Gannon, John P.L.

Conference Paper

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?", Madrid, Spain, 19th - 20th June 2023

Provided in Cooperation with:

International Telecommunications Society (ITS)

Suggested Citation: Gannon, John 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?", Madrid, Spain, 19th - 20th June 2023, International Telecommunications Society (ITS), Calgary

This Version is available at:
https://hdl.handle.net/10419/277962

Working Paper

Lessons for Canada from International Approaches to Network Resiliency and Reliability

John PL Gannon. Ph.D.[1]

[1] I would like to express my sincerest thanks to Adhish Tendulkar and Dr. Chulmin Lim for essential research assistance for this paper, and Dr. Georg Serentschy for many interesting and stimulating conversations on the topic.

Table of Contents

1. Introduction

At the present juncture, it is trite to remark that telecommunications networks are important to society and the economy, and that this importance is increasing.[2] Transport, healthcare, education, finance, industry, and energy are each expected to become inextricably interwoven with the continuous availability of high-quality telecommunications network connections,[3] and this is to say nothing of the essential nature of long and short distance communications and emergency response which have now been reliant on such network connections for some time.

Telecommunications infrastructure and services, long considered critical, are becoming continuously interlaced with other forms of critical infrastructure and activity. This is not truly unique, with most infrastructure and services already reliant on the functioning of monetary and energy infrastructure, but nonetheless represents a transformation of telecommunications from a mere means of communication and a platform for a small portion of economic activity to a broader position of criticality. Whether we therefore think of telecommunications networks as a foundation, lynchpin, keystone, or backbone of present and future societies and economies, there is undoubtedly inherent risk in engendering and permitting ubiquitous reliance on infrastructure subject to many potential points of both hardware and software based failures. Such risk may be significant just in terms of everyday operations and human error, without discussing the inevitable weather effects of now unavoidable climate change, a less stable world order, and burgeoning forms of hybrid warfare. In this context, it would be negligent for government not to consider how to make their jurisdiction adequately resilient to face potential challenges and, specifically, how to offset the vulnerabilities created by the growing role of telecommunications infrastructure. The challenge is how to understand the risks and the potential roles and approaches for the government. In pursuit of this, international benchmarks and the development of international best practices is crucial. For Canada in particular, increased dependency on telecommunications infrastructure and how to approach the issue of risk is very much in play, and thus research to feed into this debate is of great value.

There is not, however, much literature concerning the cross-cutting role of government in this subject, particularly not that compares the approach in different jurisdictions. The reasons why become obvious after cursory research: the issue is multi-dimensional in the extreme, and the role or roles for the government are therefore very difficult to pin down. For example, there are two general relevant sets of policies, one for resiliency, and another for reliability. Resiliency is a network's ability to recover from disruptions and continue to function. This concerns, for example, encouraging diversification of network infrastructure and regulation around standards for network robustness. Reliability, on the other hand, is the extent to which telecommunications can be relied upon or expected to be continuously available, and what we do when they are not. To clarify, if the idiom is ‘don’t put all your eggs in one basket, resiliency policy is about how to protect the basket or ensure that it is robust, and reliability policy is how many eggs to put in the basket. The multidimensional nature of the problem means that is also very difficult to capture all the relevant legislation in a given jurisdiction, relevant policy can stem from consumer protection, through technical requirements for cybersecurity, and onto the sector specific regulation concerning how financial institutions should use telecommunications. Any part of the government, at any time, could have dwelt on the potential risk of an outage and taken some action.

---

[2] Galasso, C., McNair, J., Fujii, M. et al. Resilient infrastructure. Commun Eng 1, 27, 28 (2022). https://doi.org/10.1038/s44172-022-00032-5

[3] See e.g: PWC. The global economic impact of 5G. (2021) https://www.pwc.com/gx/en/tmt/5g/global-economic-impact-5g.pdf

Despite this complexity, events such as significant outages evidently inspire governments, and different parts of government, to ask what their role is or should be in facing the challenge of imperfect but often essential telecommunications infrastructure. For example, a significant outage may inspire a telecommunications regulator to begin thinking about whether they are adequately playing their role, or the assessment of a merger in the context of a recent outage may mean that resiliency and reliability weigh on the assessment of a competition authority. As such, a general picture of how this risk is being managed across a jurisdiction is valuable. This paper seeks to provide such a general picture through an initial critically analysis of approaches to resiliency and reliability in telecommunications across different jurisdictions, capturing the key points of policy consideration, key pieces of legislative reform, and high-level approaches to the issue. In so doing, it seeks to inform ongoing policy discussions in Canada concerning the resiliency and reliability of telecommunications infrastructure. Alongside an exposition of the many dimensions of the problem, the paper provides some qualitative analysis of current developments in the areas of resiliency across the G7, South Korea, and Australia to benchmark current discussions in Canada.

In engaging with regulatory activities in other jurisdictions, the paper does not presume or assert that any particular regulation or approach can or should be simply transplanted from one jurisdiction to another; as will be seen, different histories of the telecommunications market, geographical accident, and associated risk profiles all likely necessitate some divergence in approach, as do government structures and cultural approaches to regulation. Indeed, even those EU member states assessed herein, who have each been required to implement the same EU directive, demonstrate meaningful levels of divergence in their approach.[4] There is also a noticeable political angle to the approaches taken, with the focus of regulators and legislators often framed by the specific risks that have already materialized and caused harm.[5] Nonetheless, there are significant lessons which can be drawn through a comparative approach; addressing resiliency is a not a bright-line exercise, and how different jurisdictions understand and assess risk, determine the acceptable level of risk, mitigate risk, and decide who should bear the costs when risks materialize can inform policy debates elsewhere.

The paper will be structured as follows: Section 2 will describe the current state of the resiliency debate in Canada, including a discussion of the events motivating this discussion, the existing and potential responses to these events, and some of the specifics of the Canadian market which are relevant to the conversation around resiliency. Section 3 will frame the concepts associated with resiliency and reliability. Section 4 will identify reliability policies across the jurisdictions in scope. Section 5 will discuss directly the different potential dimensions of policies seeking to maximize resilience, comparing approaches across the jurisdictions under examination. Section 6 will conclude, identifying important lessons for Canada in attempting to design a framework to provide adequate resiliency and deal with inevitable risk.

2. Resiliency and Reliability in Canada

In the summer of 2022, a significant national network outage in Canada affected the wireline cable internet and cellular networks of one of the three major Canadian telecommunications operators, Rogers

[4] Compare Germany to France and Italy.
[5] See Section 3 concerning framing events.

Communications.[6] This outage, caused by a mishandled maintenance on the network core,[7] brought down the operator's flagship brand, flanker brands, and providers with wholesale access to their network, causing mass disruption for a huge proportion of the country.[8] The outage affected significant numbers of Canadians in their work, public services, prevented Canadians contacting emergency services and ground much of the economy to a halt as card payment systems ceased to function and bank machines ceased to dispense cash.[9] A day later, the operator reported that most services had been restored, with some customers nonetheless complaining of continued issues several days later.[10] The company was roundly criticized for the manner in which it communicated with the public and government during the outage, and a similar outage from the same operator in 2021 was widely noted.[11] The outage was particularly problematic as existing gentlemen's agreements between operators dealing with outages failed to mitigate the impact, with the nature of the outage preventing customers connected to the affected network from switching to another provider's infrastructure.[12] Following this outage, the operator voluntarily paid significant amounts of compensation to the affected consumers and committed to splitting its wireless and wireline networks, to a total tune of $400m dollars, $150mn CAD in compensation, and $250mn CAD to split the network.[13] Although this outage in particular captured the political and public imaginations because of its scale and scope, other outages have occurred in recent years due to severe weather events, such as hurricanes on the east coast, [14] dramatic flooding in the west,[15] and significant annual forest fires, [16] although these have been more localized.

