

Discussion summary: Roundtable on information and communication infrastructure resiliency

Connectivity infrastructure, such as mobile and broadband connectivity, is critical infrastructure. Evolving environmental and geopolitical risks mean that Canada's connectivity infrastructure is becoming increasingly vulnerable to disasters, such as, wildfires, and cyber threats. This poses a challenge as connectivity disruptions can result in significant cascading costs and repercussions. Consider the 2022 Rogers outage which disrupted public services, payment processing, emergency service calls, etc.¹ The incident was a stark reminder of the potentially far-reaching impacts of telecommunication service disruptions. Minimizing these impacts requires coordinated efforts from both the public and private sectors to engage in comprehensive planning and Emergency preparedness.

The next federal election is an opportunity to prioritize Emergency management for Canada's connectivity infrastructure. With support from TELUS, the Institute of Fiscal Studies and Democracy (IFSD) convened an expert roundtable to define the basic components/considerations of an Emergency response approach for Resiliency of connectivity infrastructure. The purpose of the roundtable was to define the basic components of an Emergency response framework to ensure the Resiliency and reliability of connectivity infrastructure. Participants included operators, government, consultants, lobbyists, and academics from Canada and other countries. Consistent with Chatham House Rules, the following is a general summary of the discussion rather than meeting minutes.

In its deliberations, the roundtable was clear: fostering Resiliency is a multi-faceted and multi-actor effort. Economic security and social well-being require that strategies and tools to foster Resiliency cover the full stakeholder environment. As risks are varied and unknown, coordination for long-term planning is required.

Resiliency of ICT should be incentivized at the levels of operators, the state, and end-users because risks are varied and unknown. Economic security and social well-being are inextricably interconnected with ICT, making Resiliency everyone's concern, demanding collective action and investment.

From its deliberations, the following recommendations for the Government of Canada are proposed:

¹ Xona Partners Inc., *Assessment of Rogers Networks for Resiliency and Reliability Following the 8 July 2022 Outage – Executive Summary* (CRTC, 2024), <https://crtc.gc.ca/eng/publications/reports/xona2024.htm>; John P.L. Gannon, "Lessons for Canada from International Approaches to Network Resiliency and Reliability," (paper presented at the 32nd European Conference of the International Telecommunications Society (ITS): "Realising the digital decade in the European Union – Easier said than done?", Madrid, Spain, 19th - 20th June 2023), <https://www.econstor.eu/bitstream/10419/277962/1/Gannon.pdf>.

- 1) Define ICT infrastructure Resiliency as a national issue of importance. Resources and initiatives should be aligned to support long-term strategic management and planning to protect Canada's economic security and social well-being.
- 2) Convene ICT-specific operators and supporting services such as utilities, law enforcement, and recycling, to engage in information sharing and to explore opportunities for joint initiatives, including, collective training/simulation.
- 3) Establish or amend existing legislation to protect ICT critical infrastructure (consistent with the proposed changes in Bill C-26, e.g., adding security as a policy objective and enabling the Government of Canada to act to protect the telecommunications system, etc.) to enhance security and Resiliency.
- 4) Leverage credits to incentivize operators to invest in network Resiliency, focusing on infrastructure hardening, redundancy, and recovery.
- 5) Establish a taxpayer-funded response fund for Emergency that impact ICT infrastructure or networks for restoring infrastructure, enabling rapid recovery, and ensuring continuity of critical telecom services during and after events.
- 6) Define the data required to size ICT Resiliency risk, and align mechanisms such as standardized reporting and Emergency management frameworks to ensure informed planning and investment decisions.

Why does ICT Resiliency matter?

In August 2024, the Government of Canada announced public consultations on potential new measures to advance and defend the country's economic and security interests.² Securing the Resiliency of Canada's ICT infrastructure and networks is an essential step in defending these interests.

The recognition of the importance of acting to protect economic and security interests has only been amplified with the election of Donald Trump in the United States. The shifting political environment will require Canada to enhance its economic and continental security activities so that it is not perceived or targeted as a vulnerable actor.

The Business Council of Canada called upon the federal government in 2023 to establish a national security strategy with economic security as a central component.³ Cyber and other threats to Canada's business and research infrastructure are threats to its economic security. The Parliamentary Committee on Economic Security's summary committee notes from February 2023 indicated that:

² Global Affairs Canada, "Launch of public consultations on potential new measures to advance and defend Canada's economic security interests," *Government of Canada*, last modified August 9, 2024, <https://www.canada.ca/en/global-affairs/news/2024/08/launch-of-public-consultations-on-potential-new-measures-to-advance-and-defend-canadas-economic-security-interests.html>.

