Photo: Public Safety Canada

2.1 RISK MITIGATION IN CRITICAL INFRASTRUCTURE

June 2022

DRRPathways.ca

RESILIENCE PATHWAYS

CO-CREATING NEW KNOWLEDGE FOR UNDERSTANDING RISK AND RESILIENCE IN BC

This article is part of the Resilience Pathways Report. The report has the following objectives: a) to share knowledge about existing practices and recent advances in understanding and managing disaster and climate risk in BC, including some information on relevant federal programs, and b) to provide insights on gaps and recommendations that will help build pathways to resilience in BC.

This article belongs to *Chapter 2 Climate and Disaster Risk Management: Practice*. To read all articles in the report, see DRRPathways.ca.

The Resilience Pathways Report is a project of Natural Resources Canada.

2.1 RISK MITIGATION IN CRITICAL INFRASTRUCTURE

BY:

Alisha Texeira, Public Safety Canada

CONTRIBUTORS:

CI Policy Unit, Public Safety Canada

EDITORS:

Sahar Safaie, Sage On Earth Consulting

Shana Johnstone, Uncover Editorial + Design

COORDINATING RISK MITIGATION

NATIONAL STRATEGY FOR CRITICAL INFRASTRUCTURE

The *National Strategy for Critical Infrastructure (2009)* (the Strategy) sets out Canada's approach to strengthening the resilience of critical infrastructure (CI). The Strategy defines CI as the "processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government."[1] CI can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders. Disruptions of CI could result in catastrophic loss of life and injuries, adverse economic effects, and significant harm to public confidence.

The Strategy advances coherent and complementary actions among federal, provincial, and territorial initiatives and among the ten CI sectors: energy and utilities, finance, food, transportation (Figure 1), water (Figure 2), government, information and communication technology, health, safety, and manufacturing.[2] A Lead Federal Department (LFD) is responsible for each sector and for bringing together a network of stakeholders and representatives from within each sector. The Strategy is built around three strategic objectives: 1) building partnerships among federal, provincial and territorial governments and CI sectors, 2) implementing an all-hazards risk management approach, and 3) advancing the timely sharing and protection of information among partners.[3]

Between 2018 and 2020, Public Safety Canada led an examination of the Strategy to determine if there was a need to update Canada's overall approach to CI resilience. The examination's findings recommended a renewal process, which will take place over the next three years (2021–2023).[4] The renewal of the Strategy is an opportunity to shed light on what is working well, what needs to be improved, and what our vision for the future should be, as Canada faces an evolving list of risks and threats.

1. BUILDING PARTNERSHIPS

As detailed in the *Emergency Management Framework for Canada*,[5] strengthening the resilience of CI requires complementary and coherent action by all partners to promote the most effective use of resources and execution of activities. Harmonizing approaches to strengthening the resilience of CI at all levels will enable efforts to facilitate timely and effective prevention, mitigation,

Figure 1: Trains and rail lines provide critical transportation infrastructure (Photo: Public Safety Canada).

preparedness, response and recovery measures to deal effectively with disruptions. The Strategy recognizes that each responsible jurisdiction, department and agency, as well as CI owners and operators, will take action as they deem appropriate for strengthening the resilience of CI in Canada. To be successful, however, the implementation of the Strategy requires the collaboration of federal, provincial, territorial and CI sector partners and the establishment of engagement mechanisms to facilitate this collaboration.[6]

2. IMPLEMENTING AN ALL-HAZARDS APPROACH

The Strategy promotes the application of risk management and sound business continuity planning. Risk management refers to the "continuous, proactive and systematic process to understand, manage and communicate risks, threats, vulnerabilities and interdependencies across the CI community." A comprehensive risk management process requires that federal, provincial and territorial governments collaborate with their CI partners to develop all-hazards risk analyses that take into account accidental, intentional and natural hazards. While governments promote a common approach to strengthening the resilience of CI, and share tools, lessons learned and best practices, CI stakeholders are ultimately responsible for implementing their own risk management approach given their situation.[7]

As part of the Strategy, federal, provincial and territorial governments conduct exercises and assist in the coordination of regional exercise planning across jurisdictions and with CI sectors. Exercises help partners with an assessment of their CI and recommend improvements to their plans, which ensure an effective response and recovery in the face of a CI disruption.