These events and the effects of the loss of connectivity on Canadians have subsequently garnered significant attention from the Canadian government, with some action already taken to prevent recurrence and more planned. The Minister responsible, the Minister for Innovation, Science and Economic Development (ISED), set in a motion a process immediately following this major outage whereby almost all significant operators were required to enter into a memorandum of understanding concerning emergency roaming, mutual assistance, and a communications protocols in the event of a critical network outage during an impactful emergency, as well as entailing obligations to submit action plans to the government with plans to deal with such circumstances.[17] The Minister also requested that Canadian Security Telecommunications Advisory Committee (CSTAC) produce a report detailing best practices in ensuring

---

[6] Farooqui S et al, Industry Minister to meet with telecoms after 'unacceptable' Rogers outage (2022) Globe and Mail, https://www.theglobeandmail.com/business/article-2022-rogers-communications-outage/

[7] CTV, What we know about the network system failure that led to the Rogers outage (2022) https://www.ctvnews.ca/business/what-we-know-about-the-network-system-failure-that-led-to-the-rogers-outage-1.5982790

[8] Farooqui S et al, *supra* n 6.

[9] Finextra, Rogers outage shuts down Canadian banks' ATMs, POS and internet banking (2022) https://www.finextra.com/newsarticle/40611/rogers-outage-shuts-down-canadian-banks-atms-pos-and-internet-banking

[10] Evans, P, Rogers says services mostly restored after daylong outage left millions offline (2022) CBC https://www.cbc.ca/news/business/rogers-outage-cell-mobile-wifi-1.6514373

[11] Gheist, M, Responding to the Rogers Outage: Time to Get Serious About Competition, Consumer Rights, and Communications Regulation (2022) https://www.michaelgeist.ca/2022/07/responding-to-the-rogers-outage-time-to-get-serious-about-competition-consumer-rights-and-communications-regulation/

[12] An interesting consideration is that, had affected consumers removed their SIM cards, they would have been able to call emergency services.

[13] Adena, A, Rogers to spend $150 million on customer credits after July 8 outage (2022) https://www.ctvnews.ca/business/rogers-to-spend-150-million-on-customer-credits-after-july-8-outage-1.6003851

[14] Gorman, M, N.S. premier blasts telecom companies in wake of Fiona, calls on Ottawa to step in with regulation (2022) CBC https://www.cbc.ca/news/canada/nova-scotia/premier-tim-houston-telecommunications-hurricane-fiona-1.6598450

[15] CBC News, No power overnight for some B.C. Hydro customers, Bell's mobile network also damaged (2021) https://www.cbc.ca/news/canada/british-columbia/service-outage-bc-storm-1.6249986

[16] Reuters, Eastern Canada's Halifax declares emergency over wildfire (2023) https://nypost.com/2023/05/29/eastern-canadas-halifax-declares-emergency-over-wildfire/

[17] Innovation, Science and Economic Development Canada, Memorandum of Understanding on Telecommunications Reliability (2023) https://ised-isde.canada.ca/site/ised/en/memorandum-understanding-telecommunications-reliability

that networks are resilient. In addition to this framework, forthcoming security legislation seeks to give the Minister powers to intervene in networks, including the removal of network equipment from certain equipment providers and dealing with cybersecurity issues.[18] An inquiry into the specifics of the national 2022 outage has also been commissioned. Furthermore, the outgoing Chair of the sectoral regulator, the Canadian Radio-television and Telecommunications Commission (CRTC) at the end of 2022 publicly indicated plans for proceedings concerning resiliency and reliability in the coming year.[19] These latter proceedings are expected to cover measures to enhance resiliency, compensation, penalties, and consumer communications.[20] To date, the CRTC has only initiated a proceeding concerning the collection of data on outages,[21] but resiliency has appeared in multiple other public consultations. In particular, proceedings concerning telecommunications resiliency in the far north of Canada have dealt with issues of reliability and reliability,[22] and the ongoing consultation on the Broadband Fund, a fund sourced from mandatory contributions by industry participants and administered by the regulator,[23] devotes an entire section to the role of the fund in providing capital, operating costs, and even spare parts for projects to promote resiliency.[24] Also of note is that the government has reserved for itself a significant portion of available spectrum to set up a Public Safety Broadband Network (PSBN), although this has sat idle for over a decade and the roadmap to implementation remains unknown.[25]

Related to this engagement with the subject of resiliency in telecommunications is that the government is also in process of passing Bill C-26: An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts.[26] The Bill amends the Telecommunications Act to add security to the nine other policy objectives currently identified in that Act, in line with other critical sectors and adds new authorities which would enable the Government to take action to promote the security of the Canadian telecommunications system.[27] These new authorities include powers for the Governor in Council and ISED Minister to issue orders to telecommunications service providers, which could be used when it is necessary to secure the Canadian telecommunications system against threats such as interference, manipulation or disruption.[28] Such orders could concern, for example, the removal of infrastructure provided by a particular third party.[29] The Bill also covers several cybersecurity elements through the Critical Cyber Systems Protection Act, which seek to ensure that risks to critical cyber systems are identified and managed in a vital system or service.[30] These 'vital' systems

[18] Canadian Telecommunications Network Resiliency Working Group, Telecommunications Network Resiliency in Canada: A Path Forward (2023) https://ised-isde.canada.ca/site/spectrum-management-telecommunications/sites/default/files/attachments/2023/CTNR%20Recommendations%20v1.0%20Final%20(EN).pdf
[19] Ian Scott, Speech to CTS (Nov, 2022)
[20] ibid.
[21] Canadian Radio-television and Telecommunications Commission, Telecom Notice of Consultation CRTC 2023-39: Call for comments – Development of a regulatory framework to improve network reliability and resiliency – Mandatory notification and reporting about major telecommunications service outages (2023) https://crtc.gc.ca/eng/archive/2023/2023-39.htm
[22] Canadian Radio-television and Telecommunications Commission, Telecom Notice of Consultation CRTC 2022-147-2: Telecommunications in the Far North, Phase II (2022) https://crtc.gc.ca/eng/archive/2022/2022-147-2.htm
[23] Canadian Radio-television and Telecommunications Commission, Broadband Fund: About the Broadband Fund (2023) https://crtc.gc.ca/eng/internet/fnds.htm
[24] Canadian Radio-television and Telecommunications Commission, Telecom Notice of Consultation CRTC 2023-89: Call for comments – Broadband Fund policy review (2023) https://crtc.gc.ca/eng/archive/2023/2023-89.htm
[25] On last update, see: Temporary National Coordination Office, A Public Safety Broadband Network (PSBN) for Canada (2022) https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-psbn/2021-psbn-en.pdf
[26] Government of Canada, Bill C-26: An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts: Charter Statement (2023) https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c26_1.html
[27] ibid.
[28] ibid.
[29] ibid.
[30] ibid.

include telecommunication services, interprovincial or international pipeline and power line systems, nuclear energy systems, transportation systems, banking systems and clearing and settlement systems, with scope left for additional services to be added later.[31] Insofar as the bill grants broad powers to the Minister, it may also have direct relevant to resiliency in the telecommunications sector and other 'vital' sectors and could potentially serve as a vehicle for some forms for resiliency and, as will explained, reliance policy. Of interest is the model of regulation which taken an observe-and-order approach, whereby the government relies on disclosures from industry to make orders concerning their behaviour on a continuous basis. As such, the question of government policy and the role of government in network resiliency in particular is very much a live question in Canada which will develop substantively over the coming years.

