Telecommunications Policy 49 (2025) 102914

Contents lists available at ScienceDirect

Telecommunications Policy

journal homepage: www.elsevier.com/locate/telpol

Crisis-ready telecom: Global approaches to emergency management in telecommunications

Peter Jiang [a], Joe Rowsell [b,*,1], Stephen Schmidt [b,2]

[a] *Munk School of Global Affairs & Public Policy, University of Toronto and TELUS Graduate Research Fellow, Canada*
[b] *TELUS Communications, Canada*

ABSTRACT

This paper examines the integration of Emergency Management (EM) frameworks into telecommunications regulation to address climate-driven disasters. EM principles—prevention, preparedness, response, and recovery—offer a structured approach to strengthen telecom networks and manage crises. By analyzing international practices, the study identifies critical gaps in funding, coordination, and regulatory alignment, highlighting opportunities to align telecom policy with EM planning. The findings provide actionable recommendations to foster cross-sector collaboration, promote regulatory flexibility, and enhance infrastructure resilience in an increasingly interconnected and disaster-prone world.

> "True cyber resilience doesn't stop at infrastructure … Now more than ever, we need an integrated approach that strengthens legal frameworks, builds capacity, and fosters international cooperation."
>
> —Doreen Bogdan-Martin, ITU Secretary-General (2024)

> "Emergency management is not a static end-state; it requires ongoing adaptability, flexibility, and improvement."
>
> —Public Safety Canada (2017)

1. Introduction

In an increasingly interconnected world, telecommunications network resilience is critical for public safety and national security. Over the past decade, climate change has driven a 40% global increase in extreme weather events (UN Office for Disaster Risk Reduction, 2023). In the U.S. alone since 1980, natural disasters related to higher temperatures such as droughts, floods, heatwaves, and wildfires have contributed to $2 trillion USD in economic costs and more than 15,000 disaster-related deaths (Bhola et al., 2023). Wildfires, in particular, have become a significant global concern. The 2023–2024 fire season saw record-breaking emissions globally, driven by events such as unprecedented wildfires in Canadian boreal forests, deadly incidents in Hawaii and Chile, and the largest recorded wildfire in the European Union (Matthew et al., 2024).

The escalating frequency and severity of natural disasters—ranging from record-breaking wildfires to devastating

This article is part of a special issue entitled: Resilience published in Telecommunications Policy.

[*] Corresponding author.

E-mail address: joe.rowsell@telus.com (J. Rowsell).

[1] The opinions expressed in this content are solely those of the author and do not reflect the views or beliefs of TELUS or its affiliates.

[2] The authors would like to acknowledge Peter Anderson, Eric Edora, John Gannon, Stanford Levin, David Peaker, Georg Serenstchy, and Ramon Zuluet for their time and valuable insights on the topics and draft versions of this paper.

https://doi.org/10.1016/j.telpol.2025.102914
Received 30 September 2024; Received in revised form 23 January 2025; Accepted 25 January 2025
Available online 13 March 2025

floods—underscore the need for robust communication infrastructure capable of withstanding crises. As climate change intensifies, a structured and comprehensive approach to resilience becomes imperative. The Emergency Management (EM) framework offers a promising model, systematically organizing efforts across four interconnected stages: prevention, preparedness, response, and recovery. Each phase delineates specific tasks and responsible actors, providing a roadmap for enhancing the resilience of critical infrastructure.

Yet integrating EM frameworks into telecom regulation presents significant challenges. Regulators often operate with exclusive authority over telecommunications but lack collaboration with emergency management agencies or local governments. This siloed approach hinders the integrated planning and execution necessary for effective EM. Traditional command-and-control models, characterized by quasi-judicial “once-and-done” proceedings, limit the iterative, collaborative processes required for resilience planning. Additionally, regulatory bodies often lack the skills and frameworks needed for deep coordination across government levels and with private sector partners.

Facilities-based competition supports telecommunications resilience by incentivizing duplication of facilities and network infrastructure. Providers compete on resiliency-related attributes such as coverage, reliability, redundancy, and infrastructure diversity. This competition drives investment in competing networks and technological advancements, reducing the risk of cascading failures. Properly regulated, competitive markets deliver faster recovery and greater resilience than monopolistic or state-controlled systems. However, markets may fall short in underserved remote and rural areas where investments are less viable. Targeted government interventions, such as subsidies and tax incentives, can bridge these gaps, complementing private-sector efforts to extend competitive service to remote and rural areas. Effective policies must promote competition while incentivizing long-term investments that enhance infrastructure resilience. These policies should ensure that the benefits of robust and reliable networks extend to underserved areas, addressing gaps in coverage and ensuring all communities have access to critical communications during crises.

This paper explores the integration of EM frameworks into global telecommunications resiliency, examining current initiatives, international best practices, and regulatory challenges. It offers recommendations to strengthen funding strategies, align policies, enhance coordination, and promote regulatory flexibility. By assessing the strengths and weaknesses of existing resiliency frameworks, evaluating EM frameworks’ potential to improve telecom resilience, and providing actionable guidance for policymakers and regulators, the paper advances the discourse on telecom resilience. As climate change and digital transformation reshape the global landscape, building robust and adaptable networks remains an urgent priority.

2. Literature review

The integration of Emergency Management (EM) frameworks into telecommunications resilience bridges economic policy, regulatory strategy, and technological innovation. As climate-driven disasters and cyber threats escalate, resilience must be viewed as a quasi-public good—essential to public safety and economic stability but underprovided by market forces. This review synthesizes key theoretical and empirical insights to explore the systemic challenges of resilience and inform effective policy interventions.

2.1. Market resilience through investment and public-private collaboration

Facilities-based competition supports telecommunications resilience by driving investment in competing networks, infrastructure diversity, and redundancy. Providers compete on key attributes such as coverage, capacity, reliability, and performance, which incentivizes network hardening and technological innovation. This basis of competition ensures that disruptions in one network are less likely to cascade across the system. Empirical studies demonstrate that countries with robust facilities-based competition achieve faster recovery times and greater service continuity during crises compared to those reliant on single-network models or monopolistic systems (Gannon, 2023; Serentschy, 2024). Properly regulated, competitive markets can therefore play a central role in enhancing telecommunications resilience.

Canada provides a strong example of how facilities-based competition fosters resilience. Its telecommunications sector features multiple independent networks operated by ILECs, cable providers, and wireless operators, creating a dense and diverse infrastructure. This diversity ensures system robustness, as redundancy across parallel networks allows critical communications to continue even when one system experiences outages. For instance, the competitive landscape encourages providers to differentiate themselves by investing in resilience, improving recovery capabilities and service reliability. As a result, Canada’s telecommunications infrastructure is considered more resilient than that of many countries with less-developed competitive frameworks (Schmdit et al., 2017).

