that is damaged beyond repair. See "Bricking," *Techopedia*, n.d.a., https://www.techopedia.com/definition/24221/bricking. See also: SANS Industrial Control Systems (SANS ICS) and Electricity Information Sharing and Analysis Center (E-ISAC), *Analysis of the Cyber Attack on the Ukrainian Power Grid*, March 18, 2016, p. 2, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

displayed more sophistication. After mapping the grid's operating systems, attackers used the system's industrial control system (ICS) protocols to open circuit breakers, creating blackouts.[52] The malware was unusually difficult to detect, and included a wiper module that could brick grid control system components on a large scale.[53] Attackers also had the ability to deny or corrupt situational awareness data, making the grid extremely prone to cascading failures.[54] In addition, recent analysis of the attack has revealed that these immediate effects were merely intended to be "the precursors for an attempt at a more ambitious attack." Perpetrators intended to cause blackouts on a much wider scale by disabling the protective relay devices in places to stop power failures from cascading across the grid.[55] That broader attack failed. However, these cyberattacks moved cyberwarfare against electric systems from theory to limited, but unprecedented, practice.

Potential adversaries are testing additional ways to attack the grid and other critical infrastructure. The ongoing Dragonfly 2.0 campaign, conducted by cyber attackers within the Russian government, enables them to use utility vendors and other trusted third parties to conduct attacks on targeted systems.[56] 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.[57] The XENOTIME hacking group responsible for these

[52] "Alert (ICS-ALERT-17-206-01): CRASHOVERRIDE Malware," Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), July 25, 2017, https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-206-01; "Alert (TA17-163A): CrashOverride Malware," US Computer Emergency Readiness Team (US-CERT), June 12, 2017, https://www.us-cert.gov/ncas/alerts/TA17-163A; Dragos, Inc, *CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations*, June 13, 2017, p. 8, available at https://dragos.com/blog/crashoverride/CrashOverride-01.pdf; and Defense Science Board (DSB), *Task Force on Cyber Deterrence* (Washington, DC: DOD, February 2017), p. 4, https://www.acq.osd.mil/dsb/reports/2010s/DSB-cyberDeterrenceReport_02-28-17_Final.pdf.

[53] "Alert (TA17-163A): CrashOverride Malware," US-CERT.

[54] Dragos, Inc., *CRASHOVERRIDE*, p. 24.

[55] Joe Slowik, *CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack*, Hanover, MD: Dragos, Inc., September 2019, p. 1, https://dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf.

[56] "Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," US-CERT, March 15, 2018, https://www.us-cert.gov/ncas/alerts/TA18-074A.

[57] Andy Greenberg, "Unprecedented Malware Targets Industrial Safety Systems in the Middle East," *WIRED*, December 14, 2017, https://www.wired.com/story/triton-malware-targets-industrial-safety-systems-in-the-middle-east/.

attacks continues to target U.S. electric and ONG networks, and is considered the "most dangerous threat to ICS" due to their proven ability to carry out destructive attacks.[58]

Yet, sophisticated as these attacks are, they do not reflect the true scale and severity of the cyber threat confronting North American energy systems. Russia, China, North Korea, and other potential adversaries have powerful incentives to hold their most destructive cyber weapons in reserve; doing so helps hobble efforts at building protections against such weapons. Recent studies by the U.S. Department of Energy (DOE), 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, including:

- *Supply Chain Corruption.* As noted in the Trump Administration's Executive Order on the U.S. grid, foreign adversaries may seek to implant malware in critical grid components to help conduct catastrophic attacks. Infrastructure owners and operators often find it difficult to ensure the integrity of their supply chains.[59] Software, firmware, hardware, or network services are all vulnerable to supply chain compromise, potentially enabling adversaries to inject destructive malware and/or gain access to sensitive components and data in utility systems. This is particularly concerning for industry-standard grid components used by many utilities across the United States, Mexico, and Canada, creating the potential for threat actors to simultaneously trigger failures across all three North American interconnections.

- *Attacks on Protection Systems.* Attacks on systems that safeguard the integrity of the grid and protect key components from power surges are potentially catastrophic. Protective relays that isolate faults to protect equipment and prevent cascading power failures are prime targets. These relays were once electromechanical; now, much of the grid relies on

[58] "Threat Proliferation in ICS Cybersecurity: XENOTIME Now Targeting Electric Sector, in Addition to Oil and Gas," Dragos, Inc., June 14, 2019, https://dragos.com/blog/industry-news/threat-proliferation-in-ics-cybersecurity-xenotime-now-targeting-electric-sector-in-addition-to-oil-and-gas/.