³ According to the Business Council of Canada, economic security threats, "represent serious risks of substantial harm to our country as a whole – to our sovereignty, values, economy, and people. As such, they are well beyond the capacity of conventional tools [such as civil litigation] to address alone and require a coordinated national response." Examples of threats to economic security include: "mercantilism, weaponized trade, espionage, cyberattacks, malign foreign influence, and co-opted academic research." Business Council of Canada, "Economic Security is National Security: The Case for an Integrated Canadian Strategy," September 7, 2024, <https://www.thebusinesscouncil.ca/report/economic-security-is-national-security/>.

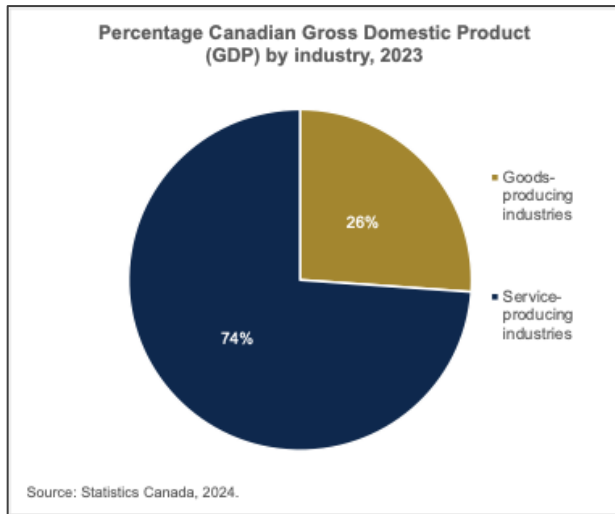
The issue of Critical Infrastructure intersects with national, cyber, and economic security. From an economic security perspective, the NS [National Security] community is most interested in those CI [Critical Infrastructure] sectors that are most vulnerable to foreign state disruption, surveillance, or control, all of which can be harmful to Canada's national security.⁴

There is a clear multi-sector emphasis on the centrality of critical ICT infrastructure for Canada's economic security. The Government of Canada's action through public consultations, while it establishes Critical Infrastructure as a priority for economic security, does not offer a coordinated and clear plan to maintain economic security in an environment of evolving geopolitical, climate, and technological risks.

Canada is a service-based economy. In 2023, nearly three-quarters of gross domestic product (GDP) by industry was service-based (Figure 1). This should make Canada and other advanced economies especially concerned with the Resiliency of ICT. From the purchasing of goods and services to the management of utilities to access to health care, mobile and broadband connectivity permeate all facets of economic and social life in Canada.

Given the central role of ICT in Canadian economic security, the ability to anticipate and absorb threats, adapt and transform, recover from disruptions, and learn from past events is crucial for those operating and leveraging connectivity infrastructure.

Figure 1



⁴ Public Safety Canada, "Parliamentary Committee Notes: Economic Security," *Government of Canada*, February 26, 2023, <https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20230929/15-en.aspx>.

Recommendation: Define ICT infrastructure Resiliency as a national issue of importance. Resources and initiatives should be aligned to support long-term strategic management and planning to protect Canada’s economic security and social well-being.

ICT Resiliency literature and ecosystem

While there are numerous recent reports, statements, and memoranda of understanding (MOU),⁵ from the outside, **it is not clear who is coordinating planning and responses in Canada. Resiliency in ICT requires a whole of government approach (beyond ISED and CRTC).** Laws, regulations, procurement practices, policy decisions, etc., have a direct influence on how Resiliency is planned and practiced.

Much of the outside literature (on engineering and communications infrastructure) is focused on designing and building Resiliency into networks. There is substantial analysis of approaches to building Resiliency to mitigate or manage certain types of risk, e.g., earthquakes, or for certain types of networks, e.g., fibre, optical. The analysis is both technical and theoretical, while leveraging lessons and case studies of actual disaster or Emergency circumstances.⁶