However, the resilience benefits of competition can be undermined by poorly designed regulatory policies. Spectrum allocation without deployment requirements or mandated roaming and MVNO access without infrastructure obligations may reduce incentives for operators to build and maintain independent networks. In Canada, such policies risk concentrating traffic on fewer networks, thereby increasing systemic vulnerabilities. Policymakers must ensure that regulatory frameworks support infrastructure diversity and investment while maintaining competition. Balancing these goals is critical to preserving the resilience advantages of facilities-based competition.

While facilities-based competition drives resilience in many environments, market forces often fall short in two key contexts: remote and rural areas and regions requiring systematically hardened networks. In remote and rural areas, the low population density and high costs of deployment—such as building towers, transport infrastructure, and power generation—make it economically unviable to serve customers with even a single network, let alone multiple redundant networks or hardened infrastructure. Similarly, in regions facing extreme environmental risks, such as areas prone to wildfires, flooding, or hurricanes, the economic incentive to invest in layers of duplication and advanced hardening is often insufficient without external support. Government interventions, such as subsidies, tax incentives, and public-private funding programs, are essential to bridge these gaps. Programs like Canada's Universal Broadband Fund illustrate how targeted public investments can complement private-sector efforts, extending resilient infrastructure to underserved regions and ensuring equitable access to reliable communications.

Effective funding models address these challenges through risk-sharing mechanisms that align public and private incentives. The literature identifies three successful approaches: direct public investment, matched funding, and incentive-based mechanisms (Fabre & Straub, 2023). For example, Australia's Mobile Network Hardening Program demonstrates the impact of matched funding, leveraging public resources to stimulate private investment. Similarly, Japan's sustained infrastructure investments highlight the effectiveness of multi-year commitments to building resilient networks. Dedicated funding streams tied to clear performance metrics and long-term planning yield the best outcomes. Comparative studies across OECD countries reveal that nations with dedicated resilience funding experience faster recovery times and higher levels of infrastructure hardening (Gannon, 2023).

2.2. Cross-sector, flexible, and dynamic approaches to resilience

Effective telecommunications resilience depends on integrating cross-sector collaboration, flexible response mechanisms, and dynamic learning systems (Linkov & Trump, 2019; Brown et al., 2017; von Lubitz et al., 2008; Kunreuther & Michel-Kerjan, 2013). These interconnected pillars ensure networks can withstand disruptions, adapt to evolving risks, and continuously improve.

Sectoral regulation

Sectoral regulation directly influences investment, deployment, adoption, and innovation. Well-designed regulatory frameworks can incentivize network expansion, encourage infrastructure diversity, and ensure operators prioritize resilience as a key component of their operations. Conversely, poorly conceived regulations may stifle investment, exacerbate vulnerabilities, and reduce the sector's overall ability to withstand and recover from disruptions.

Cross-sector coordination

Coordination across critical infrastructure sectors—such as energy, transportation, and emergency services—is vital for optimizing resources and minimizing cascading failures. South Korea's Safe-Net program exemplifies this integration, enabling seamless communication between telecom operators and first responders. The EU's NIS-2 Directive offers another example, fostering regulatory frameworks that align telecommunications resilience with broader critical infrastructure protections while allowing regional variations.

Flexible response mechanisms

Adaptability is critical in responding to diverse and unpredictable crises. Scalable resource allocation systems, adaptable regulatory frameworks, and evolving technical standards are essential for maintaining operational continuity during disruptions. Flexible approaches ensure telecom providers can respond dynamically to both anticipated risks, such as hurricanes, and emergent challenges, like cyberattacks.

Dynamic learning systems

The unpredictability of modern risks necessitates continuous learning and adaptation. Systematic post-incident analyses, stakeholder feedback mechanisms, and regular updates to risk assessments are critical components of resilience governance (Linkov & Trump, 2019). These mechanisms enable networks to evolve alongside technological advancements and emerging threats, ensuring sustained resilience.

Consumer behavior and market information

Consumer behavior plays a pivotal role in driving resilience outcomes within telecommunications markets. However, systemic biases—such as choice overload, status quo bias, and present bias—often hinder optimal decision-making (Thaler & Sunstein, 2021). These biases reduce consumer engagement with resilience metrics and diminish competitive pressure for providers to invest in robustness.

Behavioral interventions offer promising tools to address these challenges. Standardized resilience metrics—including comparable scores, clear outage histories, and performance benchmarks—make complex risk assessments more accessible. Choice simplification tools, such as structured comparison platforms and default options, reduce cognitive overload and empower consumers to make informed decisions. Smart disclosure mechanisms—like regular performance reports, proactive service alerts, and personalized usage analysis—maintain consumer awareness and engagement over time (Ariely & Holzwarth, 2017).

The literature also emphasizes the role of switching costs in shaping market efficiency. Simplifying administrative processes, such as number portability and contract termination, increases consumer mobility and encourages competition on quality metrics. Markets with lower switching costs show higher resilience standards, as providers are incentivized to differentiate themselves through network robustness and reliability.

2.3. Summary

The literature underscores the necessity of integrating EM frameworks into telecommunications resilience to address market failures, align incentives, and enhance systemic coordination. Effective approaches balance public and private priorities, leveraging adaptive governance and targeted funding to build robust networks. These findings provide a foundation for policy recommendations, emphasizing the need for regulatory innovation and collaborative mechanisms to navigate climate-driven risks and evolving market dynamics.

3. Emergency management frameworks

3.1. Phases of Emergency Management

EM frameworks provide a structured approach for addressing crises, offering a continuous cycle of prevention, preparedness, response, and recovery. For telecommunications resilience, these phases ensure that networks can withstand, adapt to, and recover from emergencies. By adopting such a holistic framework, regulatory bodies can shift from reactive to proactive, enhancing the resilience of telecommunications infrastructure against both natural and human-made disasters (ITU, 2024; OECD, 2022).

As shown in Fig. 1, the EM framework typically consists of four interconnected phases.

- **Prevention/Mitigation:** Actions aimed at reducing or eliminating risks before they manifest. In telecommunications, this might involve investing in redundant infrastructure or fire-proofing telecom equipment in high-risk areas (Coppola, 2020).
- **Preparedness:** Activities and measures taken beforehand to ensure readiness for emergencies. This includes emergency drills, establishing communication protocols, and stockpiling resources to maintain service continuity (Coppola, 2020).
- **Response:** Immediate actions taken during an emergency to minimize damage and protect lives. In telecom, this could involve deploying mobile communication units or rerouting traffic through unaffected networks (ITU, 2024).
- **Recovery:** Efforts to restore normal operations after a disaster. This might involve repairing damaged infrastructure or rebuilding it to be more resilient to future threats (ITU, 2024; Comfort et al., 2010).

These phases form a continuous cycle, where lessons learned from each event inform future prevention and preparedness efforts (ITU, 2020). This cyclical approach emphasizes continuous improvement, which is vital for addressing the complex and evolving nature of telecommunications resilience in the face of increasing climate and cyber risks.

3.2. Application of EM to telecommunications resiliency

The integration of EM frameworks into telecommunications is crucial to ensuring the resilience of critical infrastructure in the face of increasing natural disasters and other emergencies. This section explores how EM principles can be effectively applied to telecommunications, drawing from successful examples in Canada, the United States, and the European Union.