While benchmarking against other jurisdiction is therefore valuable, this must take into account many features of the Canadian telecommunications landscape that may differentiate it from other jurisdictions. Canada, as the second largest on earth with a population of 39.99 million, and therefore has extremely low population density.[32] Furthermore, population dispersion is a significant consideration, with a very large portion of the population found in two of the ten provinces and only 130,000 people living in the three territories which make up over a third of Canada's landmass.[33] Even within the provinces, Canada's population dispersion differs from countries of similar size, such as Australia, in that it is far less concentrated around urban centers with many small and medium-sized towns.[34] Given the size of Canada, it's risk profile also differs from other countries in that there is great variation in biome across the nation and a larger exposure to different forms of severe weather event.[35] These geographical and population factors, alongside others such as relatively small subscriber bases by international standards, operations being in Canadian dollars, costs imposed by regulation, and remarkably high spectrum costs,[36] mean that operators in Canada face cost factors of production that may be negatively compared to international comparators.[37]

Despite these challenges, 91.4% of Canadians have access to speeds of at least 50Mbps down and 10Mbps up where they live and work (the Universal Service Objective), with the country on track to reach 100% coverage by 2031.[38] 99.7% of the population are covered where they live and work by at least one of HSPA+, LTE, LTE-A and 5G.[39] Communications infrastructure investment sits at record levels,[40] with

---

[31] ibid.
[32] Statistics Canada, Canada's Population Clock (2023) https://www150.statcan.gc.ca/n1/pub/71-607-x/71-607-x2018005-eng.htm
[33] ibid.
[34] PWC, The Importance of a Healthy Telecommunications Industry to Canada's High Tech Success (2020) p10 *available on request*
[35] World Bank, Climate Change Knowledge Portal: Canada (2023) https://climateknowledgeportal.worldbank.org/country/canada/climate-data-historical#:~:text=Canada%20has%20a%20wide%20range,cold%20winters%20and%20warm%20summers).
[36] Crandall Robert, How Canada's wireless spectrum policy drives up mobile rates (2022) Policy Options https://policyoptions.irpp.org/magazines/october-2021/how-canadas-wireless-spectrum-policy-drives-up-mobile-rates/
[37] Christensen Associates, Key Cost Drivers of Mobile Wireless Services in Canada: Implications for Pricing (2020) https://www.lrca.com/wp-content/uploads/2020/10/Key-Cost-Drivers-of-Mobile-Wireless-Services-in-Canada-Implications-for-Pricing-US-Included.pdf
[38] Canadian Radio-television and Telecommunications Commission, Communications Market Reports (2023) https://crtc.gc.ca/eng/publications/reports/PolicyMonitoring/
[39] ibid.
[40] Statistics Canada, Infrastructure Statistics Hub (2023) https://www150.statcan.gc.ca/n1/pub/71-607-x/71-607-x2018013-eng.htm

investment per subscriber far above the OECD average.[41] There are three major facilities-operating telecommunications networks, with a recent merger having been approved between one of these operators and largest regional operator subject to divestiture of some wireless assets to a smaller operator.[42] Notably, the ISED Minister suggested that the issue of resiliency would play in to his decision as to whether to permit the transfer of spectrum licenses necessary for this merger to go through.[43] These three major operators are subject to ownership rules, requiring that they be largely Canadian owned.[44]

The subject of telecommunications is perhaps more politically significant in Canada than in other jurisdictions, particularly as concerns prices. Although prices have been falling in real and nominal terms across both wireless and wireline networks in recent years, political pressure to further reduce prices remains notable.[45] This has manifested itself in several forms, such as a government mandate to cut prices of certain popular plans by 25% between 2020 and 2022,[46] the introduction of a regulated Mobile Virtual Network Operator (MVNO) regime on wireless networks in 2021,[47] previous and ongoing consultations concerning regulated wholesale access to wireline and, in particular, fibre infrastructure,[48] and competitive measures in spectrum auctions seeking to encourage the emergence and maintenance of 4th wireless carriers in each region since 2008.[49] While the merits of this pricing debate will not be dealt with herein, what is of note is that the government and the regulator have and are taking action to reduce prices through various means, and that there is continuing political pressure to do so.

The question of the resiliency and reliability of telecommunications networks in Canada, as in every other jurisdiction, is clearly a unique cocktail of historical and geographical accident, market structure and political backdrop. Nonetheless, this live and complex issue in the country should not happen in a vacuum, particularly given that other countries have faced similar major outages in recent years and have developed different strategies to dealing with the increasing importance of the functioning of telecommunications infrastructure. As will be seen, recent years have seen and are seeing a flurry of activity on the topic, and the debate in Canada can benefit from approaches taken elsewhere.

3. Framing Resiliency and Reliability

As noted in the introduction, the issue of the resiliency and reliability of telecommunication is of increasing importance.[50] An initial point of note is the paucity of theoretical literature generally underpinning or

[41] Calculated using data from OECD.stat: telecom investment totals in USD and divided by populations
[42] Soni, A, Mehta, C, Canada clears C$20 bln Rogers-Shaw deal with tough conditions (2023) Reuters https://www.reuters.com/markets/deals/canadas-decision-rogers-shaw-deal-may-come-friday-2023-03-31/
[43] Posadzki, A, Rogers outage may weigh on decision around $26-billion takeover of Shaw, Champagne says (2022) Globe and Mail https://www.theglobeandmail.com/canada/article-house-of-commons-committee-to-study-rogers-network-outage-impacts-and/
[44] Canadian Radio-television and Telecommunications Commission, Canadian Common Carrier Ownership and Control Requirements (2010) https://crtc.gc.ca/eng/dcs/current/faq_57.htm
[45] Soni, A, Mehta, C, Canada clears C$20 bln Rogers-Shaw deal with tough conditions (2023) Reuters https://www.reuters.com/markets/deals/canadas-decision-rogers-shaw-deal-may-come-friday-2023-03-31/
[46] Government of Canada, Government of Canada delivers on commitment to reduce cell phone wireless plans by 25% (2022) https://www.canada.ca/en/innovation-science-economic-development/news/2022/01/government-of-canada-delivers-on-commitment-to-reduce-cell-phone-wireless-plans-by-25.html
[47] Canadian Radio-television and Telecommunications Commission, Telecom Regulatory Policy CRTC 2021-130 (2021) https://crtc.gc.ca/eng/archive/2021/2021-130.htm
[48] Canadian Radio-television and Telecommunications Commission, Telecom Notice of Consultation CRTC 2023-56: Notice of hearing – Review of the wholesale high-speed access service framework (2023) https://crtc.gc.ca/eng/archive/2023/2023-56.htm
[49] TELUS Communications, Reforming Canadian spectrum policy for 5G and beyond (2022) telus.com/spectrumpolicy
[50] Galasso, C., McNair, J., Fujii, M. et al. Resilient infrastructure. Commun Eng 1, 27, 28 (2022). https://doi.org/10.1038/s44172-022-00032-5

analyzing the role of governments in this area of policy. While there are many pieces of work dealing with the technical elements of ensuring that networks are not easily disrupted, there appears to be very little literature dealing with the interplay between a critical role for telecommunications networks, regulation, and government more broadly.

Again, this perhaps becomes less surprising once one realizes that the role of government is not easy to pin down. For example, when considering resilience, with whom responsibility for network integrity lies between private sector and government, and within different arms of government, is not clear in principle. Alongside the role of market forces, government bodies such as those dealing with telecommunications regulation, cybersecurity, defense, and public safety and disaster response all have a role to play, may not be particularly well coordinated, and may enjoy different levels of independence from political decision-makers.[51] It may be nobody's job explicitly, and everyone's at the same time.