[59] Idaho National Laboratory, *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector*, August 2016, p. 20, https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf.

microprocessor-based relays that adversaries can target with cyberattacks.[60] Attacks that take these relays offline will not cause power outages on their own. However, without relay protection in place and in the event of an unexpected loss of generation or transmission capacity, the system is vulnerable to power surges that could cause equipment damage and cascading failures until relays can be manually reset.[61]

- *Intentional Mis-Operation of Other Grid Components*. The 2007 "Aurora" test conducted at the Idaho National Laboratory provided an early demonstration of the ability to remotely operate and physically damage power generators.[62] Since then, efforts have been underway to remediate the vulnerabilities that Aurora demonstrated. While those efforts must continue, new attack vectors are emerging that warrant further investigation:

    - Operator Control Systems. Adversaries can cause severe outages by compromising operator workstations, using them to send malicious commands to grid control systems. Adversaries have the ability to gain access to devices that utility operators use to control grid components, and they may be able to do so without any visible indication to the operator.[63] Adversaries may seek to attack far more U.S. substations than in the 2015 human machine interface (HMI)-based attacks on Ukraine, and may also specially design those attacks to create cascading failures.

    - Industrial Control Protocols for Grid Operation. Communication protocols native to grid components are the backbone of ICS operations, communicating actions to those components to control the flow of power. U.S. adversaries may use these

[60] Chris Sistrunk, "ICS Cross-Industry Learning: Cyber-Attacks on Electric Transmission and Distribution (Part One)," SANS Industrial Control Systems, January 8, 2016, https://ics.sans.org/blog/2016/01/08/ics-cross-industry-learning-cyber-attacks-on-a-an-electric-transmission-and-distribution-part-one.

[61] Anton Cherepanov (ESET), *Win32/Industroyer: A new threat for industrial control systems*, June 12, 2017, p. 15, https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf; "Alert (TA17-163A): CrashOverride Malware," US-CERT.

[62] NERC, *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System*, June 2010, p. 32, https://www.energy.gov/sites/prod/files/High-Impact%20Low-Frequency%20Event%20Risk%20to%20the%20North%20American%20Bulk%20Power%20System%20-%202010.pdf.

[63] Tim Conway, "Pictures and Theories May Help, but Data Will Set Us Free," SANS Industrial Control Systems, December 21, 2016, https://ics.sans.org/blog/2016/12/21/pictures-and-theories-may-help-but-data-will-set-us-free.

communication protocols to directly induce malicious changes, and do so with greater scale and sophistication than occurred in the 2016 Ukraine attack. Because these protocols were designed decades ago without any considerations for cybersecurity, attackers do not necessarily have to find 'vulnerabilities' within them; they simply need to embed the protocol language into the malware to cause "cascading failures and … serious damage to equipment."[64] This type of cyberattack presents significant challenges because many utilities lack the situational awareness and monitoring capabilities to detect attacks targeted deep in control system protocol stacks.

- *Load Manipulation.* A new threat vector has emerged in part due to the modernization of the grid. While threat assessments often focus on generation and transmission assets, power flows from these potential targets represent only half of the load-generation balance required for grid stability. A drastic change in load could also lead to instability and power swings, causing outages and equipment damage. Digital smart meters (also known as advanced metering infrastructure) are increasingly replacing their analog predecessors to improve accuracy and energy efficiency. Some meters have the ability to be switched off remotely.[65] If adversaries gain access to large numbers of these smart meters, they could potentially cause "a widespread blackout by switching smart meter loads on and off repeatedly."[66] While DOE emphasizes the importance of cybersecurity for advanced metering infrastructure (AMI), recent studies suggest advanced cyberattacks against AMI remain "a clear and present danger."[67]

---

[64] Anton Cherepanov and Robert Lipovsky, "Industroyer: Biggest threat to industrial control systems since Stuxnet," ESET Blog: WeLiveSecurity, June 12, 2017, https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/.

[65] DOE, *Advanced Metering Infrastructure and Customer Systems: Results from the Smart Grid Investment Grant Program*, September 2016, p. 20, https://www.energy.gov/sites/prod/files/2016/12/f34/AMI%20Summary%20Report_09-26-16.pdf.

[66] Anca Gurzu, "Hackers threaten smart power grids," *POLITICO*, January 11, 2017, http://www.politico.eu/article/smart-grids-and-meters-raise-hacking-risks/.

[67] DOE, *Advanced Metering Infrastructure and Customer Systems*, p. 69; Aaron Hansen, Jason Staggs and Sujeet Shenoi, "Security analysis of an advanced metering infrastructure," *International Journal of Critical Infrastructure Protection*, Vol. 18. (September 2017): p. 3.