A comprehensive risk management process requires that federal, provincial and territorial governments collaborate with their CI partners to develop all-hazards risk analyses that take into account accidental, intentional and natural hazards. . . . CI stakeholders are ultimately responsible for implementing their own risk management approach given their situation.

3. SHARING AND PROTECTING INFORMATION

Information sharing and information protection play a key role in collaborative efforts to strengthen the resilience of CI. Improved information sharing, within existing federal, provincial and territorial legislation and policies, enhances the timely exchange of information on risks and the overall status of

critical assets, so that CI owners and operators, governments and others can assess risks and take appropriate action.[8] Information exchange is crucial before, during and after a disruption or emergency, as it enables a "common operating picture" among all levels of government and CI sectors an improved approach across the range of prevention, mitigation, preparedness, response and recovery.[9]

> Information sharing and information protection play a key role in collaborative efforts to strengthen the resilience of CI. Improved information sharing, within existing federal, provincial and territorial legislation and policies, enhances the timely exchange of information on risks and the overall status of critical assets.

Due to the many interdependencies in Canadian CI, the inappropriate release of sensitive information poses a risk for a province or local authority and Canada as a whole. There are some exemptions from disclosure for reasons of national security and public safety, existing under federal, provincial and territorial access to and freedom of information legislation.[10] A consequential amendment to the *Access to Information Act*, as part of the Government of Canada's *Emergency Management Act*, gave clear protection to sensitive information provided by CI owners and operators. Governments continue to ensure an appropriate level of protection to sensitive emergency management and CI information.[11]

THE NATIONAL CROSS SECTOR FORUM ACTION PLAN FOR CRITICAL INFRASTRUCTURE

The *National Cross Sector Forum Action Plan for Critical Infrastructure* (the Action Plan) acts as a blueprint for how the Strategy is implemented to enhance the resilience of Canada's CI. Since the publication of the Strategy in 2009, four supporting action plans (2010–2013; 2014–2017; 2018–2020; and 2021–2023) have been released, each outlining concrete steps towards advancing the three objectives set out in the Strategy.[12]

The first Action Plan (2010–2013) set out the roles and responsibilities of the federal government, provincial and territorial governments, and CI owners and operators along with action items in the areas of partnerships, risk management and information sharing.[13] Within years one and two, partners focused on the development of sector networks and the National Cross Sector Forum (NCSF) as well as improved information sharing. Initial activities in support of risk management were also undertaken at this time. During subsequent years, effective sector networks and improved information has enabled further risk management activities (e.g., development of sectoral risk profiles, guidelines for risk assessments) and emergency management planning and exercises.[14]

Public Safety Canada currently conducts all-hazard risk assessments through the physical-based Regional Resilience Assessment Program and the Canadian Cyber Security Tool and cyber assessment program. This includes working with provinces and territories to determine priority sites for physical assessment and identifying and implementing measures to increase the impact and reach of the cyber and physical programs. Public Safety Canada also produces risk assessment products based on specific hazards (flood, wildfire, earthquake, hurricane, etc.) or in response to potential or occurring emergencies with potential to disrupt CI.

To continue supporting the advancement of the Strategy's three strategic objectives until the release of the renewed national approach to CI resilience, Public Safety Canada (PS) has created the *National Cross Sector Forum 2021–2023 Action Plan for Critical Infrastructure*. The Action Plan (2021–2023) reaffirms the Government of Canada's commitments to work closely with CI sector partners, provinces and territories towards a more secure and resilient Canada. The Action Plan (2021–2023) also continues to support the three strategic objectives identified in the Strategy and builds upon progress made through past

action plans, identifies new activities based on the changing threat environment, and will support a collaborative approach to enhance the security and resilience of Canada's CI.[15]

ALIGNMENT WITH THE SENDAI FRAMEWORK

The work under the Strategy and subsequent Action Plans for CI contribute to the Sendai Framework for Disaster Risk Reduction's seven global targets. The work directly contributes to (18) Target (d) and is critical for achieving Targets (a), (b), (c), and (g).