1. Prevention/Mitigation

In this phase, the focus is on reducing the likelihood and impact of potential disasters. For telecom networks, this involves investing in infrastructure hardening, creating redundancy, and adopting robust design standards. Regulatory bodies can play a critical role by monitoring these standards and providing incentives for private sector investment in resilient technologies.

Fire-Smarting, Seismic Hardening, and Flood-Proofing Sites: In Canada, telecom operators have implemented fire-smarting practices by clearing vegetation and biofuels around wireless towers to mitigate wildfire risks. In earthquake-prone areas, operators have adopted seismic hardening techniques, reinforcing buildings and structures to withstand seismic activity. Additionally, to mitigate the impact of floods, telecom operators have adopted flood-proofing strategies, such as elevating radio access network (RAN) equipment and other essential hardware above projected flood levels. These proactive measures reduce the vulnerability of telecom infrastructure during extreme weather events, ensuring critical systems remain operational during disasters.

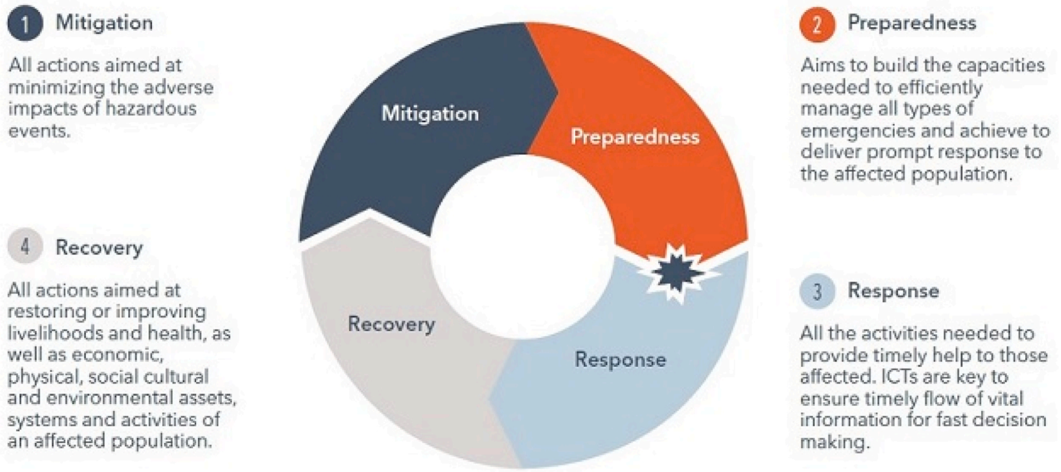
1 Mitigation
All actions aimed at minimizing the adverse impacts of hazardous events.
2 Preparedness
Aims to build the capacities needed to efficiently manage all types of emergencies and achieve to deliver prompt response to the affected population.
3 Response
All the activities needed to provide timely help to those affected. ICTs are key to ensure timely flow of vital information for fast decision making.
4 Recovery
All actions aimed at restoring or improving livelihoods and health, as well as economic, physical, social cultural and environmental assets, systems and activities of an affected population.
Mitigation
Preparedness
Response
Recovery

Fig. 1. Phases of emergency management (ITU, 2024).

2. Preparedness

Preparedness involves ensuring that both telecom providers and regulatory bodies are ready to respond effectively to emergencies. This includes developing emergency protocols, conducting regular drills, and fostering public-private partnerships to maintain operational readiness.

One of the most critical aspects of preparedness is the creation of comprehensive emergency playbooks that outline roles, responsibilities, and protocols for telecom providers during disasters. For example, in the United Kingdom, regular joint emergency drills between telecom providers and government agencies have been pivotal in fine-tuning responses to emergencies. Similarly, in the United States, the Federal Communications Commission (FCC) coordinates nationwide disaster preparedness exercises with telecom operators, ensuring alignment between public and private sectors. These drills help to identify gaps in response capabilities and ensure that real-time coordination occurs during an actual disaster.

Another key aspect of preparedness is working with provincial/territorial and local authorities to secure access for positioning and/or refueling backup generators, as well as to carry out repairs. Ensuring that telecom providers can quickly reach damaged sites to refuel generators and restore service is crucial during emergencies when commercial power is lost. This collaboration is essential to maintaining continuous service during prolonged outages.

3. Response

The response phase involves the immediate actions taken during an emergency to minimize its impact. For telecom operators, this includes ensuring continuity of services, providing real-time information to first responders, and coordinating with government agencies to expedite recovery efforts.

In the US, during Hurricane Sandy in 2012, telecom operators such as AT&T and Verizon applied mitigation strategies by prepositioning mobile cell towers and deploying backup generators. Their coordination with the Federal Emergency Management Agency (FEMA) allowed for quick recovery and minimized disruptions. Redundancies can also exist at the response level like These actions highlight the importance of pre-positioned infrastructure in maintaining telecom services during emergencies.

In Germany, in response to severe floods in 2021, Deutsche Telekom's preparedness efforts included comprehensive emergency protocols and close collaboration with emergency management agencies. The rapid deployment of temporary cell towers and the rerouting of traffic through unaffected networks exemplified the importance of preparedness in maintaining telecom services during emergencies. Redundancies can and should also exist during the response phase. For example, France's Réseau Radio du Futur (RRF) incorporates redundancy strategies like backup radio frequencies and failover systems to ensure continuous communication for emergency responders even when parts of the network are compromised (Richard et al., 2024). The RRF further prioritizes emergency communication traffic over commercial use, maintaining seamless connectivity in critical moments.

4. Recovery

The final phase focuses on restoring telecom services to their full capacity and learning from the event to improve future resilience. This includes repairing damaged infrastructure, assessing the effectiveness of the response, and updating regulatory frameworks as necessary. Intergovernmental and interagency collaboration is crucial in informing recovery strategies and strengthening network resilience during this phase.

A notable example of effective recovery in Canada occurred when TELUS rebuilt wildfire-impacted communities using fibre instead of copper. Fibre networks are more resilient and less prone to damage, which not only restored services but improved the long-term durability of telecom infrastructure in the affected regions.

In cases where multiple jurisdictions and critical infrastructure dependencies exist, coordination is crucial. For instance, restoring aerial fibre and wireline facilities that are co-located on other utilities' infrastructure, such as power poles, often depends on the replacement of those poles. Similarly, when telecom infrastructure is situated along transportation corridors (e.g, railways, highways) impacted by floods or landslides, restoration efforts are contingent on repairs to the transportation infrastructure. An example of best practices in post-disaster telecom recovery within the EU is highlighted by the emphasis on "building back better" during infrastructure reconstruction (ITU, 2020a; ITU, 2020b). This approach ensures that the telecommunications network is not only restored but improved to withstand future disasters.