- *Attacks on Grid State Estimation.* Adversaries could significantly amplify the effects of a cyberattack on critical electric infrastructure by disabling or corrupting grid state estimation capabilities. Grid operation depends on state estimators for real-time assessments of system conditions and subsequent contingency analysis based on those estimations. System-generated alerts based on these state estimates are "the fundamental means by which system operators identify events on the power system that need their attention."[68] As such, failures of or attacks on state estimators can have devastating effects on grid operation. For example, a malfunction in a state estimator system was a significant contributor to power failures across the northeastern United States and Canada in the August 2003 blackout. Grid operators are developing fallback systems to manage power flows in the absence or compromise of state estimation inputs. Nevertheless, adversarial corruption of state estimator data during a cyberattack remains a threat, as it could delay corrective actions or cause incorrect operator responses. Successful attacks on state estimators could initially obscure the effects or existence of a cyberattack, contributing to multi-region cascading failures.

- *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. DDoS attacks entail sending such high volumes of web traffic at a target that it is unable to function, rendering key resources unavailable.[69] 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.[70] As such, networked system control components may be vulnerable to DDoS attacks, and

[68] U.S.-Canada Power System Outage Task Force, *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, April 2004, p. 52, https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf.

[69] DHS, *Distributed Denial of Service Defense (DDoSD)*, November 2016, p. 1, https://www.dhs.gov/sites/default/files/publications/FactSheet%20DDoSD%20FINAL%20508%20OCC%20Cleared.pdf.

[70] DOE, *QER*, p. 7-3.

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 may attempt to debilitate electric utilities by using data wiper modules to destroy large amounts of data or brick targeted systems.[71] Historically, wiper module attacks have been limited to wiping computers and other information technology devices, without targeting industrial control systems or other operational technology components. The 2012 attack on Saudi Aramco, for example, wiped 30,000 Windows-based computers, but did not affect industrial control systems.[72] However, more recent attacks, including the CrashOverride malware that Russia employed against Ukraine's grid in 2016, have included wiper modules that target control systems and networks.[73] 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.[74] Moreover, because electric utilities anticipate threats to SCADA systems, they are increasingly planning for the loss of SCADA functionality and upgrading manual grid operation capabilities in the event of control systems degradation or failure.[75] 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.

[71] ICS-CERT, *Destructive Malware*, March 2017, p. 1, https://ics-cert.us-cert.gov/sites/default/files/documents/Destructive_Malware_White_Paper_S508C.pdf.

[72] Jim Finkle, "Exclusive: Insiders suspected in Saudi cyber attack," Reuters, September 7, 2012, https://uk.reuters.com/article/us-saudi-aramco-hack-idUKBRE8860CR20120907.

[73] "Alert (TA17-163A): CrashOverride Malware," US-CERT.

[74] Michael J. Assante, "Confirmation of a Coordinated Attack on the Ukrainian Power Grid," SANS ICS, January 9, 2016, https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid.

[75] Federal Energy Regulatory Commission (FERC) and NERC, *Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans – Further Joint Study: Planning Restoration Absent SCADA or EMS (PRASE)*, June 2017, p. 4, https://www.ferc.gov/legal/staff-reports/2017/06-09-17-FERC-NERC-Report.pdf.

- *Ransomware*. Ransomware attacks are an increasingly 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.[76] This malware often exploits network vulnerabilities and moves laterally, infecting as many endpoints as possible.[77] Once infected, the only way to potentially 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. While 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 (PLCs) in a simulated water plant; the researchers warned that these tactics are the "next logical step" for ransomware attacks.[78] Such an advanced form of ransomware attack has yet to occur. However, one cybersecurity firm recently identified ICS-targeting ransomware which – while fairly limited in functionality – represents "a relatively new and deeply concerning evolution in ICS-targeting malware."[79] As adversaries continue to improve their offensive capabilities, the use of ransomware to disrupt utility operations and restoration efforts present a growing threat. Ransomware attacks against local governments can also inadvertently disrupt operations of municipally owned electric systems.[80]

---

[76] Alert (TA16-091A): Ransomware and Recent Variants," US-CERT, last updated September 29, 2016, https://www.us-cert.gov/ncas/alerts/TA16-091A.

[77] "Alert (ICS ALERT-17-181-01C) Petya Malware Variant (Update C)," ICS-CERT, last revised July 10, 2017, https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-181-01C.

[78] John Toon, "Simulated Ransomware Attack Shows Vulnerability of Industrial Controls," Georgia Tech, February 13, 2017, http://www.news.gatech.edu/2017/02/13/simulated-ransomware-attack-shows-vulnerability-industrial-controls.

[79] "EKANS Ransomware and ICS Operations," Dragos, February 3, 2020, https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/.

[80] Paul Ciampoli, "More than 20 Texas Entities Hit with Ransomware Attack, American Public Power Association, August 19, 2019, https://www.publicpower.org/periodical/article/more-20-texas-entities-hit-with-ransomware-attack.