In the Sendai Framework, item 18 (d) states: "Substantially reduce disaster damage to critical infrastructure and disruption of basic services, among them health and educational facilities, including through developing their resilience by 2030."[16]

While in most clauses of the Sendai Framework CI is bundled with all other assets, one commitment is specific to CI. Item 33 (c) states: "To achieve this, it is important: . . . To promote the resilience of new and existing critical infrastructure, including water, transportation and telecommunications infrastructure, educational facilities, hospitals and other health facilities, to ensure that they remain safe, effective and operational during and after disasters in order to provide life-saving and essential services."[17]

ENGAGEMENT MECHANISMS

The following section outlines activities and action items that support the risk management principles outlined in the Strategy's strategic objectives. The purpose of the activities is to strengthen Canada's CI resilience by helping to prevent, mitigate, prepare for, respond to, and recover from disruptions. Additionally, they are designed to foster collaboration and information sharing among all levels of government, private sector partners, and allied countries.[18]

THE NATIONAL CROSS SECTOR FORUM

The Strategy and Action Plan (2010–2013) established the National Cross Sector Forum (NCSF) to maintain a comprehensive and collaborative Canadian approach to enhance the resilience of CI, by providing a standing mechanism for discussion and information exchange within and between levels of governments and CI sectors. Membership is drawn from the ten sector networks and is representative of a wide-ranging number of CI owners and operators, associations, and provincial and territorial governments.[19] Typically, one to three senior-level members of each sector network represents the CI sector at the NCSF.

The NCSF membership has developed terms of reference for the NCSF, including the designation of three chairs—the Deputy Minister of Public Safety, one industry representative, and one provincial/territorial representative. The chairs work with members to set agendas, determine the frequency of meetings and manage the business of the NCSF.[20] The Critical Infrastructure Division, Public Safety Canada, serves as the NCSF's secretariat, where the Division's staff provide strategic advice, support information sharing, develop the cross-sector risk profile, and provide general support to the NCSF.

THE MULTI-SECTOR NETWORK

The MSN provides a platform to examine Canada's CI priorities from a cross-sector and multi-jurisdictional perspective, facilitate the timely exchange of relevant information on CI risks and emerging issues, and foster cross-sector partnerships among CI owners and operators.[21] It brings together working-level representatives from each of the ten CI sectors and may also include representatives from the NCSF, LFDs, provinces and territories, and the international CI community to discuss topics related to CI resilience.

THE FEDERAL, PROVINCIAL AND TERRITORIAL CRITICAL INFRASTRUCTURE WORKING GROUP

The Federal, Provincial and Territorial Critical Infrastructure Working Group (FPT CI WG) is the primary

Figure 2: Wastewater treatment plants provide critical water infrastructure (Photo: Public Safety Canada).

mechanism for federal, provincial and territorial government collaboration on current and emerging issues facing CI sectors, including recent COVID-19 response efforts. Membership is open to all governments for participation if it meets their needs and as their resources permit.

The FPT CI WG is co-chaired by a representative from Public Safety Canada and a provincial/territorial representative determined by group consensus. The co-chairs report to the Federal-Provincial-Territorial Senior Officials Responsible for Emergency Management (SOREM) on CI matters. Public Safety Canada serves as the secretariat for the FPT CI WG by organizing meetings, as identified by the co-chairs, and is responsible for preparing and distributing material.[22]

THE LEAD FEDERAL DEPARTMENTS CRITICAL INFRASTRUCTURE NETWORK (LFD CI NETWORK)

The Lead Federal Departments Critical Infrastructure Network (LFD CI Network) is a group of officials from departments leading each of the ten CI sectors, as follows:

- Energy and Utilities (Natural Resources Canada)
- Finance (Department of Finance Canada)
- Food (Agriculture and Agri-Food Canada)
- Health (Public Health Agency of Canada
- Information and Communication Technology (Innovation, Science and Economic Development Canada)

- Manufacturing (Department of National Defense)
- Manufacturing (Innovation, Science and Economic Development Canada)
- Transportation (Transport Canada)
- Government/Safety/Water (Public Safety Canada)

Through network meetings between government departments that are industry leads, the group works to strengthen their collective ability to identify and address disruptions to Canada's CI and share information with their networks of CI stakeholders.