⁵ See for instance, Public Safety Canada, *Emergency Management Strategy for Canada: Toward a resilient 2030* (Government of Canada, 2019), <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/mrgncy-mngmnt-strtg/mrgncy-mngmnt-strtg-en.pdf>; Bell Canada, Bragg Communications Inc., Cogeco Communications Inc., Rogers Communications Canada Inc., Saskatchewan Telecommunications, Shaw Communications Inc., Freedom Mobile Inc., Tbaytel, Telestat Canada, Telus Communications Inc., Videotron Ltd., Xplornet Communications Inc., and Zayo Canada Inc., parties, “Memorandum of Understanding on Telecommunications Reliability,” *Innovation, Science and Economic Development of Canada, Government of Canada*, effective date September 9, webpage last modified December 9, 2024, <https://ised-isde.canada.ca/site/ised/en/memorandum-understanding-telecommunications-reliability>; Public Safety Canada, *Renewing Canada’s Approach to Critical Infrastructure Resilience: What we heard*, (Government of Canada, 2022), <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/rnwng-cnd-pprch-crtcl-nfrstrctr-rslnc-2022/rnwng-cnd-pprch-crtcl-nfrstrctr-rslnc-2022-en.pdf>; Canadian Centre for Cyber Security, *National Cyber Threat Assessment 2023-24*, (Communications Security Establishment, Government of Canada, 2022), <https://www.cyber.gc.ca/sites/default/files/ncta-2023-24-web.pdf>; Public Safety Canada, “Temporary National Coordination Office,” *Government of Canada*, last modified September 23, 2024, <https://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/tnco-en.aspx>; Innovation, Science and Economic Development Canada, “Canadian Security Telecommunications Advisory Committee (CSTAC),” *Government of Canada*, last modified May 13, 2024, <https://ised-isde.canada.ca/site/spectrum-management-telecommunications/en/learn-more/committees-and-stakeholders/committees-and-councils/canadian-security-telecommunications-advisory-committee-cstac>; etc.

⁶ See for instance, M. Sathurshan et al., “Resilience of Critical Infrastructure Systems: A Systematic Literature Review of Measurement Frameworks,” *Infrastructures* 7, no. 5, (Spring 2022): 67, <https://doi.org/10.3390/infrastructures7050067>; Emily M. Wells, Mariel Boden, Ilana Tseytlin, Igor Linkov, “Modeling critical infrastructure resilience under compounding threats: A systematic literature review,” *Progress in Disaster Science* 15 (Fall 2022): 100244, <https://doi.org/10.1016/j.pdisas.2022.100244>; Seyedabdolhossein Mehvar et al., “Review article: Towards resilient vital infrastructure systems – challenges, opportunities, and future research agenda,” *Natural Hazards and Earth System Sciences* 21, no. 5, (Spring 2021): 1383-1407, <https://doi.org/10.5194/nhess-21-1383-2021>; Canadian Centre for Cyber Security, *National Cyber Threat Assessment 2023-24*.

In discussions of ICT, the literature emphasizes the nodal and multi-level analysis of Emergency response, e.g., community, financial, civil, etc. There is limited consideration of the cost of Emergency response, its economic impacts, coordination of responses across borders, and how jurisdictions incent Emergency preparedness.

Given the importance of critical infrastructure, including ICT, the Government of Canada has announced strategies, convened actors, and declared commitments to protect and ensure its Resiliency. Below, Figure 2 depicts elements of the Government of Canada’s approach to ensuring the Resiliency of critical infrastructure. In Figure 3, an overview of legislation, initiatives, and actors engaged directly or indirectly in ICT Resiliency (from a federal viewpoint) is presented. The use of legislation such as the *Emergency Management Act* or *Emergencies Act* would be exceptional. It is expected that the departmental initiatives and centres engage consistently to anticipate and manage ICT risks. However, no department or center appears to take a coordinating role to ensure a whole of government approach to ICT Resiliency.