- *Artificial Intelligence.* Over the longer term, adversaries may use Artificial Intelligence (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 North American 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.[81] 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.[82] 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 attack vectors pose intensifying threats to integrated North American energy infrastructure. Sharing information about them – and including industry in both gathering and receiving such data – will be essential to manage the risks of cross-border failures and to strengthen grid resilience for the mutual benefit of Mexico, Canada, and the United States.

2. Expecting the Unexpected: COVID-19 and Beyond

No pandemic, regardless of severity, is likely to tempt China or other adversaries to launch an "opportunistic" cyberattack on the continent's interconnections. As long as the United States is able to maintain a credible deterrent – that is, convince adversaries that disrupting the grid would prompt a devastating and unacceptably costly response – only the most severe regional

[81] Greg Allen and Daniel Chan (Belfer Center for Science and International Affairs), *Artificial Intelligence and National Security*, July 2017, p. 24, https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf.

[82] Elsa B. Kania (Center for a New American Security), *Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power*, November 2017, p. 4, https://s3.amazonaws.com/files.cnas.org/documents/Battlefield-Singularity-November-2017.pdf?mtime=20171129235804.

confrontations or other geopolitical crises could conceivably create the conditions for such an attack.

Nevertheless, COVID-19 has revealed new challenges for cyber preparedness. State and non-state actors have drastically increased their efforts to penetrate critical infrastructure networks across multiple infrastructure sectors. Their targets include the North American power grid. NERC reported in June 2020 that "Opportunistic actors are attempting to find and exploit new vulnerabilities that arise as entities shift work processes and locations to maintain business continuity."[83] NERC's Electricity Infrastructure Sharing and Analysis Center (E-ISAC) is sharing information on specific threats, including attacks on conferencing and remote access infrastructure, disinformation, and spear phishing campaigns attempting to harvest credentials and other information.[84] Moreover, these cyber-specific threats are rising at the same time that workforce disruptions and supply chain interruptions present new challenges to grid operations.

The ESCC and other industry-led organizations have provided detailed recommendations to utilities on how to sustain reliable operations in the face of the pandemic's effects.[85] Power companies are also strengthening their preparedness to conduct post-hurricane power restoration operations despite these COVID-related challenges.[86] Going forward, these companies and their partners should conduct equivalent efforts to prepare for post-cyberattack power restoration, with plans to mitigate additional risks created by the need for remote work in pandemic environments, including a dependence on potentially vulnerable internet-based communications, public switched phone networks, and cell systems. The Cyberspace Solarium Commission highlighted a number of these challenges and offered recommendations on how industry and government can build

[83] NERC, *2020 Summer Reliability Assessment*, June 2020, p. 13, https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_SRA_2020.pdf.

[84] NERC, *2020 Summer Reliability Assessment*, p. 13.

[85] Electricity Subsector Coordinating Council, "Assessing and Mitigating the Novel Coronavirus (COVID-19), June 26, 2020, https://www.electricitysubsector.org/-/media/Files/ESCC/Documents/ESCC_COVID_Resource_Guide_v2-03242020.ashx?la=en&hash=D3732CBFB46827AA0331277E8D5CBE0CC4DFC3BF.

[86] "Duke Energy prepares for hurricane season during COVID-19 pandemic," Duke Energy, May 29, 2020, https://news.duke-energy.com/releases/duke-energy-prepares-for-hurricane-season-during-covid-19-pandemic; Robert Walton, "When storms collide: Utilities' new approach to hurricane restoration in the age of COVID-19," Utility Dive, June 4, 2020, https://www.utilitydive.com/news/when-storms-collide-utilities-new-approach-to-hurricane-restoration-in-th/578976/.

resilience against cyberattacks that occur during pandemics.[87] The development of plans and capabilities against such opportunistic attacks should also seek to avoid "failures of imagination." Anticipating how adversaries may attack and collaborating on emergency threats and opportunities to defeat them constitutes a core challenge for defending North America's interconnections.

C. Developing a Trilateral Threat Assessment

As noted earlier in this paper, strong foundations already exist to improve continent-wide protections against cyberattacks. Information sharing exemplifies how far collaboration has come, but also how much progress will be necessary against the intensifying threat. The E-ISAC will be crucial for making such progress. The Center has forged close working relationships between industry, DOE, and other federal agencies and is partnering with those agencies to create specialized initiatives such as the Cybersecurity Risk Information Sharing Program, which provides bi-directional sharing of unclassified and classified threat information among energy sector stakeholders.[88]

The E-ISAC also enables cross-border information sharing. The Center supports Canadian grid owners and operators and collaborates with Natural Resources Canada, Public Safety Canada, and the Canadian Centre for Cyber Security to provide cross-border outreach and collaboration.[89] Extensive government-to-government information sharing also exists between both nations' broader intelligence and national security communities. As "Five Eyes" intelligence partners (along with the UK, Australia, and New Zealand), and with the extraordinarily close defense relationship reflected in the bi-national command structure of NORAD, Canada and the United

[87] Cyberspace Solarium Commission, *Cybersecurity Lessons from the Pandemic*, May 2020, https://www.solarium.gov/public-communications/pandemic-white-paper.