The answer to with whom responsibility lies may also be separated according to the type of risk, with the private sector or telecommunications regulator responsible for everyday maintenance, public safety responsible for natural disasters, and a specialist ministry responsible for cyber threats, for example. Again, who is responsible for may not even be clear. Issues of reliability, on the other hand, may make relevant many sectoral regulators responsible for other form of critical activity, if that activity could be disrupted by a telecommunications outage. This is therefore a complex, fast moving picture, with the potential for significant amounts of confusion and uncertainty around the role of the different potential actors. A final challenge is that, while no jurisdiction appears to be frozen in place by this complexity, this also means that there are many relevant changes to regulation across jurisdictions and across government departments internationally, which interplay with changing risk profiles because of increased dependency on networks, and changes in geopolitical, environmental, and criminal threats.

As noted in the introduction, a reasonable question on the basis of this analysis is whether it is sensible or possible to engage with risks associated with the critical role of telecommunications networks in a general sense or to separate it into different elements. For example, disaster response, telecommunications and climate change, consumer protection in terms of service continuity, defence and telecommunications, and so on and so forth. While a narrower focus would certainly be more useful in directing or benchmarking a particular area of policy, it would miss the interconnectedness of the issue writ large. For example, the nature of disaster response is tied to how consumer protection in terms of service continuity impacts the deployment of privately owned infrastructure when there is no disaster. The issue with dealing with the issue in silos is akin to the fable of the blind men and the elephant, with each stakeholder grabbing holding of one element and thereby understanding the problem in a different way, with nobody potentially with a full picture of the nature of the elephant itself. Certain policymakers, however, such as competition authorities or an industry regulator will wish to assess the resiliency implications of a particular form of activity, merger, or prospective regulation, and this level of analysis is thus therefore necessary. Even these actors however, may not see all of the reliability part of the 'elephant', but it is important that some policymaker, somewhere, is thinking about the interplay between these two areas of policy to ensure a resilient society, even if telecommunications cannot be made perfectly resilient. Analysis at the level of resiliency and reliability writ large, therefore, makes sense as a starting point.

[51] For example, many countries have telecommunications regulators that are independent, but Ministries of Defence which are very much part of the government.

3.1. Conceptualizing Resiliency

In many ways, the challenge of resiliency is a perennial problem: how many resources to redirect from activities with short-term, certain benefits to offset risks of unknown frequency and proportion. As Araki suggests: 'operators and regulators should choose appropriate measures depending on the acceptable level of risk'.[52] This is easy to say, but not quite as easy to do. 'Resiliency' is an experience good, the value of which is difficult to assess in advance.[53] This is true from the perspective of consumers, operators, and of governments; even if steps are taken to alleviate the massive information asymmetries between operators and other stakeholders concerning how resilient a particular network is, in the face of unknown future events it is impossible to tell in advance what is sufficiently or insufficiently resilient, and even what is excessive. As suggested by Boureau and Feasey, it is only when a connection is disrupted that resiliency becomes an issue for consumers, and even then it may be difficult to attribute responsibility.[54] This same challenge, however, is also faced by operators and governments. This point is aptly demonstrated by recent legislation in California, which requires that wireless sites have 72-hours-worth of diesel available in the event of a loss of power,[55] when compared to recent Australian initiative to improve batteries at sites the provide 12 hours of backup power.[56] Again, alongside who is responsible for this decision and how it should be made decision based upon other decisions made elsewhere in government or the behaviour of the public, the issue is that there is no right answer *ex ante* about the value of any one act.

Alongside heterogeneous challenges resulting from differences in geography, different risk profiles, different market structures and different roles for existing regulation, when examining operator and governmental approaches to network resiliency a pattern emerges in that they appear to often be shaped by specific challenges that have materialized domestically. These can be described as 'framing events'. The nature of these events in a given jurisdiction appears to have a tendency to shape the debate and subsequent approaches to resiliency measures, regulation, and the role of the public sector in resiliency. This is to be expected; a tsunami,[57] a cyberattack of potential state origin,[58] capacity issues during a pandemic,[59] a failure in an OTT messaging service,[60] and even an error made in a software update[61] understandably inspire different emphasis on the various elements of resiliency and the potential challenges the network is expected to be able to deal with and its role when problems do arise. This is likely because the problem is thereby better defined, the nature of the risk is made more obvious, and the political pressure placed on governments and regulatory pressure placed on operators focuses on the specifics of the event rather than resiliency more broadly.

---

[52] Araki, N, ICT Standardization Trends for Disaster Relief, Network Resilience, and Recovery ITU-T (2018) NTT Technical Review, 16(10): 77-82, https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201810gls.html
[53] Boureau, M, Feasey R, Addressing Threats to Digital Infrastructure (2022) in CERRE, *Global Governance for the Digital Econsystems* (2022) 143-178, 155.
[54] ibid.
[55] California Public Utilities Commission, Decision 21-02-029 (2021) S 5.4.4. https://docs.cpuc.ca.gov/PublishedDocs/Published/G000/M366/K625/366625041.PDF
[56] Australian Government: Department for Infrastructure Transport, Regional Development, Communications and Arts, Mobile Network Hardening Programme (2023) https://www.infrastructure.gov.au/media-communications-arts/phone/mobile-network-hardening-program
[57] As in Japan in 2011
[58] As in Ukraine in 2016
[59] As in the EU 2020-2021
[60] As has inspired South Korea's new resiliency rules
[61] As in Canada in 2022

It is important to reflect on whether the role of these framing events means that operators and governments in their respective silos are sometimes preoccupied with preparing for yesterday's crises but, regardless of the nature of the particular event, the thorny question of the attribution of responsibility for the outage and resultant harm, and therefore where and how governments need to intervene, naturally arises. While individual consumers are unlikely to be at fault in any material outage, a particular operator, the telecommunications industry as a whole, critical businesses that took too little stock of the potential for outage, and the government itself are all potential candidates for blame and need for reform. Unlike consumers, who may attribute responsibility to any relevant set of decision-makers, or operators and other businesses, who will reflect merely on whether they correctly assessed risks to their bottom-line in the given context, the government has to grapple with its far wider role in shaping the level of risk taken and the extent of the subsequent harm.

There are a multitude of potential missteps a government may have taken regarding the resiliency of network infrastructure which are thrown into sharp relief by a framing event. A government may have relied too heavily on market incentives to offset particular risks, may have intervened in markets and undermined incentives for businesses to invest in measures to offset risk or created barriers to beneficial industry coordination, may have set insufficiently high minimum standards, may have provided inadequate public funding to protect privately owned networks from risk, or may have created perverse incentives in their financial, political, or regulatory responses to previous crises (the "moral hazard" problem).[62] Alternatively, a government may consider a certain type of outage merely a brute fact, imposing acceptable costs for the advantages brought by telecommunications, treating an outage as akin to a 'snow day', impossible or impractical to prepare *ex ante* for when conditions are extreme. As telecommunications becomes more critical, the space for this 'snow day' attitude will diminish. For government, therefore, the necessary responses to increased dependence on telecommunications networks are a challenging combination of preparing for risks of differing, often unknown frequency and proportion by grappling with a web of regulatory and market structures that have likely developed with little mind to resiliency.