One key recommendation is to assess weaknesses in the damaged infrastructure immediately after a disaster. This process helps identify vulnerabilities that might have been overlooked during initial construction. For instance, replacing overhead cables with underground ones can make the system more resistant to wind and temperature extremes, although it may introduce new challenges such as longer repair times. Moreover, digital twinning is an emerging technology being integrated into reconstruction efforts. By creating virtual models of physical telecom networks, operators can simulate various disaster scenarios and improve real-time monitoring and control capabilities. This enhances both immediate recovery and long-term resilience of the infrastructure.

The Post-Disaster Needs Assessment framework is another best practice, enabling telecom providers and governments to estimate the costs and scope of rebuilding efforts while prioritizing modern, resilient technologies. This approach was crucial in Europe following disasters like floods and wildfires, where the focus was on deploying redundant systems and integrating cutting-edge technology to future-proof networks against similar events.

The application of EM frameworks to telecommunications is not just a theoretical proposition; it represents a strategic and empirically validated approach to bolstering network resilience. These international examples illustrate the tangible benefits of integrating EM principles into telecom regulation. The consistent success across diverse settings highlights the universal importance of preparedness, coordination, and robust infrastructure. The next section delves into the key attributes that make these EM frameworks effective, offering a blueprint for enhancing telecom resilience globally.

3.3. Key attributes of effective EM frameworks in telecommunications

An effective EM framework in the telecommunications sector requires several key attributes to enhance network resilience. Below is a list of seven key attributes, supported by academic literature and government reports, as well as international examples:

1. **Holistic Integration Across the EM Cycle:** Effective EM frameworks must integrate all four phases—prevention/mitigation, preparedness, response, and recovery—across all levels of government and society. This comprehensive approach ensures that every stage of emergency management is addressed systematically, promoting resilience and reducing the risk of failure during crises. The ITU's National Emergency Telecommunications Plan similarly emphasizes the importance of comprehensive planning that addresses all disaster phases to ensure continuous communications during emergencies (ITU, 2024; OECD, 2014). Such integration is crucial for building resilient systems that can adapt and respond effectively to various threats
2. **Comprehensive Coordination:** Collaboration among federal, provincial, local, and Indigenous governments, along with private sector partners, is vital for effective emergency response. Even in countries where clear EM frameworks are established with clear roles to reduce confusion and overlap, approaches can vary by province and municipality, complicating efforts for national telecom providers. As noted by OECD guidelines on cross-border cooperation in emergency telecommunications, international collaboration across jurisdictions is also critical for maintaining service continuity during transnational disasters (2022).
3. **Clearly Defined Roles and Responsibilities:** Establishing clearly defined roles, considering legislative and institutional competencies, is essential for effective emergency management. The Sendai Framework for Disaster Risk Reduction 2015–2030, a global strategy adopted by the United Nations, emphasizes the importance of governance and institutional frameworks in managing disaster risks effectively. It prioritizes the identification of risks, fostering collaboration across sectors and levels of government, and building resilient infrastructure to minimize disaster impacts (UNISDR, 2015). This clarity in roles enables swift and coordinated actions during crises. Similarly, the ITU's guidelines for managing emergency telecommunications highlight how delineating responsibilities ensures seamless cross-agency collaboration during emergencies (ITU, 2024).
4. **Flexibility and Adaptability:** EM frameworks must be designed to remain effective in the face of evolving threats and technological changes. This requires the capacity to adjust to various types of emergencies, from natural disasters to cyberattacks, ensuring their relevance across a wide spectrum of potential disruptions to telecommunications networks. Coppola's Introduction to International Disaster Management highlights the importance of flexibility in EM frameworks, emphasizing the need for constant updates in light of emerging risks such as climate change and cybersecurity threats (2021; OECD, 2014).
5. **Risk-Based Approach:** A risk-based approach prioritizes resources based on risk assessments, focusing efforts for maximum impact. The OECD's disaster risk assessment reports stress the need for governments to establish national standards for hazard mapping and infrastructure resilience against extreme weather events (OECD, 2022). Without these, telecom networks may remain vulnerable to climate-induced disasters.
6. **Continuous Learning and Improvement:** Mechanisms for continuous learning and improvement are critical for robust EM frameworks. Through ongoing evaluations, after-action reviews, and the integration of new research and best practices, these frameworks evolve over time, becoming increasingly sophisticated and effective in addressing the complex challenges of telecommunications resilience. The ITU and OECD guidelines stress the importance of regular training, audits, and system upgrades as part of an evolving approach to disaster management (ITU, 2024; OECD, 2022). This continuous improvement ensures that lessons learned from previous emergencies inform future preparedness efforts.

3.4. Fund network resilience: A foundational Prerequisite

While effective EM frameworks rely on attributes such as coordination, adaptability, and risk-based planning, these qualities cannot be implemented without sustainable funding. Resilience-building measures—including infrastructure hardening, redundancy creation, and recovery system deployment—require significant financial investments. However, resilience, like other quasi-public goods such as education or research and development, is often underprovided by market forces. The social benefits of resilience, such as enhanced public safety and economic stability, far exceed the private benefits realized by individual operators. This misalignment of incentives discourages sufficient private investment, leading to chronic underprovision.

Government intervention is essential to bridge this gap. Public funding mechanisms, such as subsidies, tax credits, and dedicated resilience funds, play a pivotal role in reducing financial barriers and incentivizing private-sector investments. International examples underscore the importance of funding: Australia's STAND program targets high-risk areas with grants to support infrastructure hardening, while the EU Solidarity Fund provides critical post-disaster recovery resources. Public-private partnerships further enhance efficiency, ensuring resources are directed to projects with the greatest impact.

By embedding funding as a foundational element, EM frameworks empower telecommunications stakeholders to proactively address vulnerabilities, enhance preparedness, and facilitate recovery in an increasingly disaster-prone world. Sustainable funding transforms the theoretical attributes of EM into actionable, impactful measures, aligning private incentives with public needs and enabling resilience at a scale that benefits society as a whole.

The integration of these key attributes into EM frameworks for the telecommunications sector is crucial for building resilient networks capable of withstanding a wide range of emergencies. However, the effectiveness of these attributes depends on how well they are implemented within the specific regulatory and operational contexts of each country.

3.5. Challenges in Applying EM to telecommunications regulation

While the EM framework offers significant potential for enhancing telecommunications resiliency, its application in regulatory contexts presents several challenges (see Table 1). Telecommunications regulators are not first responders and are traditionally accustomed to a command-and-control rule-making model, which differs from the collaborative approach required in EM. Telecommunications regulation, when conceived of and practiced as a policing power, classically involves the development, application and enforcement of rules, by a quasi-judicial regulatory authority, against industry actors. However, effective EM in telecommunications requires deep collaboration with private sector operators and other stakeholders, which can be challenging within traditional conceptions of regulatory practice. Effective EM in telecommunications underlines the importance of alternative conceptions of regulation (collaboration vs. control; share responsibility vs. unitary authority; ongoing involvement vs. point in time decisional interventions; etc.).