[88] DOE, *Cybersecurity Risk Information Sharing Program (CRISP)*, September 2018, p. 1, https://www.energy.gov/sites/prod/files/2018/09/f55/CRISP%20Fact%20Sheet.pdf.

[89] James B. Robb, "Status and Outlook for Cybersecurity Efforts in the Energy Industry," Testimony Before the U.S. Senate Committee on Energy and Natural Resources, February 14, 2019, p. 1, https://www.energy.senate.gov/public/index.cfm/files/serve?File_id=9849D816-4D29-42E7-B535-DCCE1CAD2701.

States can build on many decades of experience to strengthen their common assessment of threats to energy infrastructure.[90]

Information sharing with Mexico has been far less extensive. However, a precedent does exist for developing trilateral threat assessments. In March 2012, at the inaugural Trilateral Meeting of North American Defense Ministers in Ottawa, the three nations agreed to develop a joint assessment of emerging threats and strengthen cooperation accordingly. Then Canadian Minister of National Defence, Peter MacKay, noted that "Canada, the United States and Mexico share common challenges and concerns when it comes to the defence and security of North America."[91] To help address those shared challenges, the representatives of Canada, Mexico, and the United States agreed to "develop a joint trilateral defence threat assessment for North America to deepen our common understanding of the threats and challenges we face."[92]

The United States, Mexico, and Canada should consider widening the trilateral threat assessment project beyond traditional defense agencies to include the civilian agencies responsible for the energy sector and cybersecurity. Including power companies in that expanded effort and leveraging the work of the E-ISAC and other appropriate organizations is essential as well. A trilateral threat assessment for the grid would be most valuable if it focused on the attack vectors that could create outages in all three nations, especially common failure modes that adversaries may seek to exploit.

An integrated assessment should also account for the modernization of energy sector infrastructure and the growing importance of cross-border energy flows for grid reliability. Recent amendments to the U.S. *Federal Power Act* (FPA) lay the foundation for additional integration between the United States, Mexico, and Canada on cross-border grid resilience. The FPA states that the Federal Energy Regulatory Commission (FERC) and the Secretary of Energy "shall, in consultation with

[90] On the commitment of the Five Eyes nations to "explore enhancing cross-border information sharing," see: "Security summit ends with pledges to tackle emerging threats," UK Home Office, July 30, 2019, https://www.gov.uk/government/news/security-summit-ends-with-pledges-to-tackle-emerging-threats.

[91] "Inaugural Trilateral Meeting of North American Defence Ministers," Department of National Defence and the Canadian Armed Forces, March 27, 2012, http://www.forces.gc.ca/en/news/article.page?doc=inaugural-trilateral-meeting-of-north-american-defence-ministers/hgq87xwv.

[92] *Ibid*.

Canadian and Mexican authorities, develop protocols for the voluntary sharing of critical electric infrastructure information with Canadian and Mexican authorities and owners, operators and users of the bulk power system outside the United States."[93] Representatives of Mexico, Canada, and the United States should partner with grid owners and operators to establish information sharing networks to help understand and mitigate threats that cause cross-border instabilities and wide-area blackouts.

The trilateral assessment should also include threats to natural gas pipeline systems that fuel power generation and meet other critical energy needs across the continent. One promising effort underway to address these threats and to better understand and mitigate the danger that adversaries will seek to exploit gas-electric system interdependencies lies in the North American Energy Resilience Model (NAERM). The DOE launched the NAERM initiative with the explicit goal of modeling such risks on a continent-wide basis and including Mexico and Canada as key partners in the effort. According to Assistant Secretary of Energy Bruce Walker, who is leading the effort, the model will not only be continent-wide but also include "all different components of the energy infrastructure."[94]

The NAERM is intended to support incident response by improving threat identification, and providing real-time situational awareness and modeling to inform operational decision-making.[95] Indeed, DOE is working towards building a capability for "automated next-worse cases analysis" which will provide energy system operators with a predetermined set of mitigation strategies.[96] The NAERM will also benefit long-term planning by using its advanced modeling to identify potential infrastructure investments that will be particularly effective in improving system-wide resilience. Critically, the NAERM will also improve modeling, simulation, and assessment

[93] 16 U.S.C. § 824o–1, Section (d)(5), https://www.law.cornell.edu/uscode/text/16/824o-1.