SECTOR NETWORKS

The Strategy and first Action Plan (2010–2013) established sector networks: "national sector-specific standing fora for each of the ten CI sectors to address sectoral and regional issues, and enable information sharing on CI."[23] The sector networks reflect a partnership model that enable governments and CI sectors to undertake a range of activities (e.g., risk assessments, plans to address risks, exercises) unique to each sector. The Strategy provided a framework for the functions of the sector networks, including:

- Promotion of timely information sharing.
- Identification of issues of national, regional or sectoral concern.
- Use of subject-matter expertise from CI sectors to provide guidance on current and future challenges.
- Development of tools and best practices for strengthening the resilience of CI across the full spectrum of prevention, mitigation, preparedness, response and recovery.[24]

Working with CI partners, each LFD has facilitated the development of sector networks to meet the needs of their stakeholders.[25] Sub-sector networks have also been established to reflect the diversity of a particular sector where appropriate. Participation in these networks is voluntary. The sector networks are composed of CI owners and operators as well as national associations from CI sectors and relevant federal, provincial and territorial departments and agencies.[26]

CI GATEWAY

Public Safety Canada also engages CI partners and stakeholders through the CI Gateway—a practical online tool for facilitating information sharing across the ten CI sectors. It hosts information products such as risk management documents, best practices, lessons learned, meeting materials, standards, and event calendars to enhance situational awareness. Membership is granted to stakeholders belonging to a CI sector network and to relevant government partners. There is ongoing work to renew and modernize the GI Gateway in the coming years.[27]

CROSS-CUTTING ISSUES

SUPPLY CHAIN MANAGEMENT AND IMPACTS TO CI

Canada relies on national and international supply chains, which means that the goods and services that CI requires, from fertilizer to pharmaceuticals, can come from anywhere in the world. As a result, Canada's critical functions can be impacted by both domestic and international disruptions. A trade dispute, international conflict (e.g., 2022's Russian invasion of Ukraine), a transportation issue (e.g., 2020's Canadian National Railway blockade, 2022's blockages by the "Freedom Convoy") or other disruption in another country could impact the ability for Canada's CI to acquire important supplies.[28] Increasingly, malicious actors are leveraging supply chain vulnerabilities to conduct cyber-attacks. For example, a 2020 cyber-attack led to thousands of organizations, from the information and communications technology sector to government, downloading malware through IT management software supplied by SolarWinds. At the time of writing, the Canadian Security Establishment's (CSE) Centre for Cyber Security is warning CI organizations and suppliers to bolster their awareness and protection against Russian state-sponsored cyber threads amid the invasion of Ukraine.[29]

RANSOMWARE ATTACKS DURING COVID-19

One of the most significant threats to Canada's CI during the COVID-19 pandemic has been ransomware cyber-attacks. Ransomware attacks are those where criminals hold data or computer systems hostage in exchange for payment. CSE's Centre for Cyber Security predicted that as the pandemic continues, attacks directed against Canada will continue to target large enterprises and CI owners and operations Canadian CI is also at risk of the type of ransomware attack that recently shut down the Colonial pipeline in the US for multiple days. Health-sector organizations have also become popular ransomware targets during the COVID-19 pandemic, due to the importance of keeping health services available and reliable with zero downtime or disruption. At such a critical time, network downtime can have life-threatening consequences for patients, while increasing the likelihood that victims of such attacks will pay the ransom.[30]

THE NATIONAL STRATEGY FOR CRITICAL INFRASTRUCTURE RENEWAL

DRIVERS OF CHANGE IN CANADA'S CI ENVIRONMENT

The risk landscape facing the Canadian CI community is a complex one, characterized by a range of uncertainties and evolving threats and pressures, including environmental and climate change impacts, security (e.g., cyber, national, physical, economic, health, and foreign interference), aging CI, and economic recovery. The global pandemic health crisis has identified the need for greater focus by CI stakeholders on organizational preparedness, business continuity and management of risks posed by globally distributed supply chains that support critical infrastructure operations.[31]

Several key drivers of change were identified as part the Strategy examination: digitalization of systems and processes, environmental risks, security threats, and economic prosperity. These drivers are adding to the pressures and demands to which CI must adapt.