Shared accountability for Emergency Management (EM) versus exclusive telecom jurisdiction poses significant challenges. In many countries, authority over telecommunications is concentrated within a single regulatory body or ministry. However, natural disasters—floods, fires, earthquakes—are total and cross-cutting, causing destruction without regard to jurisdictional boundaries or the neatness of departmental mandates. These events necessitate coordinated responses and shared accountability across all levels of government and public safety organizations, requiring a collaborative approach that extends beyond traditional telecom regulation (Galasso et al., 2022).

This accountability is particularly critical in dense urban areas, where interconnected infrastructure systems amplify cascading failures. Incorporating resilience into urban planning is essential for minimizing disruptions and ensuring coordinated recovery efforts. Canada's emergency initiatives, such as ISED's RETOs and essential services letters—facilitating telecom employees' mobility during wildfires—demonstrate how gaps between telecom providers and emergency services can be bridged. Expanding such collaboration will be key to embedding EM principles more comprehensively into telecom governance.

Despite these challenges, telecom regulators have a critical role to play in EM, particularly in the areas of prevention and mitigation, preparedness, response, and recovery. The following table outlines the specific roles and actions that telecom regulators can take during each phase of the EM cycle.

By understanding these challenges and the core principles of EM frameworks, telecommunications regulators can better navigate the complexities of enhancing network resilience. The following section will explore international best practices and specific recommendations for integrating EM principles into telecommunications regulation.

4. International comparisons and best practices

This section examines how various countries have integrated the 4-phase EM framework into their telecommunications resilience efforts, along with select initiatives that fall outside this framework that merit discussion. Table 2 provides a summary of these efforts in the United States, the United Kingdom, Australia, Japan, and the European Union.

4.1. United States

The U.S. has deeply integrated the 4-phase EM framework into its telecommunications resilience strategy, primarily through the FEMA and the FCC.

- **Prevention/Mitigation**: The FCC's Communications Security, Reliability and Interoperability Council (CSRIC) develops best practices for network hardening and risk reduction (FCC, n.d.).

Table 1
Role of telecom regulators in emergency management.

EM Phase	Role of Telecom Regulators
Prevention and Mitigation	- Fund network resilience. - Promote facilities-based competition (multi-operator, multi-platform) as a primary defense against resilience risks. - Awareness and education initiatives to inform the public and businesses about enhancing telecom resilience.
Preparedness	- Formally adopt an EM framework approach. - Collaborate with industry to develop EM playbooks and continuity plans. - Proactively engage with local and provincial EM stakeholders, ahead of emergencies.
Response	- Real-time coordination amongst first responders, local governments, and operators—to protect, restore, and operate telecom facilities during an emergency. - Establish funding mechanisms to help critical infrastructure providers recover the costs of deploying temporary solutions such as mobile wireless towers during emergencies.
Recovery	- Support restoration of services with resilience funding and regulatory flexibility (accelerated approvals, suspended rules, streamlined reporting).

- **Preparedness**: The Integrated Public Alert and Warning System (IPAWS) ensures readiness for emergency communications (FEMA, April 2024).
- **Response**: The Disaster Information Reporting System (DIRS) facilitates rapid information sharing during crises through a single, coordinated process (FEMA, March 2024).
- **Recovery**: The FCC's Disaster Response and Recovery Working Group focuses on restoring communications post-disaster.
- **Unique Initiative**: The First Responder Network Authority (FirstNet) is a dedicated, nationwide broadband network for emergency responders (FirstNet, n.d.) implemented in 2012. This public-private partnership model is operated through AT&T's network and offers a level of dedicated infrastructure to first responders and public safety workers.

4.2. Canada

Canada faces unique challenges in telecommunications resilience due to its vast geography, dispersed population, and system of federalism. While several initiatives have been launched, significant gaps remain, particularly in the integration of EM principles into telecommunications regulation and policy.

- **Prevention/Mitigation:** Canada's approach to telecommunications resilience is mainly supported by the Universal Broadband Fund (UBF) and the Canadian Radio-television and Telecommunications Commission (CRTC) Broadband Fund, which focus on network expansion in underserved areas (CRTC, 2023). However, Canada lacks specific standards for telecom adaptation to climate change. To address this, funding programs like the UBF and CRTC could help providers to meet resiliency targets, such as conducting Hazard, Risk, and Vulnerability Assessments (HRVAs) and implementing backup power systems. ISED could also introduce resiliency requirements for spectrum authorizations, similar to existing environmental impact assessments.
- **Preparedness:** Canada's Alert Ready system serves as the national public alerting platform, enabling authorities to warn citizens about emergencies through multiple communication channels (CRTC, 2024; Pelmorex Corp, 2022). While effective within national borders, it lacks cross-border coordination, unlike the EU's EU-Alert system. Given Canada's proximity and interconnectedness with the U.S., enhancing cross-border alerting and emergency communication systems is an opportunity to strengthen preparedness for large-scale, transnational disasters like wildfires.
- **Response:** Canada's response capabilities in telecommunications during emergencies are largely coordinated by Public Safety Canada in collaboration with a sub-group of CSTAC, Canadian Telecommunications Emergency Preparedness and Management (CTEPM), composed of EM and business continuity planning professionals.
- **Recovery:** Currently, Canada lacks a dedicated fund for the recovery of telecommunications infrastructure post-disaster. In contrast, the EU Solidarity Fund offers financial support for restoring essential infrastructure, including telecommunications, after major disasters. Establishing a similar fund in Canada could provide crucial financial resources for rebuilding and enhancing telecom resilience, particularly in rural and remote areas where recovery is more challenging. Additionally, Canada lacks a mechanism to recover response costs, such as the deployment of mobile towers and provisioning of equipment and services to EOCs.
- **Unique Initiative:** A major initiative currently underway is the Public Safety Broadband Network (PSBN), which has been under development for over 13 years (Department of National Defense, 2024). The PSBN would be a mobile communications network specifically designed for first responders and others working in public safety roles, such as search and rescue, military, and transportation operations. Once implemented, it would allow first responders in Canada to communicate beyond push-to-talk radios and utilize new technologies, applications and services on a secure high-speed network.

4.3. United Kingdom

The UK's approach, led by the Office of Communications (Ofcom) and the Cabinet Office, shows strong alignment with the 4-phase EM framework.

- **Prevention/Mitigation**: Ofcom's network resilience requirements mandate risk assessments and mitigation strategies that are generally more comprehensive than its peers as a result of the UK's Telecommunications (Security) Act of 2021.
- **Preparedness**: The Electronic Communications Resilience & Response Group (EC-RRG) has operated a MOU between telecommunications providers on mutual assistance during emergencies since as early as 2010 (Department for Digital, Culture, Media & Sport [DCMS], 2010).
- **Response**: In addition to being a forum of telecommunications stakeholders, the EC-RRG is also involved in coordinating industry responses during emergencies as well as site visits and debriefing after incidents (DCMS, 2022). The National Emergency Plan for Telecommunication outlines the UK's strategy for responding to emergencies that impact telecommunications infrastructure. It includes provisions for maintaining service continuity, such as rerouting calls and ensuring backup power supplies. It also highlights the need for regular stress testing of backup systems to ensure functionality during a crisis (OfCom, 2020).
- **Recovery**: Ofcom's has proposed significant resilience guidelines for providers, that includes a structured approach to service restoration (Ofcom, 2023). Its expected that Ofcom will publish next steps on these guidance measures by summer 2024.
- **Unique Initiative**: The Mobile Telecommunications Privileged Access Scheme (MTPAS) is a system designed to give priority access to cellular networks for authorized emergency responders during times of crisis or network congestion (Cabinet Office of the United

Kingdom, 2021). MTPAS contributes to telecommunications resilience by ensuring that critical communications for emergency responders are maintained during crises, when normal cellular networks might be congested or partially compromised.