[94] Jeremy Dillon and Peter Behr, "DOE unveils 'what if' model of growing grid threats," E&E News, July 24, 2019, https://www.eenews.net/stories/1060783223.

[95] Bruce Walker, "Keeping the Nation's Critical Energy Infrastructure Secure and Resilient Requires a Strong STEM Workforce," *Department of Energy*, April 5, 2019, https://www.energy.gov/articles/keeping-nation-s-critical-energy-infrastructure-secure-and-resilient-requires-strong-stem.

[96] Bruce Walker, presentation to the 2018 Southeastern Association of Regulatory Utility Commissioners (SEARUC) Conference, Charleston, South Carolina, June 11, 2018, p. 7, https://www.energy.gov/sites/prod/files/2018/07/f53/Walker%2006-11-18%20SEARUC%20Remarks%20-%20As%20Prepared.pdf.

capabilities on a cross-sector basis, including "analysis regarding the significant interdependencies that have evolved over the last couple decades," and can inform mitigation strategies for vulnerabilities caused by such interdependencies.[97] A trilateral threat assessment could offer a valuable means of sharing the results of this modeling.

However, industry priorities will be essential in guiding the development of the trilateral assessment and ensuring that it supplements and supports existing sharing mechanisms under the E-ISAC and other organizations. Industry support remains strong for trilateral information sharing. For example, the Canadian Electricity Association (CEA), which represents power companies across the nation, emphasizes that "sharing of threat information among sectors and governments of Canada, the US, and Mexico is our first line of defence towards securing the integrity of our systems."[98] In addition, however, the CEA recommends strengthening an additional line of defense: that of developing "integrated, cross-border incident response plans for cyber and physical security threats of national significance."

D. Coordination of Emergency Operations

Government agencies in Mexico, Canada, and the United States are creating forward-looking strategies for responding to cyberattacks on their critical infrastructure and other targets.[99] As in the case of the U.S. *National Cyber Incident Response Plan* (NCIRP), they are also developing increasingly detailed mechanisms for coordination within their governments and with the private sector.[100] The time has come to make equivalent progress to manage energy sector disruptions that spread across national borders. In doing so, governments and their industry partners will need to account for persistent gaps in preparedness, including ambiguities in government roles and

[97] Walker, presentation to the SEARUC Conference, p. 7.

[98] "Protecting the Power Grid," Canadian Electricity Association, n.d., https://electricity.ca/lead/powering-canadas-economy/protecting-power-grid/.

[99] Government of Mexico, *National Cybersecurity Strategy*, 2017, https://www.gob.mx/cms/uploads/attachment/file/399655/ENCS.ENG.final.pdf; Public Safety Canada, *National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age*, 2018, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf; White House, *National Cyber Strategy of the United States of America*, September 2018, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

[100] DHS, *National Cyber Incident Response Plan*, December 2016, https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf.

responsibilities and inadequate coordination of emergency measures by gas and electric system operators.

1. Grid Security Emergencies and Beyond

A number of agreements exist for emergency cooperation between the United States and Canada. How they fit together is unclear. The *Agreement Between the Government of Canada and the Government of the United States on Emergency Management Cooperation* is intended to be "comprehensive."[101] However, the 2015 *Cybersecurity Action Plan* created by DHS and Public Safety Canada provides very different coordination mechanisms. Moreover, the U.S. NCIRP offers only a top-level description of how Cyber Unified Coordination Groups and other government organizations would manage cross-border collaboration and how these groups would coordinate with grid owners and operators.[102] The two governments should streamline emergency coordination mechanisms and (in collaboration with industry) provide additional details to support operational collaboration for protecting and restoring grid reliability.

An immediate opportunity to achieve such progress lies in developing plans and coordination mechanisms for cross-border collaboration in grid security emergencies (GSEs). While the North American power companies subject to NERC reliability standards are increasingly well prepared to assist each other in response to cyberattacks, government agencies will have a strong stake in helping prioritize the restoration of power to meet national priorities. The U.S. Congress has given the Secretary of Energy significant new authorities to guide such emergency operations. Most important, the Secretary now has the authority to issue emergency orders to U.S. power companies when cyberattacks and other severe events occur. The Secretary can and direct these companies to take whatever measures she or he deems necessary to protect and restore grid reliability, and do so in ways that help ensure electric service to critical defense facilities and other vital assets.[103]

---

[101] Governments of Canada and the United States, *Agreement Between the Government of Canada and the Government of the United States of America on Emergency Management Cooperation*, signed December 12, 2008, https://www.treaty-accord.gc.ca/text-texte.aspx?id=105173.

[102] DHS, *National Cyber Incident Response Plan* pp. 14 and 26-27.