DIGITALIZATION OF SYSTEMS AND PROCESSES

The digitalization of systems and processes, and the ability to control CI operations remotely, continues to present new cyber security challenges. The increased use of digital systems to operate physical infrastructure has improved overall connectivity, communications, and service delivery to Canadians. However, the use of internet-enabled systems increases the likelihood and scale of both intentional and unintentional disruptions. Malicious actors continue to find new ways to

THE EXTENDED NATIONAL CROSS SECTOR FORUM (E-NCSF) ON COVID-19

In March 2020, at the onset of the pandemic, NCSF meetings were expanded to include hundreds of new participants across all ten CI sectors and began to be delivered in a virtual format. This new forum was rebranded as the Extended National Cross Sector Forum (E-NCSF) on COVID-19 in order to differentiate its activities from the "core" NCSF. The CI community used this outlet as events continued to unfold in the pandemic, to review the current status of the COVID-19 virus in Canada, update CI stakeholders on federal planning activities, and share areas of priority for CI industry owners and operators. E-NCSF meetings have included updates from the Public Health Agency of Canada, Public Safety Canada and the Government Operations Centre on various topics including supply chain and liquidity issues, personal protective equipment (PPE), testing and vaccination, guidance, and more. Representatives from each of the ten CI sectors also provide updates share common challenges and impacts to their respective sectors and supply chains during E-NCSF roundtable discussions. On average, 120–150 stakeholders attended E-NCSF meetings.

use cyber-attacks to disrupt CI and exploit Canadians.[32]

ENVIRONMENTAL AND CLIMATE CHANGE RISKS

Canada's climate is changing. The effects of global warming are apparent in many parts of the country and are anticipated to increase in the future. These shifts are significantly affecting Canada's natural environment, built infrastructure, economy, and the health of Canadians. Extreme weather events, such as floods and fires in Western Canada, continue to threaten the ability of CI to deliver services.[33]

SECURITY THREATS

Terrorism, extremism, organized criminals, and hostile state actors all pose threats to Canada's national security and CI. Foreign actors, with the support of state-level resources, are developing advanced capabilities to target CI and other public-private sector institutions, increasingly leveraging cyber systems to conduct espionage, steal intellectual property, and disrupt operations. Security concerns related to the rise of global supply chains, which CI depends on for products and services continues to pose significant concern. Supply chains are world-wide, making it difficult to identify single points of failure and rendering them vulnerable to accidental and international disruption.[34]

ECONOMIC PROSPERITY

Dependable CI drives economic growth by creating jobs, improving productivity and enabling business confidence, which fosters innovation and investment in CI. Continued investment requires customers, taxpayers and a thriving economy to fund investments, whether privately or publicly owned.[35] However, as record deficits have added to government debt at a time when aging infrastructure requires servicing, the full impact of the pandemic is yet to be seen. While recovering from the impacts of the pandemic, Canada will have to address inequitable access to infrastructure in order to allow all Canadians to prosper.

The challenge of securing and maintaining Canada's critical assets and systems in a complex and fast-changing risk landscape will require coordinated approaches between the public sector, private sector, and citizens, which in turn will foster ingenuity, promote adaptability, and ensure collaboration.[36] The National Strategy for CI renewal provides an opportunity to help bring CI communities together and equip them with a common framework for identifying and managing risks and for coordinating decision-making activities to meet collective resilience goals.

CONSULTATION

The purpose of the consultation process, as part of the Strategy renewal, is to solicit input, advice, and ideas to renew the Strategy and Canada's overall approach to CI resilience. Consultation will focus on six key areas of inquiry.