Figure 2

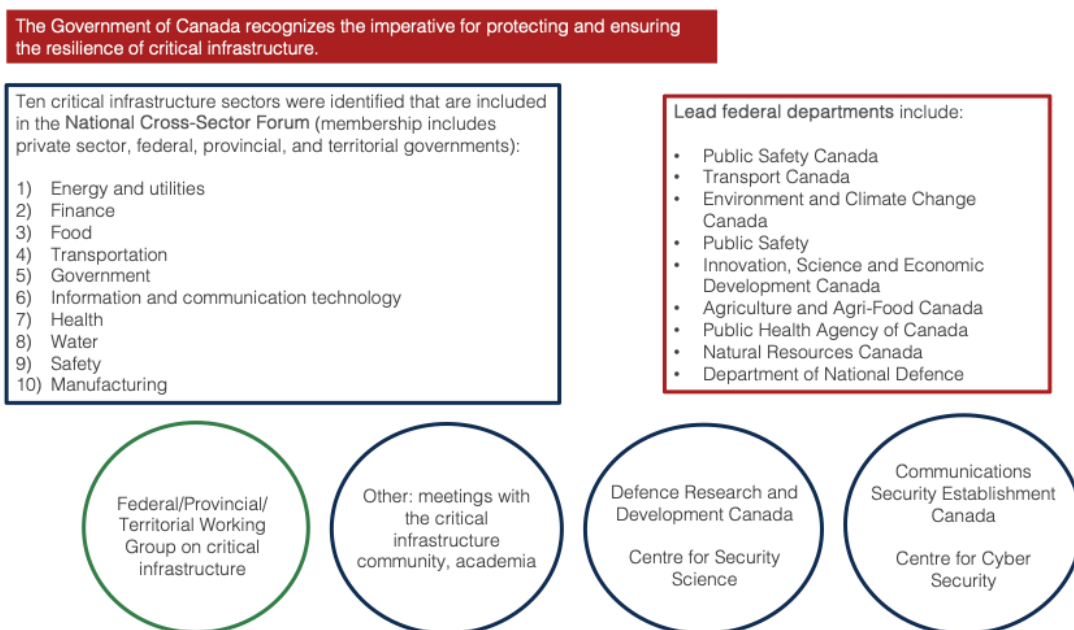
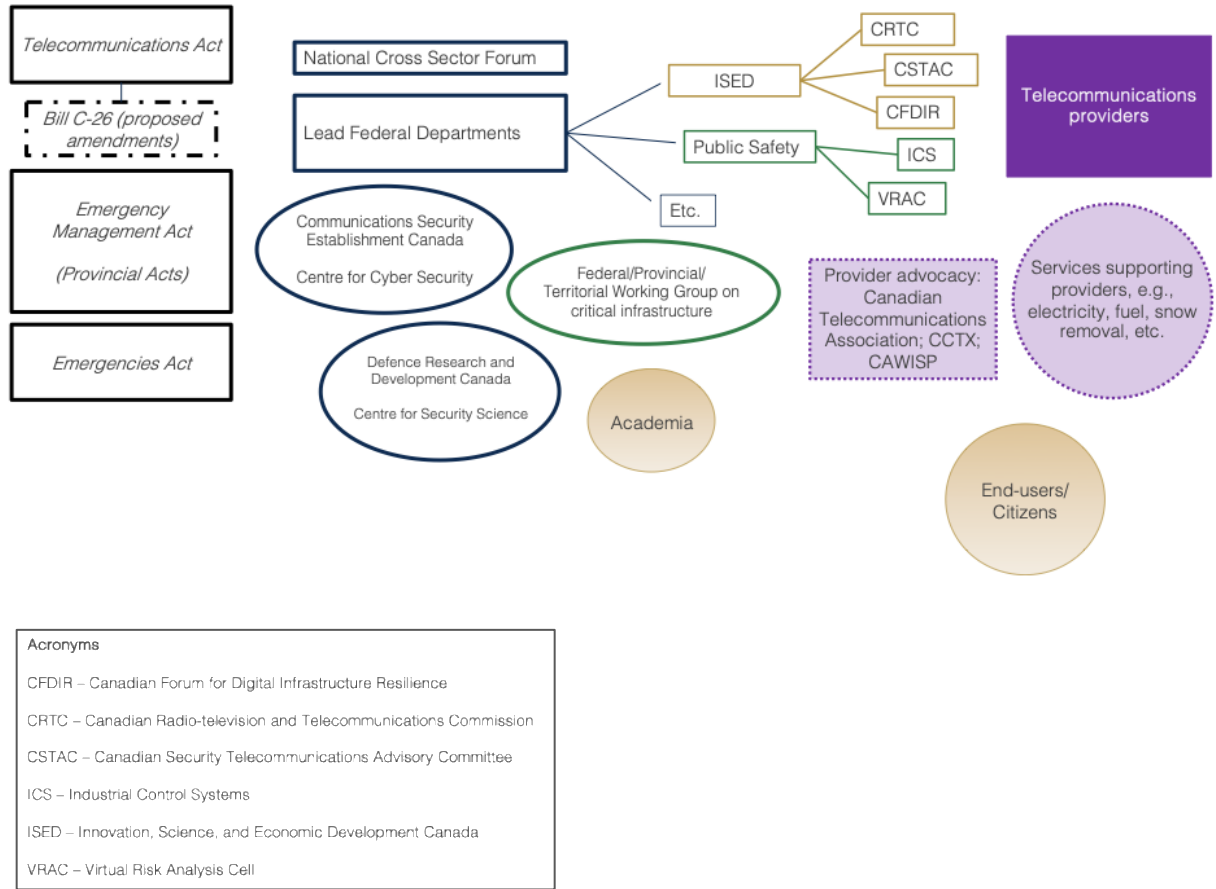