4.4. *Australia*

Australia has made significant strides in incorporating the EM framework into its telecommunications resilience strategy.

- **Prevention/Mitigation**: The Telecommunications Sector Security Reforms (TSSR) focus on identifying and mitigating national security risks (Department of Home Affairs, n.d.). This legislative framework includes mandatory security obligations and reporting requirements rather than guidelines.
- **Preparedness**: The Trusted Information Sharing Network (TISN) facilitates collaboration between government and critical infrastructure sectors (Department of Home Affairs, 2024). The TISN has a broad scope across all critical infrastructure owners and operators, as well as academic and research institutions.
- **Response**: Developed by an Australian industry body the Telecommunications Emergency Communications Protocol outlines coordinated response procedures (Communications Alliance LTD, 2022). It clearly outlines the process through the four EM phases, followed by a fifth phase of reporting.
- **Recovery**: TISN's Critical Infrastructure Resilience Strategy includes specific recovery planning for the telecommunications sector, with deep integration in its EM framework (Department of Home Affairs, 2023).
- **Unique Initiative**: The Strengthening Telecommunications Against Natural Disasters (STAND) program provides targeted grants of up to AUD$7.7 million for improving telecommunications resilience in high-risk areas vulnerable to natural disasters (Department of Industry, Science and Resources, 2024).

4.5. *Japan*

Japan's approach to telecommunications resilience is notably comprehensive, reflecting lessons learned from frequent natural disasters like earthquakes, tsunamis, and typhoons.

- **Prevention/Mitigation**: The Ministry of Internal Affairs and Communications (MIC) mandates stringent infrastructure standards to withstand natural disasters. These standards include measures like underground fibre, mandated backup power systems, and movable ICT resource units (MIC, n.d.).
- **Preparedness**: Japan operates advanced early warning systems that are integrated with telecommunications networks for rapid alerts (MIC, n.d.).
- **Response**: Japan's disaster management strategy integrates telecommunications systems to ensure that they remain operational during emergencies to support public safety and disaster response (Cabinet Office of Japan, 2021).
- **Recovery**: Following most major disasters, Japan's Cabinet Office implements measures to provide special financial support for disaster recovery projects for educational and industrial infrastructure (Cabinet Office of Japan, 2021). Japan's Disaster Emergency Message Board Service demonstrates how post-disaster evaluations can refine recovery processes, ensuring infrastructure is rebuilt efficiently.

Table 2
Summary table of international telecommunications EM integration.

Country	Prevention/Mitigation	Preparedness	Response	Recovery	Highlighted Initiative
United States	CSRIC for best practices	IPAWS (Integrated Public Alert and Warning System)	DIRS (Disaster Information Reporting System)	FCC Disaster Response and Recovery Working Group	FirstNet: Dedicated network for first responders
Canada	Multiple government funding programs for broadband expansion	Alert Ready system	Public Safety Canada, CSTAC	Ad hoc telecommunications recovery efforts	Public Safety Broadband Network (not yet deployed)
United Kingdom	Ofcom network resilience requirements	EC-RRG (Electronic Communications Resilience and Response Group)	EC-RRG, MOU of mutual assistance	New 2023 guidelines on network resilience	Mobile Telecommunications Privileged Access Scheme (MTPAS)
Australia	TSSR (Telecommunications Sector Security Reforms)	TISN (Trusted Information Sharing Network)	Telecomm Emergency Communications Protocol	Critical Infrastructure Resilience Strategy	STAND program for targeted resilience funding
Japan	Stringent infrastructure standards for natural disasters	Advanced early warning systems integrated with telecom networks	Cabinet Office Disaster Management Strategy	Significant financial support for recovery projects	Disaster Emergency Message Board service
European Union	EU Network and Information Security Directive NIS2	NIS2 + EU Cyber Solidarity Act	NIS2	National Funding + EU Solidarity Fund	Cross-border interoperability standards

- **Unique Initiative**: The Disaster Emergency Message Board is a service operated by Japan's largest incumbent telecommunications operator, NTT. It automatically activates during major disasters and allows users to check on the safety of relatives and friends through their mobile devices (NTT Docomo, n.d.).

4.6. European Union

The European Union's approach to telecommunications resilience is built around a comprehensive framework that emphasizes cross-border coordination and standardization across member states.

- **Prevention/Mitigation:** The EU Cybersecurity Act and NIS2 Directive establish a robust framework for mitigating cybersecurity risks in telecommunications. These regulations mandate telecom operators implement strong risk management procedures and report incidents, ensuring resilience against cyberattacks and other threats (European Commission, 2023). Additionally, the Critical Entities Resilience (CER) Directive requires national governments to assess infrastructure risks every four years and prepare telecom operators for disruptions.
- **Preparedness:** The EU-Alert system standardizes public warning systems across member states, ensuring that emergency alerts can be sent quickly and reliably to individuals, including tourists, via mobile networks. This system uses technologies such as cell broadcast and location-based SMS and mandates regular testing to ensure functionality during crises. The cross-border standardization offers lessons for North American coordination in response to large-scale natural disasters, such as cross-border wildfires (European Emergency Number Association, 2018).
- **Response:** The EU Civil Protection Mechanism facilitates coordinated disaster response, including expert telecommunications support, ensuring rapid mobilization of resources across member states. This mechanism also provides funding for prevention and preparedness, further strengthening the region's ability to respond effectively to emergencies (European Commission, 2024). Countries within the EU also often operate their own secure networks to facilitate communication for emergency services, like France's RRF.
- **Recovery**: The EU Solidarity Fund is a unique initiative that can be mobilized to support recovery efforts for infrastructure, including telecommunications, after natural disasters. This dedicated fund ensures that telecom operators receive financial support for rebuilding efforts (European Commission, n.d.).
- **Unique Initiative**: The EU places significant emphasis on cross-border interoperability in telecommunications resilience. The NIS2 Directive, CER Directive, and the European Electronic Communications Code (EECC) Article 110 ensure that telecom infrastructure is equipped to handle cross-border emergencies, improving resilience and interoperability across the Union.

5. Recommendations for enhancing resilience globally

Telecommunications networks are the backbone of modern society, providing essential connectivity that underpins economic activities, public safety, and social interactions. As climate change exacerbates the frequency and severity of natural disasters, the resilience of these networks is increasingly under threat. There is a pressing need for a coordinated and well-funded strategy that integrates EM principles across the telecommunications sector to ensure that infrastructure is robust, adaptive, and capable of withstanding future crises.