The challenge of securing and maintaining Canada's critical assets and systems in a complex and fast-changing risk landscape will require coordinated approaches between the public sector, private sector, and citizens, which in turn will foster ingenuity, promote adaptability, and ensure collaboration. The National Strategy for CI renewal provides an opportunity to help bring CI communities together and equip them with a common framework for identifying and managing risks and for coordinating decision-making activities to meet collective resilience goals.

1. FUNDAMENTAL CONCEPTS AND DEFINITIONS

Assessing the criticality of CI is not easy because criticality can be dynamic; it changes depending on the current context and situation. For example, during the COVID-19 pandemic, the federal, provincial and territorial governments published

lists of essential services. These lists helped determine which businesses could remain open and access reserves of personal protective equipment (PPE), but they were not exhaustive. Criticality affects risk management, planning and preparedness efforts and helps governments respond more effectively during event state. In steady state, the concept of criticality is helpful for governments in determining supports, such as risk assessments provided at no cost to the business, and minimum standards of resilience. It could be argued that a range of key CI-related concepts and definitions are either dated, not widely agreed upon, or could be improved.[37]

2. CROSS-SECTOR INTERDEPENDENCIES AND DIGITALIZATION

CI sectors are highly interdependent, which means that sectors rely on one another to deliver the goods and services that Canadians need. The resilience of a CI sector is therefore determined not only by its own efforts to secure its operations but by the resilience of the many integrated systems that it relies on within other CI sectors. The interdependency of CI sectors means that a failure in one sector can have a domino effect on other sectors. Additionally, the growing connection of CI to the internet not only causes greater cyber security challenges but adds to the dependence of CI on the information and communications technology sector.[38] CI relies heavily on the information and communications technology sector to communicate, conduct business and connect with other sectors. An information and communications technology disruption, caused by a natural disaster, a cyber-attack, or an accident, could have far-reaching consequences (Figure 3).

Figure 3: Satellite ground systems provide critical information and communication infrastructure (Photo: Public Safety Canada).

Digitalization will continue to create greater interdependencies that will require greater coordination of risk management practices across CI sectors, as an attack on a physical-cyber system could result in a catastrophic failure in an area we previously considered unrelated to CI. The digital and interconnected nature of CI complicates interdependency analysis in such a way that will not easily be addressed by one model. A way to address this issue could be to develop new types of responses to protect CI systems and mitigate risk to ensure their resilience.[39]

3. CI SECTOR CONFIGURATION AND COLLABORATION

It can be argued that Canada's ten designated CI sectors and engagement mechanisms are in need of a review because the current sectors do not represent the full range of Canada's vital assets and systems. Exclusions of these businesses and systems from the ten CI sectors means that experts in these areas are not represented in current CI engagement forums.[40] For example, current engagement mechanisms do not include key CI representatives, like Indigenous leadership or municipal governments. Indigenous and municipal governments own and provide CI, for example, in the water sector. As previously discussed, the interdependency of CI sectors presents significant risks that can only be better understood through collaboration. A possible solution could be the reconfiguration of CI sector networks into networks grouped by function, could help to identify interdependencies and related risks, as well as facilitate cross-sector information sharing.[41]

4. CROSS-SECTOR COORDINATION, GOVERNANCE AND COMPLIANCE

Although CI is the common factor that connects many initiatives, priorities and approaches to CI and resilience often vary across various initiatives, CI sectors and regions. Although the current Strategy was developed to be the coordinating link between various domains (i.e., emergency management, national security, cyber security), other initiatives and strategies often have stronger governance, authorities, incentives and compliance mechanisms to address specific risks within a particular domain.[42] Several cross-sector CI fora exist; however, these engagement mechanisms do not have cross-sector authorities or compliance measures.

A way to address these issues could be to develop a clear framework that supports results and accountability to help ensure that a focused direction exists, that objectives are achieved for public and private sector investments, and that efforts to enhance the security and resilience of CI are measurable. Canada currently does not have a national results-based framework in place that effectively measures the collaborative, non-regulatory efforts to achieve CI objectives (as set out in the Strategy) and supporting action plans.[43]

A way to address these issues could be to develop a clear framework that supports results and accountability to help ensure that a focused direction exists, that objectives are achieved for public and private sector investments, and that efforts to enhance the security and resilience of CI are measurable. Canada currently does not have a national results-based framework in place that effectively measures the collaborative, non-regulatory efforts to achieve CI objectives (as set out in the Strategy) and supporting action plans.