Figure 3

Canada has committed to protecting critical infrastructure. From a federal lens, ICT resilience is supported (directly and/or indirectly) by:



Existing best practices, statements, and legislation

The 2022 Memorandum of Understanding on Telecommunications Reliability (MOU) defined a protocol for shared emergency roaming during a critical network failure caused by an Emergency.⁷ In the preamble to the MOU, “the importance of telecommunications quality and resiliency” is recognized as a driver for the arrangement. In addition, a 2022 decision from regulators in the United States is referenced, identifying mobile services as “a significant lifeline” in Emergency and disaster situations that require providers to establish procedures for roaming, mutual aid, and stakeholder/public communications in Emergency circumstances. The MOU is recognition of the need to promote network Resiliency through provider collaboration in Emergency contexts.

⁷ “Memorandum of Understanding on Telecommunications Reliability,” *Innovation, Science and Economic Development Canada*.

Canada's networks are Resiliency, due to facilities-based competition, but increasing threats makes the much more challenging to maintain.

Ofcom (the United Kingdom's communications regulator) produced a guidance document on ICT reliability and Resiliency for providers required to comply with legislatively defined Resiliency-related security duties.⁸ The document defines types of risk and considerations for intervention (with the recognition that technical response will vary by provider). With an emphasis on integrating Resiliency throughout the delivery cycle (design, build, operate, maintain), Ofcom provides guidance to providers linked to concepts of infrastructure reliability and Resiliency defined through the National Infrastructure Commission. The guidance document is an example of how national standards were translated for the operations of ICT providers that Canada could emulate.

In Canada, the Canadian Telecommunications Network Resiliency Working Group (a working group of the Canadian Security Telecommunications Advisory Committee (CSTAC), produced policy recommendations in March 2023 to advance network Resiliency.⁹ There are five general recommendations: 1) establish network redundancy; 2) identify and mitigate single points of failure, e.g., geographic; 3) design physical to withstand shocks; 4) install underground cables; 5) establish business practices for rapid assessment and responsiveness. A series of more detailed recommendations for six key elements: core networks, physical structures, services and applications, internet services and infrastructure, access to networks, and processes, are included in the report. Composed of industry experts and ISED, the working group's recommendations were operator focused, but there was a call for national action and legislation to protect ICT critical infrastructure.

Bill C-26, *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts* proposes changes consistent with CSTAC's recommendation. Proposed changes include adding security to the *Telecommunications Act* as a policy objective. Amendments would authorize the Government to act to promote the security of the Canadian telecommunications system, e.g., in instances of manipulation, interference, disruption. The Minister of Industry would be empowered to issue orders to providers on the use of products/services from certain companies, the development of security plans, etc. On December 5, 2024, Bill C-26 was at its third reading in the Senate.

⁸ Ofcom, *Network and Service Resilience Guidance for Communications Providers: Guidance for communications providers on resilience related security duties under the Communications Act 2003*, (2024), <https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/272921-resilience-guidance-and-mobile-ran-power-back-up/associated-documents/network-and-service-resilience-guidance-for-communication-providers.pdf?v=385029>.

⁹ Canadian Telecommunications Network Resiliency Advisory Committee, *Telecommunications Network Resiliency in Canada: A Path Forward*, (Innovations, Science and Economic Development Canada, Government of Canada, 2023), [https://ised-isde.canada.ca/site/spectrum-management-telecommunications/sites/default/files/attachments/2023/CTNR%20Recommendations%20v1.0%20Final%20\(EN\).pdf](https://ised-isde.canada.ca/site/spectrum-management-telecommunications/sites/default/files/attachments/2023/CTNR%20Recommendations%20v1.0%20Final%20(EN).pdf).

Actions to support Resiliency and implications of decisions extend beyond ICT operators. Consider for instance, the theft of copper wire. As instances of thefts increase, localized disruptions must be addressed to maintain network Resiliency. Operators' staff, law enforcement, etc., are involved in the costly responses. Some operators recommend changing penalties in the Criminal Code and support amendments to the Telecommunications Act to increase the severity of the repercussions of the theft.