5.1. Integrate EM frameworks into regulatory structures

Embedding EM principles—prevention, preparedness, response, and recovery—into regulatory frameworks is essential to ensuring proactive resilience-building. Regulators should mandate regular risk assessments, disaster response planning, and cross-sector collaboration. For example, the U.S. FirstNet initiative shows how EM principles enhance coordination between telecom operators and first responders, while Germany's approach to the 2021 floods highlights the value of integrating preparedness and recovery strategies.

Governments should also align regulatory mandates with EM practices, establishing clear benchmarks and conducting regular audits to ensure compliance. In addition, regulators must interrogate how existing telecom policies impact resilience. For instance, mandated resale and roaming policies can concentrate traffic on single underlying networks, thereby magnifying risks flowing from outages. Likewise, undeployed spectrum can undermine infrastructure diversity and system robustness. By reevaluating these policies, regulators can identify opportunities to enhance resilience while ensuring alignment with EM goals. Sharing knowledge among regulators, emergency agencies, and industry stakeholders can further strengthen readiness and improve response capabilities. These steps operationalize EM frameworks, embedding resilience into telecom governance.

5.2. Establish dedicated resilience funding

Governments must prioritize financial mechanisms to address funding gaps in telecommunications resilience. Policies such as subsidies, tax incentives, and dedicated resilience funds can enable providers to invest in infrastructure hardening, redundancy, and recovery systems. Public-private partnerships, exemplified by Australia's STAND program and the EU Solidarity Fund, demonstrate the potential of targeted funding to address vulnerabilities, especially in high-risk and underserved regions.

Additionally, policies that incentivize facilities-based competition can encourage the private sector to invest in diverse and redundant networks, including low-earth orbit satellites, cell towers, and wireline infrastructure. These measures reduce recovery times and increase system robustness in disaster-prone areas. Government support ensures that resilience is prioritized where market forces alone cannot justify the costs, fostering long-term stability and societal benefit.

5.3. Foster multi-stakeholder coordination and adaptive capacity

Collaboration across public and private sectors is essential for effective resilience. Policymakers should establish advisory councils, regional task forces, and multi-stakeholder forums to align objectives, standardize protocols, and streamline resource allocation. The European Union's cross-border response framework demonstrates how coordinated efforts can address vulnerabilities in interconnected networks.

Cross-border and local-level partnerships also play a critical role. Regional frameworks like those in the EU promote resource-sharing and harmonized responses to large-scale crises. Meanwhile, integrating telecom providers into municipal and regional emergency plans ensures tailored resilience efforts that address local vulnerabilities. Such coordinated action reduces redundancies and maximizes the impact of resilience initiatives.

Telecom regulators must move beyond static, command-and-control models to adopt flexible, adaptive policies that evolve with emerging risks. Incentive-based models that reward providers for achieving resilience benchmarks or adopting innovative technologies, such as AI-driven disaster prediction, can drive continuous improvement.

Adaptive planning processes, including regulatory sandboxes and iterative reviews, enable regulators to refine strategies in real time. Measurable Key Performance Indicators (KPIs) for network recovery, infrastructure hardening, and disaster preparedness ensure transparency and guide policy adjustments. By embedding flexibility and adaptability into regulatory frameworks, stakeholders can address vulnerabilities proactively while fostering innovation.

5.4. Expand public awareness and consumer engagement

Public engagement is a vital yet underutilized component of resilience-building. Educating consumers about network reliability and their role in disaster preparedness builds public trust and increases support for resilience investments. Awareness campaigns should promote actionable steps, such as maintaining personal backup systems and understanding emergency communication options.

Incorporating consumer feedback into resilience planning can also improve outcomes. Surveys, focus groups, and participatory sessions provide valuable insights into community-specific needs. By making consumers active participants in resilience efforts, policymakers and telecom providers can create more inclusive, effective frameworks for managing disaster risks.

6. Conclusion

Integrating EM frameworks into telecommunications regulation is critical to strengthening network resilience in the face of escalating climate-driven disasters. EM offers a structured, proven approach to managing risks, enhancing coordination, and improving recovery capabilities—an urgent need for modern society.

Key Findings:

- **Bridging Telecom Policy and EM Planning:** This paper highlights the opportunity to integrate two distinct yet complementary domains: telecom policy and emergency management planning. These fields have historically evolved in silos, but integrating their frameworks offers a pathway to more comprehensive resilience strategies.
- **Gaps in Funding and Coordination:** While progress has been made, critical gaps remain in proactive funding, unified EM adoption, and cross-jurisdictional collaboration.
- **Power of EM Frameworks**: EM principles—prevention, preparedness, response, and recovery—provide a systematic foundation for embedding resilience into telecom policy and practice.
- **Lessons from International Best Practices:** Countries such as the U.S., Japan, and the EU demonstrate how EM-driven strategies—such as partnerships, targeted investments, and integrated policies—can address telecom vulnerabilities effectively.
- **Evaluating Traditional Telecom Policies:** Traditional telecom policies must be critically evaluated for their impact on resilience. Policies such as spectrum allocation without meaningful deployment requirements and resale-led wholesale frameworks that concentrate providers on single infrastructures can inadvertently undermine resilience. Policymakers should prioritize policies that promote infrastructure diversity and long-term robustness.

By prioritizing the integration of EM principles, governments and industry leaders can develop telecommunications systems that are better equipped to withstand disruptions and protect lives during crises. EM is not merely a regulatory tool; it is a transformative framework that aligns public and private efforts toward a common goal: safeguarding critical infrastructure.

The stakes are too high for inaction. A resilient telecom sector is vital not only for economic stability but also for the safety and well-being of communities worldwide. Governments, regulators, and industry must collaborate to implement EM principles, close funding gaps, and foster innovation. With decisive action, we can ensure telecommunications systems remain robust lifelines in an increasingly uncertain world.

List of Abbreviations

Abbreviation	Definition
CER	Critical Entities Resilience Directive
CRTC	Canadian Radio-television and Telecommunications Commission
CSRIC	Communications Security, Reliability and Interoperability Council
CSTAC	Canadian Security Telecommunications Advisory Committee
CTEPM	Canadian Telecommunications Emergency Preparedness and Management
DCMS	Department for Digital, Culture, Media & Sport
DIRS	Disaster Information Reporting System
EC-RRG	Electronic Communications Resilience and Response Group
EECC	European Electronic Communications Code
EM	Emergency management
EOC	Emergency Operations Centre
EU	European Union
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
HRVA	Hazard, Risk, and Vulnerability Assessment
IPAWS	Integrated Public Alert and Warning System
ISED	Innovation, Science and Economic Development Canada
ITU	International Telecommunications Union
KPI	Key Performance Indicator
MIC	Ministry of Internal Affairs and Communications
MTPAS	Mobile Telecommunications Privileged Access Scheme
NIS2	Network and Information Security Directive 2
OECD	Organisation for Economic Co-operation and Development
Ofcom	The Office of Communications
PSBN	Public Safety Broadband Network
RAN	Radio access network
RETO	Regional Emergency Telecommunications Officer
STAND	Strengthening Telecommunications Against Natural Disasters
TISN	Trusted Information Sharing Network
TSSR	Telecommunications Sector Security Reforms
UBF	Universal Broadband Fund
UN	United Nations
UNISDR	United Nations Office for Disaster Risk Reduction

CRediT authorship contribution statement

Peter Jiang: Writing – original draft, Validation, Investigation, Conceptualization. **Joe Rowsell:** Writing – review & editing, Writing – original draft, Validation, Supervision, Project administration, Methodology, Investigation, Conceptualization. **Stephen Schmidt:** Writing – review & editing, Writing – original draft, Validation, Supervision, Conceptualization.