3.2. Conceptualizing Reliability

The author would assert that this challenging combination of trying to motivate the industry to cope with unknown risk is not the right place to start. There is a danger in a conversation which jumps with both feet straight into the resiliency subsection of the potential policy responses, both in general and following an event when an outage has caused mass disruption. The conversation may move quickly from acknowledging the significant and negative impact of an outage, to how to prevent telecommunications networks from being impacted in the same way again. That is, the conversation becomes limited to resiliency without considering reliability. This might be a natural response: if an outage causes mass disruption on many forms across the economy, it's easier to identify that single point of failure than all the ways it was allowed to cascade across different parts of the economy and society.

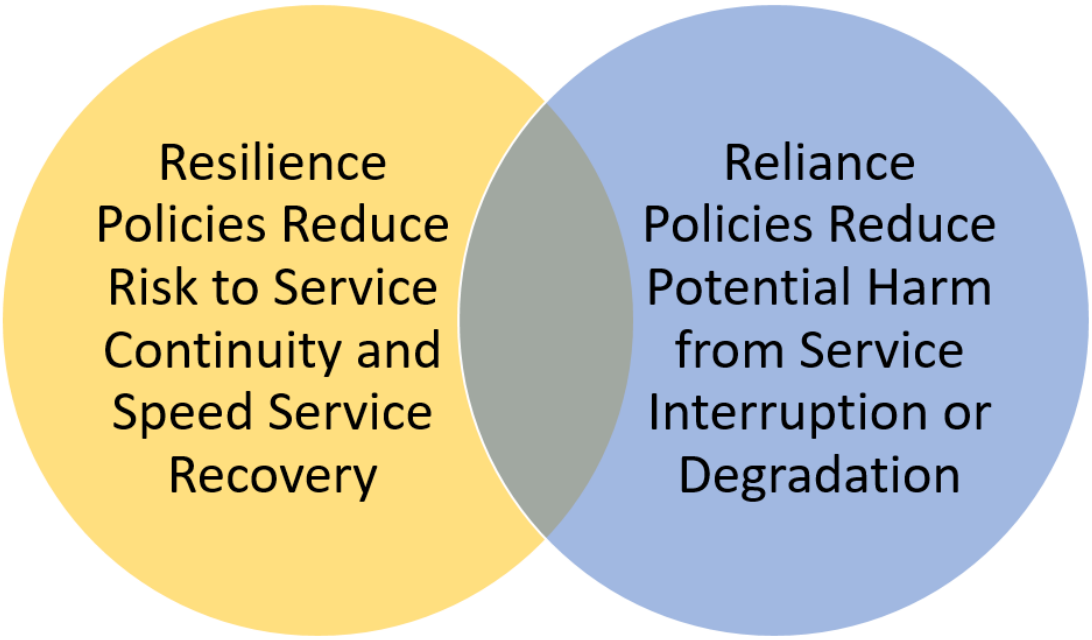
At root, whether telecommunications networks are functioning, or how they are functioning, is only ever indirectly relevant to many of the policy goals of government; it is the impact of a loss of connection that is actually important. This is why the topic herein is increasingly significant: the potential impact of an outage has grown, and continues to do so. As above, the question of the acceptable level of risk certainly turns in part upon the need to redirect resources to increase the resiliency of networks against unknown

[62] Coscelli, A, Thompson, G, Resilience and Competition Policy: Economics working paper (2022) United Kingdom Competition and Markets Authority, p 4 https://www.gov.uk/government/publications/resilience-and-competition-policy-economics-working-paper

future challenges, but the significant other side of this equation is 'what is at risk?' This is where the issue of reliability becomes apparent: did the government do enough to ensure that the public, other industries, other the government itself did not rely more than reasonable or necessary on the availability of telecommunications networks, whether wireless or wired, and which arms of government are responsible for making sure that they do not rely to an unreasonable degree.

For example, alongside the aforementioned missteps a government may have taken with regards resiliency, a government may also have failed to regulate vital industries reliant on telecommunications networks to ensure they have backup connections, protocols or systems in place for an outage, failed to ensure adequate scope for coordination between different sets of infrastructure, failed to ensure that operators communicate with the public so that the public can plan around the outage, failed in their capacity as a convener to coordinate real-time industry responses for dealing with outages, failed to educate the public on what to expect or do in the event of an outage, or failed to put in place mechanisms for consumers to obtain compensation to correct the harm caused. The point is, there may have been things the government could have done much more easily than attempting to make networks more resilient that would offset the harm from outages, which may sometimes be unavoidable.

The implication of these further policy options is that, rather than solely examining potential risks to networks, how operators will deal or respond to such risks, and what is an appropriate level of risk to take given the costs, the process should be to examine the potential harm from an outage or degraded service and the extent to which that harm can be minimized, before attempting to calculate the proportionate level of resiliency. Given natural limitations in capital and policy time, policymakers should consider whether measures to improve resiliency or measures to reduce reliance would be the most cost effective means of reducing overall harm. For example, the question of whether 12 hours or 72 hours of backup power is necessary should take place informed by the impact that will occur if the power runs out. With robust alternatives to a network, 12 hours may be sufficient given the level of risk. The question is whether there are better ways to increase the resiliency of *society and the economy* to outages rather than solely relying on the resiliency of telecommunications networks themselves.



As a simple example, if surgery could be performed on patients a significant distance from the surgeon using telecommunications networks, an outage resulting in all those patients dying on the table would be an unacceptable level of risk. It would, however, make far more sense to regulate the healthcare provider to ensure that there are contingency plans in place in case of an outage, such as a medical professional in the room with the patient, rather than approach all questions of adequate telecommunications resiliency with the possibility of many deaths in the case of an outage. There is obviously a spectrum of potential harms in the event of an outage, from emergency services being unavailable or unable to coordinate, self-driving cars swerving into oncoming traffic, or a breakdown of a country's major payment systems, to being unable to stream television or having to work offline. Some of these harms should be addressed by policies which mitigate the maximal harm of the outage, others are unavoidable in the event of an outage or may be too costly to avoid. It is only those harms that are unavoidable or too costly to avoid or offset with which questions of network resiliency should ideally be occupied. A significant role for the government, therefore, is in ensuring that stakeholders across the economy are well placed to deal with fact that networks can never practically be made perfectly resilient, and therefore only rely on networks to the extent that is reasonable.

A major barrier to this outcome is that, when outages occur, the responsibility within government may fall squarely within the remit of the telecommunications regulator and associated Ministry as the single point of failure that cascaded through the economy.[63] The weakness of this approach is that these bodies are limited in their capacity to mitigate many of the potential harms from an outage, and may therefore need to place greater emphasis on resiliency than would be warranted with a more coordinated approach across government. Similarly, it is outside the power of telecommunications operators to unilaterally reduce the potential harm from an outage other than through increased resiliency. Many of the existing and

[63] As appears to have been the case in Canada following the outage in 2022.

forthcoming uses of telecommunications networks are associated with other arms of government, and particularly other regulators.[64] In order to most effectively deal with the potential for network disruption, therefore, it is critical that telecommunications regulators coordinate with these other arms of government to minimize risks associated with network disruption, and then be able to take proportionate steps to ensure adequately levels of resiliency.