Community-level considerations should be included in Emergency management. Public service announcements, how to guides, and planning tools should be developed by government and shared. A mindset shift among citizens/end-users is needed. They will first feel the impacts of any ICT service disruptions and they should have a range of solutions to respond to them. For instance, encouraging citizens/end-users to have a generator or backup power source to ensure broadband connectivity (when power is down, internet is not necessarily down, it is that there is no power to generate the connection). Communities must have plans for their own Resiliency.

Recommendation: Convene ICT-specific operators and supporting services such as utilities, law enforcement, and recycling, to engage in information sharing and to explore opportunities for joint initiatives, including, collective training/simulation.

Recommendation: Establish or amend existing legislation to protect ICT critical infrastructure (consistent with the proposed changes in Bill C-26, e.g., adding security as a policy objective and enabling the Government of Canada to act to protect the telecommunications system, etc.) to enhance security and Resiliency.

How can Resiliency be incented?

The state is the insurer of last resort in the case of a national Emergency or crisis. This has significant public finance implications. Fostering Resiliency requires anticipating and quantifying risk. Given the complexities and unpredictability of climate change, geopolitical tensions, technical and human errors, defining all forms of risk is untenable (i.e., there is significant uncertainty surrounding the risk of Emergency that impact ICT). However, planning to respond to different circumstances and defining who is accountable is crucial.

Considering ICT Resiliency, the state, as insurer of last resort should liaise with actors and stakeholders to define, quantify, and respond to risks. Resiliency of networks and related delivery infrastructure could be incented at the front-end and back-end through two mechanisms: 1) credits, i.e., to encourage providers to apply resources to Emergency preparedness and network Resiliency; 2) response fund, i.e., resources accessible in an unforeseen circumstance with major implications.

credits

There is limited information on the costs of failed ICT Resiliency. It is challenging to quantify the cost to operators (both direct and indirect) and to consumers in an Emergency circumstance until it has passed. There are economic and social impacts to connectivity outages with quantified impacts estimated after the fact.

It would be beneficial to incent operators to build Resiliency into their networks at the front-end and in their regular operations. A credit, spending by the government by reducing or eliminating a tax (revenue) opportunity on a payer, is a potential tool to incent Resiliency.

In Canada, the six largest telecommunications firms spent approximately \$13.3B on ICT capital in 2022.¹⁰ That capital expenditure is supporting 75% of Canada's GDP, i.e., the service sector directly or indirectly. When considered in the context of sectors of economic activity, it is imperative for government to incentivize operators to build Resiliency, to test frequently, and to respond decisively to threats. This is not to say that operators are not already engaged in such activities, but there should be a clear indication of and support for industry-led initiatives for Resiliency. ICT Resiliency is essential to economic security.

Future analysis should assess the credit instrument, its terms, targets, and estimate costs. Working with industry and other users of the credit, the Government of Canada could define a spending tool to incent desired action on Resiliency in functional ways among operators. A condition to share results or practices through common forums would align to the interoperability intention in Emergency circumstances of the 2022 MOU.

Recommendation: Leverage credits to incentivize operators to invest in network Resiliency, focusing on infrastructure hardening, redundancy, and recovery.

Response fund

There is significant uncertainty surrounding ICT disasters, where there are both known unknowns and unknown unknowns. The private sector is unlikely to provide insurance for unknown threats and, even for known threats, firms are unlikely to insulate themselves from risk at socially-optimal levels. Reaching these social-optimal levels of Resiliency investments will likely require action from the Government of Canada.

ICT Resiliency requires participation from multiple actors. Given their different functions, e.g., operators, government, community, etc., an application-based fund can be a source of resources to respond to Emergency circumstances. The fund is useful in

¹⁰ The six largest firms as listed by PWC are: Bell, Rogers, SaskTel, Shaw Communications, TELUS, and Vidéotron. PWC, *Connecting Canadians through resilient networks: The impact of the telecom sector in 2022 and beyond*, (Canadian Telecommunications Association, 2023), <https://canadatelecoms.ca/wp-content/uploads/2023/11/Connecting-Canadians-through-resilient-networks.pdf>.

promoting broad-based access for a variety of actors and circumstances. A backstop for unforeseen risks in a changing environment, the fund would be a set of resources to rebuild or respond to ICT-related Emergency.

The mechanism is not as targeted as the credit but is a set of ready resources to respond to occurrences. Its broader base and reach would require assessment to estimate the appropriate capitalization.