5. ROLES, RESPONSIBILITIES AND SUPPORT TO CI OWNERS AND OPERATORS

Service delivery models and support available to CI owners and operators differ across Canada as well as at regional and municipal levels. The roles and responsibilities are not clearly understood across CI partners and stakeholders. Although different delivery models across regions might be needed to address the specific

situation, the cluttered organizational landscape makes it difficult to advance common CI priorities and resilience goals and creates conflicting advice for CI owners and operators.[44]

6. ACADEMIC RESEARCH AND EXPERTISE TO SUPPORT RISK MANAGEMENT

Through research and expertise, academia and the scientific community play an important role in supporting various CI initiatives in an ad hoc manner. However, experts from federal, provincial and territorial emergency management, municipalities, Indigenous organizations, academia, policy think tanks and subject matter experts in cyber security, physical infrastructure, digital infrastructure, climate change, economic security, and business continuity are not regularly engaged through formal engagement mechanisms like the NCSF. To address this issue, building stronger and more formalized partnerships in the future with academia and think tanks that study issues related to CI security and resilience, infrastructure protection and digital technology could provide valuable advice to Canada's CI leadership.[45]

NEXT STEPS

The consultation process to support the renewal of the National Strategy will be launched in Spring 2022 and will seek input from a broad range of CI stakeholders, including from governments, industry, academia, and Indigenous communities.

RESOURCES

1. The *National Strategy for Critical Infrastructure* (to be read in conjunction with *National Cross Sector Forum 2021–2023 Action Plan for Critical Infrastructure*) sets out Canada's approach to strengthening the resilience of critical infrastructure:

Public Safety Canada. *National Strategy for Critical Infrastructure*. Canada: Her Majesty the Queen in Right of Canada, 2009. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf

2. To continue advancing the objectives of the Strategy until the renewed national approach to critical infrastructure resilience, Public Safety Canada has created the Action Plan (2021–2023):

Public Safety Canada. *National Cross Sector Forum 2021–2023 Action Plan for Critical Infrastructure*. Canada: Her Majesty the Queen in Right of Canada, 2021. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-ctn-pln-crtcl-nfrstrctr/2021-ctn-pln-crtcl-nfrstrctr-en.pdf

ENDNOTES

[1] Public Safety Canada, *National Strategy for Critical Infrastructure* (Canada: Her Majesty the Queen, 2009), accessed June 22, 2021, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf.

[2] Public Safety Canada, *National Strategy for Critical Infrastructure*, doc. 5.

[3] Public Safety Canada, *National Strategy for Critical Infrastructure*, doc. 3.

[4] Public Safety Canada, *National Cross Sector Forum 2021–2023 Action Plan for Critical Infrastructure*, (Canada: Her Majesty the Queen, 2021), 1, accessed June 22, 2021, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-ctn-pln-crtcl-nfrstrctr/2021-ctn-pln-crtcl-nfrstrctr-en.pdf.

[5] Public Safety Canada, *An Emergency Management Framework for Canada Third Addition – Ministers Responsible for Emergency Management* (Canada: Her Majesty the Queen in Right of Canada, 2017), accessed June 22, 2021, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2017-mrgnc-mngmnt-frmwrk/2017-mrgnc-mngmnt-frmwrk-en.pdf.

[6] Public Safety Canada, *National Strategy for Critical Infrastructure*, doc. 6.

[7] Public Safety Canada, *National Strategy for Critical Infrastructure*, doc. 8.

[8] Public Safety Canada, *National Strategy for Critical Infrastructure*, doc. 9.

[9] Public Safety Canada, *National Strategy for Critical Infrastructure*, doc. 10.

[10] Public Safety Canada, *National Strategy for Critical Infrastructure*, doc. 9.

[11] Public Safety Canada, *National Strategy for Critical Infrastructure*, doc. 9.