[103] The Fixing America's Surface Transportation (FAST) Act amends Section 215A of the Federal Power Act (FPA) to grant the Secretary this authority. See: FAST Act, Public Law 114-94, *U.S. Statutes at Large* 129 (2015): 1774–1775, https://www.congress.gov/114/plaws/publ94/PLAW-114publ94.pdf.

Of course, the Secretary has no authority over Mexican or Canadian power companies. As noted above, however, cyberattacks on the U.S. grid could create disruptions across interconnected electric systems in Canada and portions of Northern Mexico. Given the unique binational U.S.-Canada partnership in the North American Aerospace Defense Command (NORAD), and each nation's obligations to defend the other as North Atlantic Treaty Organization (NATO) allies, potential cyber adversaries such as Russia or China may also seek to create grid emergencies in both nations.

The November 2019 GridEx exercise revealed significant opportunities to strengthen collaboration between the U.S. and Canadian governments in such emergencies, commensurate with the extensive coordination mechanisms that already exist between their respective power companies. The aforementioned GSE legislation provides an imperative to do so. That law requires the U.S. Secretary of Energy to consult with appropriate governmental authorities in Canada and Mexico before issuing a GSE order, "to the extent practicable in light of the nature of the grid security emergency."[104]

Left unspecified (and clear as mud) are the authorities that the Secretary should include in such consultations. Natural Resources Canada, Public Safety Canada, the U.S. DOE, and the U.S. DHS will be vital participants. The U.S. National Security Council and the Canadian Privy Council Office (which supports the Prime Minister and Cabinet) would almost certainly be included as well. In addition, the intelligence communities and Defense establishments of both nations could also have major responsibilities for responding to attacks on the grid and for providing data to prioritize restoration operations. State governors and the premiers of affected provinces might also need to be included in GSE discussions, especially given the jurisdiction that provincial authorities exercise over Canadian electric systems.[105] The governments should untangle this web of potential consultative parties well before an attack occurs and streamline collaborative mechanics so they will function rapidly and effectively in the mist of ongoing cyberattacks.

[104] 16 U.S.C. § 824o-1, Section (b)(3), https://www.law.cornell.edu/uscode/text/16/824o-1.

[105] Geoff Smith, "The Federal/Provincial Electricity Relationship in Canada: It's Complicated," Canadian Electricity Association, July 8, 2013, https://electricity.ca/blog/the-federalprovincial-electricity-relationship-in-canada-its-complicated/.

Exercises can help assess organizational options and build expertise in conducting GSE consultations. The GridEx V Lessons Learned Report recommends that "When designing the next GridEx executive tabletop, NERC and the Canadian Electricity Association should invite Canadian government representatives (e.g., the Privy Council, Natural Resources Canada, Public Safety Canada) to participate" in the exercise. The report also recommended that "in addition to federal government participants, NERC should invite government representatives at the provincial and state levels to further explore additional operational issues."[106] Other cyber exercises including DHS' Cyber Storm and DOE's Liberty Eclipse might evolve over time to address collaborative challenges as well, and – as practical – include Mexican participation.

The next layer of complexity lies in including industry in bilateral (and as appropriate, trilateral) emergency collaboration between government agencies. The *Federal Power Act* requires that to the extent practicable, the Secretary of Energy will consult also with power companies prior to issuing emergency orders.[107] GridEx revealed significant differences between industry and U.S. government perspectives on how DOE should design emergency orders. The exercise also identified opportunities to build consensus on how Canadian grid owners and operators could help anticipate and manage cross-border effects created by the implementation of emergency orders may create.[108] In addition, government and industry partners should consider how the issuance of such orders might be aligned with emergency actions by taken gas systems and their oversight agencies.[109]

E. NORAD Support for Grid Defense?

Confronted by a growing threat from nuclear-armed Soviet bombers in the 1950s, leaders of Canada and the United States determined that – rather than defend their airspace on their own – the two nations could more effectively counter this shared threat by collaborating. They established NORAD in 1957 to create a bi-national system of air defense in which each nation retained its own sovereignty. Given the rising cyber threats to North America's interconnected grid, would it make

[106] NERC, *GridEx V: Lessons Learned Report*, p. 11.
[107] 16 U.S.C. § 824o-1, Section (b)(3).
[108] NERC, *GridEx V: Lessons Learned Report*, p, 7.
[109] NERC, *GridEx V: Lessons Learned Report*, pp. 7-8.

sense for NORAD to take on new support functions for grid defense and assist utilities and their lead government partners within the framework of a proven, highly effective bi-national command structure?