To establish an ICT response fund, initial investment should define types of risk and their anticipated frequency. The size of the fund should be linked to the capital stock and potential economic impact of an ICT Emergency. There are noted information gaps in defining and quantifying risks associated to ICT. The Government of Canada should address these gaps as they provide a foundation for public and private action.

Sources of funding may include spectrum fees or a whole-of-society contribution, e.g., generator tax revenues, as industry taxes do not capture the breadth of impact of ICT Resiliency.

Access to the fund should be well-defined, considering the Emergency circumstances in which it may be called upon. A clear process, guidelines, and rules should be pre-established to facilitate access in chaotic situations.

There are precedents for government funds both prior to and in response to an Emergency.

To respond to Emergency, New Zealand established Natural Hazards Fund (managed by the Natural Hazards Commission Toka Tū Akean).¹¹ Resources to the fund are provided through a levy on homeowners' insurance. The fund provides "the first layer of insurance" for residential homes after a natural disaster event. Resources from the fund are also used to purchase reinsurance, manage the Commission, and undertake research and public education campaigns on Emergency preparedness. The fund is part of a broader approach in New Zealand to funding recovery following Emergency. There is a clear statement that should needs extend beyond the fund's capacity, the Crown would cover shortages as the insurer of last resort.¹²

CRTC has an application-based fund (funded through operator and other payments) for granting prior to an Emergency (see Figure 4). In the past, the focus has been on connectivity in transportation. However, public proceedings are underway by the CRTC to explore what else the fund could be supporting. There is an opportunity to repurpose the \$150M fund to focus on Resiliency.

There is a precedent for funds to incent actions and respond to occurrences federally. Consider for instance, the Broadband Fund, designed to incent operators to provide

¹¹ Natural Hazards Commission, "Natural Hazards Fund," *New Zealand Government*, accessed January 17, 2025, <https://www.naturalhazards.govt.nz/about-nhc/how-we-work/natural-hazard-fund/>.

¹² Natural Hazards Commission, "Natural Hazards Fund."

connectivity in underserved parts of the country;¹³ the On-Farm Climate Action Fund¹⁴ that provided resources to farmers to respond to climate change; or the Disaster Mitigation and Adaptation Fund¹⁵ that provided communities impacted by climate change with resources to improve natural and structural infrastructure Resiliency.

Figure 4

The CRTC's Broadband Fund¹⁶

The CRTC established the Broadband Fund to support the development of a telecommunications system that can provide Canadians with access to broadband Internet and mobile wireless services in underserved areas of Canada. In its 3rd call for applications, the CRTC focused on projects that bring mobile wireless and Internet transport infrastructure to underserved regions, and it gave special consideration to transport projects that also propose enhanced Resiliency to the telecommunications infrastructure project. In its ongoing review of the Broadband Fund Policy, which governs the funding program, the CRTC is considering providing funding to projects that propose to improve Resiliency as an eligible project type for future BBF funding.

In addition to the Broadband Fund, the CRTC is working towards enhancing the Resiliency and reliability of telecommunication networks in Canada through multiple consultations. A consultation on requirements for the reporting of major service outages has been launched with interim reporting requirements published and additional consultations are expected on a broader look at Resiliency, including measures to enhance network Resiliency.

Recommendation: Establish a taxpayer-funded response fund for Emergency that impact ICT infrastructure or networks for restoring infrastructure, enabling rapid recovery, and ensuring continuity of critical telecom services during and after events.

Recommendation: Define the data required to size ICT Resiliency risk, and align mechanisms such as standardized reporting and Emergency management frameworks to ensure informed planning and investment decisions.

¹³ Canadian Radio-television and Telecommunications Commission, "Broadband Fund: Closing the digital divide in Canada," *Government of Canada*, last modified December 12, 2024, <https://crtc.gc.ca/eng/internet/internet.htm>.

¹⁴ Agriculture and Agri-Food Canada, "Agricultural Climate Solutions – On-Farm Climate Action Fund," *Government of Canada*, last modified December 31, 2024, <https://agriculture.canada.ca/en/programs/agricultural-climate-solutions-farm-climate-action-fund>.

¹⁵ Housing, Infrastructure and Communities Canada, "Disaster Mitigation and Adaptation Fund: Overview," *Government of Canada*, August 8, 2024, <https://housing-infrastructure.canada.ca/dmaf-faac/index-eng.html>.

¹⁶ Exact text provided by CRTC.

At what cost?