Data availability

Data will be made available on request.

References

Ariely, D., & Holzwarth, A. (2017). The choice architecture of privacy decision-making. *Health Technology, 7*, 415–422. https://doi.org/10.1007/s12553-017-0193-3

Bhola, V., Hertelendy, A., Hart, A., Adnan, S. B., & Ciottone, G. (2023). Escalating costs of billion-dollar disasters in the US: Climate change necessitates disaster risk reduction. *The Journal of Climate Change and Health, 10,* Article 100201.

Brown, C., Seville, E., & Vargo, J. (2017). Measuring the organizational resilience of critical infrastructure providers: A New Zealand case study. *International Journal of Critical Infrastructure Protection, 18*, 37–48. https://doi.org/10.1016/j.ijcip.2017.05.002

Cabinet Office of Japan. (2021). *White paper on disaster management 2021*. Government of Japan. https://www.bousai.go.jp/en/documentation/white_paper/pdf/2021/R3_hakusho_english.pdf.

Canadian Radio-television and Telecommunications Commission (CRTC). (2023). *Broadband fund: About the fund*. Government of Canada. https://crtc.gc.ca/eng/internet/fnds.htm.

Canadian Radio-television and Telecommunications Commission (CRTC). (2024a). *Emergency alerts and the national public alerting system*. Government of Canada. https://crtc.gc.ca/eng/television/services/alert.htm.

Comfort, L. K., Boin, A., & Demchak, C. C. (Eds.). (2010). *Designing resilience: Preparing for extreme events*. University of Pittsburgh Press. https://doi.org/10.2307/j.ctt7zw8x3.

Communications Alliance LTD. (2022). INDUSTRY GUIDELINE g663:2022 telecommunications – emergency communications protocol. https://www.commsalliance.com.au/_data/assets/pdf_file/0019/71632/G663_2022.pdf.

Coppola, D. P. (2020). *Introduction to international disaster management* (4th ed.). Butterworth-Heinemann. https://doi.org/10.1016/B978-0-12-817368-8.09001-1

Department of Home Affairs. (2023). *Critical infrastructure resilience strategy*. Australian Government. https://www.cisc.gov.au/resources-subsite/Documents/critical-infrastructure-resilience-strategy-2023.pdf.

Department of Home Affairs. (2024). *Trusted information sharing network*. Australian Government. https://www.cisc.gov.au/how-we-support-industry/partnership-and-collaboration/trusted-information-sharing-network.

Department of National Defense. (2024). *DRDC conducts research to support Canadian public safety broadband network*. Government of Canada. https://science.gc.ca/site/science/en/blogs/defence-and-security-science/drdc-conducts-research-support-canadian-public-safety-broadband-network.

European Commission. (2023). The EU cybersecurity Act. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act.

European Commission. (2024). EU Civil protection mechanism. https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/eu-civil-protection-mechanism_en.

European Emergency Number Association. (2018). EU reaches agreement on warning public of terrorist attacks. https://eena.org/knowledge-hub/press-releases/eu-reaches-agreement-public-warning-wzu8t9izzey/#.WzU8T9IzZEY.

Fabre, A., & Straub, S. (2023). The impact of public–private partnerships (PPPs) in infrastructure, health, and education. *Journal of Economic Literature, 61*(2), 655–715.

Galasso, C., McNair, J., Fujii, M., et al. (2022). Resilient infrastructure. *Communications Engineer, 1*, 27. https://doi.org/10.1038/s44172-022-00032-5

Gannon, J. P. L. (2023). Lessons for Canada from international approaches to network resiliency and reliability. *32nd European conference of the international telecommunications society (ITS): "Realising the digital decade in the European union – easier said than done?* Calgary: International Telecommunications Society (ITS). Madrid, Spain, 19th - 20th June 2023.

International Telecommunication Union (ITU). (2020). Guidelines on telecommunications in disaster recovery. Available at: www.itu.int.

International Telecommunication Union (ITU). (2024). National emergency telecommunications plan guidelines. Available at: www.itu.int.

Kunreuther, H., & Michel-Kerjan, E. (2013). Managing catastrophic risks through redesigned insurance: Challenges and opportunities. In G. Dionne (Ed.), *Handbook of insurance*. New York, NY: Springer. https://doi.org/10.1007/978-1-4614-0155-1_19.

Linkov, I., & Trump, B. (2019). *The science and practice of resilience*. Springer International Publishing.

Jones, Matthew W., Kelley, Douglas I., Burton, Chantelle A., Giuseppe, Francesca Di, Barbosa, Maria Lucia F., Brambleby, Esther, Hartley, Andrew J., Lombardi, Anna, Mataveli, Guilherme, McNorton, Joe R., Spuler, Fiona R., Wessel, Jakob B., Abatzoglou, John T., Anderson, Liana O., Andela, Niels, Archibald, Sally, Armenteras, Dolors, Burke, Eleanor, Carmenta, Rachel, Chuvieco, Emilio, Clarke, Hamish, Doerr, Stefan H., Fernandes, Paulo M., Giglio, Louis, Hamilton, Douglas S., Hantson, Stijn, Harris, Sarah, Jain, Piyush, Kolden, Crystal A., Kurvits, Tiina, Lampe, Seppe, Meier, Sarah, New, Stacey, Parrington, Mark, Perron, Morgane M. G., Qu, Yuquan, Ribeiro, Natasha S., Saharjo, Bambang H., San Miguel Ayanz, Jesus, Shuman, Jacquelyn K., Tanpipat, Veerachai, van der Werf, Guido R., Veraverbeke, Sander, & Xanthopoulos, Gavriil (2024). State of wildfires 2023–2024. *Earth System Science Data, 16*, 3601–3685. https://dx.doi.org/10.5194/essd-16-3601-2024.

Richard, C., Perennou, T., Chapuis, B., Mellies, R., & Raynal, C. (2024). La stratégie de résilience continue du RRF. *Medecine de Catastrophe - Urgences Collectives, 8*(1), 3–7.

von Lubitz, D. K. J. E., Beakley, J. E., & Patricelli, F. (2008). Disaster management: The structure, function, and significance of network-centric operations. *Journal of Homeland Security and Emergency Management, 5*(1). https://doi.org/10.2202/1547-7355.1411