Expansion of NORAD's mission is not unprecedented. Since its inception as a U.S.-Canada binational defense system to protect their territories from long-range Soviet bombers, NORAD has grown to encompass new missions and plays a vital role in aerospace warning, aerospace control, and maritime warning for both nations.[110] Recognizing the need for increased security and innovation, NORAD Commander General Terrence O'Shaughnessy of the U.S. Air Force noted that, "Our competitors currently hold our citizens and national interests at risk, and we must anticipate attacks against our defense and civilian infrastructure in the event of a conflict."[111]

As such, the United States and Canada have started to implement cyber functions within NORAD. The two countries established a Joint Cyber Center under NORAD in 2012, which includes cyber situational awareness and "providing cyber consequence response and recovery support to civil authorities" among its main missions.[112]

In addition, Mexico's armed forces are increasingly coordinating with Canada and the United States via NORAD to improve North American security. Mexico's National Defense Forces (SEDENA) have participated in NORAD exercises, most recently in AMALGAM EAGLE 19 in July 2019. While this exercise focused on NORAD's core mission of aerospace defense, the exercise nonetheless helped to "Improve the operational and communications capabilities between NORAD and USNORTHCOM, and SEDENA to provide a common operational picture."[113] These

[110] "The Canada-U.S. Defence Relationship," *Department of National Defence and the Canadian Armed Forces*, December 4, 2014, http://www.forces.gc.ca/en/news/article.page?doc=the-canada-u-s-defence-relationship/hob7hd8s.

[111] Terrence O'Shaughnessy, Testimony Before the Senate Armed Services Committee, February 26, 2019, p. 2, https://www.armed-services.senate.gov/imo/media/doc/OShaughnessy_02-26-19.pdf.

[112] Thomas J. Doscher, "NORAD, USNORTHCOM Joint Cyber Center stands up," *North American Aerospace Defense Command (NORAD)*, May 1, 2012, http://www.norad.mil/Newsroom/Article/578606/norad-usnorthcom-joint-cyber-center-stands-up/.

[113] "NORAD, USNORTHCOM and the Mexican Air Force to participate in AMALGAM EAGLE 19," *NORAD*, July 16, 2019, https://www.norad.mil/Newsroom/Press-Releases/Article/1906305/norad-usnorthcom-and-the-mexican-air-force-to-participate-in-amalgam-eagle-19/.

capabilities will be critical to Mexico's inclusion in an expanded partnership to protect North American critical infrastructure from cyberattacks.

NORAD provides key opportunities for collaboration. However, there are strong reasons why its role in cyber defense of the power grid should remain limited. While defense and intelligence organizations in the United States, Mexico, and Canada can provide valuable threat information and analysis, civilian agencies in North America are primarily responsible for partnering with utilities to ensure grid resilience. Given the strong and effective ties that already exist between energy sector agencies, their industry partners, and other stakeholders, the role of defense organizations in domestic protection of the grid should remain one of support, rather than leadership.

Having NORAD retain a limited role in the cyber defense of North American critical infrastructure will also help it remain focused on its existing missions. NORAD's role in continental air defense remains vital in the face of increasingly frequent penetrations of its Air Defense Identification Zone (ADIZ) by Russian bombers, Chinese and Russian deployments of highly-sophisticated cruise missiles, and the rise of unmanned aerial vehicles (UAVs), among other national security threats.[114] NORAD provides critical security in the maritime warning realm as well, especially in the Arctic. NORAD Commander O'Shaughnessy notes that defending against these threats will require continuous adaptation and reinvigorated partnerships.[115] Notably, he has not called for NORAD to take over new roles for civilian infrastructure defense.

Even though NORAD's role in grid protection should remain limited, the organization can provide essential insight into the effective establishment of binational command mechanisms, helping the continent establish functional grid emergency response capabilities that still respect state sovereignty. As industry and government partners and other grid resilience stakeholders strengthen their collaborative mechanisms for trilateral grid defense, NORAD provides a wealth of lessons

[114] O'Shaughnessy, Testimony Before the Senate Armed Services Committee, p. 3-4, 14; Wilson Brissett, "NORAD's Next Evolution," Air Force Magazine, April 2017, http://www.airforcemag.com/MagazineArchive/Pages/2017/April%202017/NORAD's-Next-Evolution.aspx.

[115] O'Shaughnessy, Testimony Before the Senate Armed Services Committee, p. 2.

learned on how all three nations can preserve their sovereignty while contributing to their shared security.

The same is true of NERC and the E-ISAC. While not exactly "bi (or tri) national commands," these two organizations have established an extraordinary model of collaboration between power companies and their government partners across the continent. Mexican, Canadian, and U.S. policymakers and industry leaders should explore how to leverage the distinct forms of cross-border collaboration achieved by NORAD, NERC, and the E-ISAC to strengthen resilience against the increasingly severe threats to North American infrastructure.