Across jurisdictions, the risks of ICT require horizontal management. Executive direction on the criticality of ICT infrastructure and risk management requires collaborative responses and pricing of probability of forms of risk. That risk cannot be priced limits its likelihood for insurance (as it is being experienced with limitations on cybersecurity insurance), and complexifies state exposure as the insurer of last resort.

Threats from climate change, geopolitical tensions and nefarious actors, human error, and technological changes require long-term plans to address them. The threats are increasing and complexifying, not demurring. The costs of inaction are vast. The costs of action, spread across several years, are more manageable. This is a matter of public decision-making and expenditure allocation. If a government considers the threats serious and ICT as imperative to economic security and social well-being, actions and expenditures should align. While no amount of funding can eliminate risk, risk can be managed with appropriate planning and incented planning across groups of actors.

Dedicated public funding should be allocated through a combination of tools including credits and a response fund. credits may be appropriate for industry, but an ICT Emergency response fund may be more broadly applicable to actors in supporting services and communities.

The federal government should lead on the development of long-term holistic plans on an industry basis. With industry plans established, inter-industry collaboration and exchange should be encouraged, including through information sharing and joint initiatives such as collective training/simulation. Industry coordination would require federal bodies to emulate the coordination internally.

There is work to be done on costing risks of ICT Emergency and their responses. Immediate action is required to assess the costs of mitigation mechanisms designed to incent Resiliency, e.g., credits to operators, a response fund. Estimating these costs and impacts can be a step in building a long-term cohesive plan to managing the changing ICT threat environment.

As expenditures are aligned to priorities of ICT Resiliency, the federal government should pursue its roles in coordination, compelling, and convening to anticipate responses to ICT Emergency.

Connectivity Resiliency has broad implications for Canada's economy and national security. This roundtable highlights the need for the Government of Canada to take action to build Resiliency to climate change, cyber threats, and other Emergency that could threaten ICT infrastructure and networks. The Government of Canada can begin by defining ICT infrastructure Resiliency as a national issue. They can then work with *stakeholders, develop regulations, and enhance funding to ensure Resiliency ICT infrastructure Canada-wide.*

Glossary

Information and Communication Technologies (ICT):

“[...] refers to all communication technologies, including the internet, wireless networks, cell phones, computers, software, middleware, video-conferencing, social networking, and other media applications and services enabling users to access, retrieve, store, transmit, and manipulate information in a digital form.”¹⁷

Emergency:

““Impactful Emergency” means an urgent and critical situation that seriously endangers the lives, health or safety of Canadians, including but not limited to those arising from Accidents, cyber attacks or other deliberate malicious acts, fires, floods, storms, earthquakes, emergencies arising from domestic or international security threats, or armed conflicts involving Canada or its allies.”¹⁸

Resiliency:

“...resilient infrastructures [are] systems with [the] ability to (i) anticipate and absorb disturbances, (ii) adapt/transform in response to changes, (iii) recover, and (iv) learn from prior unforeseen events.”¹⁹

Tax credit:

For the purpose of this summary, a tax credit is an incentive that lowers the amount of tax due for individuals and firms meeting certain criteria.²⁰

¹⁷ Food and Agriculture Organizations of the United Nations, “Aims,” accessed January 28, 2025, [https://aims.fao.org/information-and-communication-technologies-ict#:~:text=Information%20and%20Communication%20Technologies%20\(ICTs,other%20media%20applications%20and%20services](https://aims.fao.org/information-and-communication-technologies-ict#:~:text=Information%20and%20Communication%20Technologies%20(ICTs,other%20media%20applications%20and%20services) See also, United Nations Education, Scientific and Cultural Organization’s International Institute for Educational Planning, “Information and communication technologies (ICT),” accessed January 28, 2025, <https://learningportal.iiep.unesco.org/en/glossary/information-and-communication-technologies-ict>; Statistics Canada, “Information and communications technology,” *Government of Canada*, last modified January 28, 2025, https://www23.statcan.gc.ca/imdb/plX.pl?Function=getThemeSub&PItem_Id=97413&PCE_Id=369&PCE_Start=01010001&cc=1.

¹⁸ “Memorandum of Understanding on Telecommunications Reliability,” *Innovation, Science and Economic Development Canada*.

¹⁹ Mehvar et al., “Review article: Towards resilient vital infrastructure systems – challenges, opportunities, and future research agenda,” 1383-1407.

²⁰ See, for instance, Government of Canada, “Common tax terms,” last modified August 23, 2024, <https://www.canada.ca/en/revenue-agency/services/tax/individuals/educational-programs/common-terms.html>.