4. Policy Dimensions of Reliability

4.1 Sector Specific Policies

The distinction between resiliency and reliability is significant for Canada because, although the regulatory focus following the 2022 outage has involved some harm reduction measures, the focus appears to be on network resiliency. Resiliency cannot, however, ever be truly complete, and this focus and promise of a regulatory solution may fail to incent adequate regulatory adjustment elsewhere in government to prepare for the possibility of network failure. Of most concern is that very little attention appears to have been paid to, for example, the disruption of both card payments systems and cash withdrawal systems during the 2022 outage.[65] Many were unable to call 911, and hospitals, public transit, border crossings and countless other public and private services were disrupted.[66] A significant portion of the harm caused by the outage presumably originated from these forms of impact, and the absence of evident coordination between the regulator for telecommunications and other relevant regulators to determine how to mitigate this risk in the future should perhaps raise concerns, as should the fact that such coordination does not appear to have happened *ex ante*. This is particularly the case given that the increasing role of telecommunications in other forms of critical services and infrastructure, which will require more of such coordination in the future to offset risks from outages.

A useful example of how this form of problem might be addressed can be observed in the EU. The EU holds telecom-dependent entities like banks responsible for maintaining their business resiliency, not just the telecommunications operators themselves, and EU legislation asks telecom-dependent entities to conduct risk assessments and diversify their digital providers proportional to their socio-economic risk profile. For example, The EU Network and Information Security Directive (NIS-2)[67] recognizes the risk that third-party network providers pose to networks used by important entities and prescribes the adoption of cyber hygiene and risk management practices.[68] NIS-2 acknowledges the criticality of certain technologies to the digital economy and encourages diversification strategies to strengthen their resiliency and reliability.[69] NIS-2 directs the member states to create public-private partnerships (PPPs) in the field of cybersecurity to harness private-sector expertise in planning resilience and crisis management.[70] As an example of sector specific regulation to reduce harm, The Digital Operational Resilience Act (DORA) requires financial entities to develop robust policies and procedures for the management of ICT risks to

[64] See e.g. PWC. The global economic impact of 5G. (2021) https://www.pwc.com/gx/en/tmt/5g/global-economic-impact-5g.pdf
[65] Finextra, Rogers outage shuts down Canadian banks' ATMs, POS and internet banking (2022) https://www.finextra.com/newsarticle/40611/rogers-outage-shuts-down-canadian-banks-atms-pos-and-internet-banking
[66] Farooqui S et al, Industry Minister to meet with telecoms after 'unacceptable' Rogers outage (2022) Globe and Mail, https://www.theglobeandmail.com/business/article-2022-rogers-communications-outage/
[67] European Parliament and The Council of the European Union, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (2022) OJ L 333, 27.12.2022, p. 80–152 https://eur-lex.europa.eu/eli/dir/2022/2555
[68] Ibid.
[69] Ibid.
[70] Ibid.

ensure the stability of their services. Some of these include having business continuity plans, conducting risk audits, maintaining updated and reliable ICT systems, establishing incident response procedures etc.[71]

A further example in the financial sector can be seen in the UK, where the Bank of England, Prudential Regulation Authority (PRA), and Financial Conduct Authority (FCA) have put in place a stronger regulatory framework to promote the operational resilience of firms and financial market infrastructures firms (FMIs). Although not tied directly to telecommunications, they state that 'The supervisory authorities consider that many firms and FMIs currently may not sufficiently plan on the basis that disruptions will occur, and therefore would not be able to manage effectively when they do. The aim of the policy that the supervisory authorities proposed is to ensure that firms and FMIs do this planning and deliver improvements to their operational resilience to ensure they are able to respond effectively if a disruption does occur.'[72]

These examples are informative, but the wider question should be whether there are sufficient cross-cutting bodies or authorities, or enough coordination between different regulators to deal with the risk of outage as it become more prevalent as a result of innovation. In Canada, it is clear that this was not the case with regards financial systems, and it is unclear that it is adequate elsewhere. Indeed, frequent government-wide assessments of different critical industries and their vulnerability to outage should perhaps occur, particularly in periods of rapid technological chance and adoption, and these should feed in to discussions around resiliency. Other jurisdictions, such as Japan, appear to have standing bodies that deal with these types of thorny question.[73] This is not to say, however, that telecommunications regulators have no direct role in reducing harm associated with outages, and there are several instances of 'reliance' policies that can be observed across the G7, South Korea, and Australia, including in Canada.

4.2 Public Communications

A clear recent example of a reliability measure which turns on the telecommunications regulators is the Canadian government requiring communications protocols to ensure that operators convey to the public information the need to be able to understand the extent of the service interruption so that they can then take necessary steps to find alternative means of achieving their ends if necessary.[74] This can also be observed in the EU. EU legislation requires operators to inform their consumers of all the actions they would take to deal with faults and failures. The European Electronic Communications Code (EECC) requires the operators to provide customers with information such as consumer rights, quality of service, compensation and refund mechanisms, incident response procedures etc.[75]

---

[71] European Parliament and the Council of the European Union, Regulation of The European Parliament and of The Council on on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (2022) OJ L 333, 27.12.2022, p. 1–79

[72] Bank of England, Building Operational Resilience and Impact Tolerances for Important Business Services (2021) https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/publication/2021/building-operational-resilience-impact-tolerances-for-important-business-services.pdf

[73] See e.g.: Advisory Panel on Development of Digital Infrastructure (DC, etc.), Announcement of the Interim Report of the Advisory Panel on Development of Digital Infrastructure (DC, etc.) (2020) https://www.soumu.go.jp/menu_news/s-news/01kiban04_02000197.html

[74] Innovation, Science and Economic Development Canada, Memorandum of Understanding on Telecommunications Reliability (2023) https://ised-isde.canada.ca/site/ised/en/memorandum-understanding-telecommunications-reliability

[75] European Parliament and the Council of the European union, DIRECTIVE (EU) 2018/1972 establishing the European Electronic Communications Code (2018) https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1547633333762&uri=CELEX%3A32018L1972

Another example could be a public education campaign to explain beforehand possible means of, for example, contacting emergency services if a network is down. One interesting feature of the Canadian outage in 2022 is that had affected customers removed their SIM cards, they would have been able to call emergency services. People were not aware of this, nor did they appear to be made aware of it through other means of broadcast. This can be observed both in government resources provided in Australia,[76] and, for example, in measures taken in the US Wireless Network Resiliency Cooperative Framework (Framework).[77]

4.3 Traffic Regulation

A particularly potent example of policy that can be implemented *ex ante* to make sure that critical services are not unnecessarily affected by emergency situations, degraded services, or outages is to regulate for how different forms of traffic should be treated on a degraded network. For example, Japan's Telecommunications Business Law (TBL) requires telecom operators to prioritize essential communications during natural disasters even if it requires them to halt other services.[78] The experience of Japan is particularly illuminating with respect to resiliency and reliability because of the country's experiences with the earthquake and tsunami in the early 2010s. As such, there are actually multiple measures to deal with reliance on networks and efficiently manage mass disruption, including developing services that are effective at meeting the needs of the public to contact relatives in emergency situations but without this being possible for everyone to do at once, particularly in an emergency.[79] A wealth of literature dealing with the Japanese experience has been shared with the ITU on the subject.

The ability to discriminate between forms of network use however need to be carefully balanced against principles of net neutrality in some jurisdictions, including Canada and the EU.[80] Whether principles of net neutrality can survive innovations such as network slicing is unknown, but the point remains that, at present, there may be regulatory barriers that would prevent an operator dealing with an outage or degradation of service in the manner that is most efficient.