[12] Public Safety Canada, *National Cross Sector Forum 2021–2023 Action Plan for Critical Infrastructure*.

[13] Public Safety Canada, *National Cross Sector Forum 2009 Action Plan for Critical Infrastructure*, (Canada: Her Majesty the Queen, 2021), accessed June 22, 2021, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/archive-pln-crtcl-nfrstrctr/pln-crtcl-nfrstrctr-eng.pdf.

[14] Public Safety Canada, *National Cross Sector Forum 2009 Action Plan for Critical Infrastructure*, doc. 2.

[15] Public Safety Canada, *National Cross Sector Forum 2021-2023 Action Plan for Critical Infrastructure*, doc. 1.

[16] United Nations, *The Sendai Framework for Disaster Risk Reduction 2015-2030*, (Switzerland: United Nations Office for Disaster Risk Reduction, 2015), accessed March 9, 2022, https://www.preventionweb.net/files/43291_sendaiframeworkfordrren.pdf.

[17] United Nations, *The Sendai Framework for Disaster Risk Reduction 2015-2030*, doc. 21.

[18] Public Safety Canada, *National Cross Sector Forum 2021-2023 Action Plan for Critical Infrastructure*, doc. 9.

[19] Public Safety Canada, *National Cross Sector Forum 2009 Action Plan for Critical Infrastructure*, doc. 14.

[20] Public Safety Canada, *National Cross Sector Forum 2009 Action Plan for Critical Infrastructure*, doc. 14.

[21] Public Safety Canada, *National Cross Sector Forum 2021-2023 Action Plan for Critical Infrastructure*, doc. 9.

[22] Public Safety Canada, *National Cross Sector Forum 2009 Action Plan for Critical Infrastructure*, doc. 16.

[23] Public Safety Canada, *National Cross Sector Forum 2009 Action Plan for Critical Infrastructure*, doc. 12.

[24] Public Safety Canada, *National Strategy for Critical Infrastructure*, doc. 6.

[25] Public Safety Canada, *National Cross Sector Forum 2009 Action Plan for Critical Infrastructure*, doc. 13.

[26] Public Safety Canada, *National Strategy for Critical Infrastructure*, doc. 7.

[27] Public Safety Canada, "Critical Infrastructure Gateway" (Canada: Her Majesty the Queen in Right of Canada, 2017), accessed April 6, 2022, https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/crtcl-nfrstrtr-gw-en.aspx.

[28] Catherine Tunney, "Pandemic could affect food supplies, power grids, telecommunications, says government document," *CBC News*, April 15, 2020.

[29] Brooklyn Neustaeter, "What ramifications will Russia's attach on Ukraine have in Canada?" *CBC News*, February 25, 2022, https://www.ctvnews.ca/canada/what-ramifications-will-russia-s-attack-on-ukraine-have-in-canada-1.5796186

[30] Bronskill, "Experts warn."

[31] Public Safety Canada, "Consultation Paper."

[32] Public Safety Canada, "Consultation Paper."

[33] Public Safety Canada, "Consultation Paper."

[34] Public Safety Canada, "Consultation Paper."

[35] Public Safety Canada, "Consultation Paper."

[36] Public Safety Canada, "Consultation Paper."

[37] Public Safety Canada, "Consultation Paper."

[38] Public Safety Canada, "Consultation Paper."

[39] Public Safety Canada, "Consultation Paper."

[40] Public Safety Canada, "Consultation Paper."

[41] Public Safety Canada, "Consultation Paper."

[42] Public Safety Canada, "Consultation Paper."

[43] Public Safety Canada, "Consultation Paper."

[44] Public Safety Canada, "Consultation Paper."

[45] Public Safety Canada, "Consultation Paper."

Recommended citation
Texeira, A., Risk Mitigation in Critical Infrastructure, in Resilient Pathways Report: Co-creating new Knowledge for Understanding Risk and Resilience in BC; Safaie, S., Johnstone, S., Hastings, N.L., eds., Geological Survey of Canada, Open File 8910, 2022 p. 199-212, https://doi.org/10.4095/330534