4.4 Compensation

Some regulatory measures may be effective at both promoting resiliency and reducing harm, and it may be difficult without examining specific policies to understand what the main aim actually is. For example, consumer compensation mechanisms may encourage operators to invest more heavily in resiliency or increase the priority of quick recovery, but may also offset harm caused by an outage to impacted individuals. There are, however, two massive limitations on the ability of compensation to offset harm from an outage. Firstly, given that so much economic activity now occurs over telecommunications networks and the projected increase of their importance across many critical sectors, it is not feasible to levy adequate

[76] Australian Government: Department for Infrastructure Transport, Regional Development, Communications and Arts, Communications in emergencies and natural disasters (2021) https://www.infrastructure.gov.au/media-communications-arts/phone/communications-emergencies-and-natural-disasters

[77] Federal Communications Commission, Wireless Network Resiliency During Disasters (2022) https://www.fcc.gov/wireless-network-resiliency-during-disasters

[78] Government of Japan, Telecommunications Business Act. (Act No. 86 of December 25, 1984) (1984) Art 8

[79] Araki, N, ICT Standardization Trends for Disaster Relief, Network Resilience, and Recovery ITU-T (2018) NTT Technical Review, 16(10): 77-82, https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201810gls.html

[80] For EU See: Manidaki, K, Net Neutrality Regulation in the EU: Competition and Beyond (2019) Journal of European Competition Law & Practice 10(7) 479–488, https://doi.org/10.1093/jeclap/lpz049; For Canada see: Zimmer, B, The Protection of Net Neutrality in Canada (2018) Report of the Standing Committee on Access to Information, Privacy and Ethics https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9840575/ethirp14/ethirp14-e.pdf

compensation without imposing crushing liability. Secondly, some of the events under consideration may not be covered by insurance, such as natural disasters or state sponsored cyberattack. Thirdly, and relatedly, it may not be appropriate for a private telecommunications business to compensate either for all forms of risk or for all forms of harm. In fact, other private actors should perhaps be liable if they have over-relied on telecommunications resiliency and thereby caused harm.

In terms country practice, save for in Australia there does not seem to be a strong practice of providing compensation for actual losses in order to solve for harm. Where compensation is mandated, rates are relatively low compared to the potential damage.[81] For reference, a class action concerning the 2-day outage in Canada in 2022 seeks damages per consumer of $400 CAD.[82] Furthermore, while the UK system automatically credits customers with a set rate, the outage has to be significant, lasting for more than 2 days. Considering low rates of compensation and delays in when and how that can be applied for in some countries, it is not clear that any country, save for Australia which relies on its consumer code rather than telecommunication specific regulation, actually uses compensation as a means to undo or reduce harm from an outage that has already occurred save for if the only impact is relatively minor inconvenience.

4.5 Network Diversification

A major means of improving both reliability and resiliency is network diversification. In the context of resiliency, this would mean encouraging the duplication of infrastructure through various means discussed below to provide redundancy. An example is a focus on facilities-based competition, which will increase resiliency by promoting competition on the basis of reliable service and will result in the construction of additional infrastructure so that there is redundancy. Of course having two or three separate, sets of infrastructure is thin gruel for the subscribers of the one network that goes down. Nonetheless, insofar as reliability is concerned, the amount of harm caused by an outage can be reduced by a combination on means to encourage resiliency, such as facilities-based competition, and then means of coordination during an outage.

Generally, harm from an outage will be lessened if consumers or other bodies have other means of connecting to one another and these are available to switch to. In the context of consumers and general internet usage, such switching is straightforward. It is only in the context of more specialized services, such as a payment or healthcare service, that one could not simply switch from desktop to phone, or to someone else's phone or desktop. Some jurisdictions have prepared explicitly for this type of switching behaviour in the context of emergency services.[83] Australia, for example, despite having every fire station connected to fibre, has also provided a satellite connection for each station in case the fibre is damaged.[84] In this way, even a specialized service can take advantage of diversification. Other jurisdictions have created entirely separate networks for public safety to improve redundancy and decrease the need for coordination with private businesses. These private business, however, would nonetheless provide a further backup and remain the means by which the public communicate with emergency services.

---

[81] For discussion, see *infra* Section 5.9

[82] Lamont, J, Rogers outage class action request likely to be heard in June (2023) https://mobilesyrup.com/2023/03/31/rogers-outage-class-action-likely-heard-june-2023/

[83] 'Blue Light' Services are available in Europe, with similar services in the US, Canada, South Korea, and Japan.

[84] Australian Government: Department of Infrastructure, Transport, Regional Development, Communications and Art, Provision of Satellite Connections to Emergency Services and Evacuation Centres https://www.infrastructure.gov.au/media-communications-arts/phone/provision-satellite-connections-emergency-services-and-evacuation-centres

In some circumstances, governments may not wish to impose the burden on individuals and businesses to find an alternative means to connect, even if all services in an area are not affected by an incident. Whether or not placing the onus on the user is practicable will depend on the nature of the outage or degradation of service, and relying on consumers to find ways to make do is clearly a potentially unpopular policy choice. To address this, the government can prevent any individuals, whether residential or business, over-relying on one network by encouraging, mandating or merely permitting that industry participants cooperate when dealing with outages. For example, a government may require or facilitate that traffic from an operator suffering an outage be transferred to the network of a competitor where this is possible.[85] In so doing, they will increase the resiliency of networks writ large by prevent over-reliance on one network and thereby prevent some of the most severe harms emerging from a total blackout of service for a particular subscriber base. The effect, however, may be that service deteriorates for both the customers of the operator suffering an outage and the customers of the competitor if there is insufficient capacity to deal with the increased traffic. Alternatively, a host network's consumers may be prioritized wherever there is limited capacity but, then, it is very difficult to assess *ex ante* how effective a means of addressing reliability concerns this mechanism may be. This approach has recently been put in place in Canada and the US,[86] but there are several crucial drawbacks that have to be considered because of the effect that cooperation has on incentives to build resilient networks in the first place. These will be discussed below.

5. Policy Dimensions of Creating Resilient Networks

Having ideally narrowed the potential harm from outages to those that are unavoidable or too costly to avoid, the next problem is how a government should ensure that networks are adequately resilient, in proportion to the harm that outages or the degradation of service risks, to reduce the risk of outage, the severity of outages, or shorten length of outages. This problem has many dimensions, with potentially relevant actors across the private and public sectors and concordantly huge swathes of potential policy options. In designing policy to further resiliency, it is important to consider the role of the following mechanisms which have played different roles across the surveyed countries in the pursuit of resiliency:

1. Market competition
2. Industry cooperation
3. Regulated competition, such as regulated wholesale markets
4. Resiliency Regulations
5. Public funding
6. Over the Top (OTT) services
7. Funding from other areas of the private sector, such as a 'sending-party-network-pays' model
8. Publicly owned and operated networks

[85] In Canada, see: Innovation, Science and Economic Development Canada, Memorandum of Understanding on Telecommunications Reliability (2023) https://ised-isde.canada.ca/site/ised/en/memorandum-understanding-telecommunications-reliability; in the US, see: Federal Communications Commission, Report and Order and Further Notice of Proposed Rulemaking (2022) FCC 22-50 https://docs.fcc.gov/public/attachments/FCC-22-50A1.pdf

[86] Ibid.

9. Consumer empowerment

10. Other laws, such as criminal laws dealing with theft or damage to network equipment and cybercrime aimed at network disruption

5.1 Market Competition

Market competition has played a significant role in ensuring resilient telecommunications infrastructure in many jurisdictions to the present point. The ability to provide a consistent service comparable to competitors is a key element of the value proposition of telecommunications services; consumers need to be able to predict with reasonable confidence where and when they will be able to access services, and what the quality of those services will be. In some respects, resilient infrastructure is therefore similar to wireless network footprints. Failure to provide an adequate level of confidence concerning the availability of service may motivate significant switching from an unreliable provider if competitors are present with alternative more resilient infrastructure, and conversely disincentivise switching from a more reliable operator to a less reliable competitor. While resilience can constitute an 'experience good',[87] this is only true once outages or degraded services are infrequent occurrences and are not an expected element of the service. To the extent that the current quality of networks can be attributed to competitive dynamics between competing facilities-based operators, it has been widely successful at encouraging resiliency and, indeed, adoption and reliance. As will be discussed below, consumer rights and the ability to switch providers clearly play an important role in this dynamic but, save for some of the most nefarious forms of lock-in, competition is presumably a key driver of resiliency.

Despite this, market competition as a vehicle for resiliency faces significant challenges. As the GGDE put it, it is only when a connection is disrupted that resiliency becomes an issue for consumers, and even then it may be difficult to attribute responsibility.[88] Consumers may not be familiar with information such as that a particular brand serving them is a flanker brand or subsidiary, operating on the facilities of a primary brand or associated infrastructure-owning company, or that a particular brand is merely providing services to them via wholesale access to the infrastructure of another business.[89] This level of confusion alone may significantly dampen the ability of retail market competition to drive resiliency. One offsetting factor is that, where there are competing sets of infrastructure, a company accessing a network of another provider on a wholesale basis may themselves switch in response to low levels of resiliency, potentially representing a very significant blow to the unreliable operator. The situations where this is feasible may, however, be limited.

Another significant barrier to the role of market competition in driving resiliency arises once a relatively high level of resiliency is achieved. It will be difficult for consumers to assess the value of switching operators if each seems to have very occasional outages, with differences only apparent over several years. At the point that outages become infrequent enough to cease motivating consumers to switch providers, operators will lack the competitive incentive to continue making networks more resilient. One possible dynamic of relevance is that consumer reaction to an outage may vary depending on the nature of the outage. Where, for example, an outage is caused by natural disaster, consumers could more readily point a finger at the government rather than a specific telecommunications operator, or at the industry as a whole,

[87] Boureau, M, Feasey R, Addressing Threats to Digital Infrastructure (2022) in CERRE, *Global Governance for the Digital Econsystems* (2022) 143-178, 155.
[88] Ibid
[89] For example, the wholesalers making use of the Roger's network in Canada in 2022.

whereas an error made in maintenance or vulnerability to a cyberattack may be readily attributed to the operator. This is particularly relevant when discussing the 'moral hazard' problem.[90]

Nonetheless, even in the context of infrequent outages and in the absence of explicit regulation mandating compensation for consumers, there are clear examples of companies opting to compensate customers for outages voluntarily, sometimes in excess of the value of the lost service according to the contract (such as the day rate for the period in question). It is difficult to square this phenomenon with a belief that competition no longer applies simply because outages are infrequent. Rather, this suggests significant weight being placed on reputational damage, an indication that resilience remains an important dimension of market competition. Notably however, just as the potential attribution of blame by consumers may differ depending on the cause of the outage, the voluntarily distribution of compensation may vary along the same lines.[91]

Two further possible barriers to market competition as a mechanism for encouraging resiliency are collusion and regulation. Competition based on the resilience of networks turns upon the differentiation of services on the basis of resilience. Collusion and regulation can undermine this. For example, a tacitly collusive dynamic between competing infrastructure owning firms may discourage investment in improving the resilience of infrastructure, with neither operator incented to induce competition on this dimension of a service. In such circumstances, regulation may be required to encourage competition or to identify other means of ensuring resiliency. Conversely, however, regulation can also stifle this form of competition. For example, resiliency regulation may include mechanisms such as mandatory roaming during outages, rendering resiliency effectively invisible to consumers.[92] Regulation of competition on the market, for example in the form of a regulated wholesale market, may also undermine this dynamic by intensifying dimensions of competition other than resiliency.[93]

Finally, the role that market competition can play in resiliency turns on the level of concentration. The precise relationship between different levels of concentration and competition on resiliency is difficult to assess in the abstract. On the one hand, a monopolist possessing all the telecommunications infrastructure in an area clearly has little incentive to invest in resiliency on the basis of competition as customers, whether at the retail or wholesale level, have no alternatives. At the other extreme is a very fragmented market where even minor failures in equipment may be financial ruinous, where a larger number of points of failure may be introduced, and where furious pricing competition may undermine the ability of an operator to invest in more than the bare minimum. Across all the countries considered herein, national wireless markets tend toward a small number of facilities-operating providers in the typical fashion of a grey market. As has been discussed at length in the literature, this is due to the extremely capital intensive nature of the industry. As

---

[90] Coscelli, A, Thompson, G, Resilience and Competition Policy: Economics working paper (2022) United Kingdom Competition and Markets Authority, p 4 https://www.gov.uk/government/publications/resilience-and-competition-policy-economics-working-paper

[91] For discussion see Section 5.9, See also: Gadsden, T, Does your provider owe you money for their service outages? (2022) AllConnect https://www.allconnect.com/blog/get-bill-credits-for-service-outages

[92] As is the case in the US and Canada in certain circumstances In Canada, see: Innovation, Science and Economic Development Canada, Memorandum of Understanding on Telecommunications Reliability (2023) https://ised-isde.canada.ca/site/ised/en/memorandum-understanding-telecommunications-reliability; in the US, see: Federal Communications Commission, Report and Order and Further Notice of Proposed Rulemaking (2022) FCC 22-50 https://docs.fcc.gov/public/attachments/FCC-22-50A1.pdf

[93] As in Canada, see: Canadian Radio-television and Telecommunications Commission, Telecom Regulatory Policy CRTC 2021-130 (2021) https://crtc.gc.ca/eng/archive/2021/2021-130.htm; Canadian Radio-television and Telecommunications Commission, Telecom Notice of Consultation CRTC 2023-56: Notice of hearing – Review of the wholesale high-speed access service framework (2023) https://crtc.gc.ca/eng/archive/2023/2023-56.htm

with other areas of telecommunications policy, it is not clear that there is a 'magic number' of facilities-based operators for incenting competition on the basis of resiliency.[94] When considering wireline infrastructure, however, there are significant differences between jurisdictions on the scope of facilities-based competition due to historical incumbency, public infrastructure, and the availability of competing infrastructure provided by cable network. A further consideration is the extent to which wireline and wireless operators are the same entities, with differing economies of scope for deployment and the potential for intense facilities-based competition, but also the possibility of failure across both wireline and wireless network simultaneously, as seen in Canada in 2022. In the context of the capacity of competition to create resilient facilities, there are also significant differences in the level of infrastructure-based competition in different geographical markets and, in particular, between rural and urban areas. In remote geographical markets, for example, services may be unreliable because of an effective facilities monopoly. New technologies such as internet services from LEO satellites, however, may place competitive pressure on rural providers who have not invested adequately to provide resilient infrastructure, and market competition may again be a key driver of resiliency in these contexts.

As a final point, the role of facilities-based competition will turn largely upon competition controls on mergers, but also actions to bring more facilities operators into the market. This mean that, indirectly, spectrum auctions may have a role in resiliency policy, beyond potential deployment conditions, which will be very different from, for example, wholesale competition.

5.2 Industry cooperation

An alternative to relying on competition to increase resiliency is to encourage, mandate or merely allow that industry participants cooperate when dealing with outages. For example, a government may require or facilitate that traffic from an operator suffering an outage be transferred to the network of a competitor, where this is possible. In so doing, they will increase the resiliency of networks writ large and thereby prevent some of the most severe harms emerging from a total blackout of service for a particular subscriber base. The effect, however, may be that service deteriorates for both the customers of the operator suffering an outage and the customers of the competitor if there is insufficient capacity to deal with the increased traffic. Alternatively, a host network's consumers may be prioritized wherever there is limited capacity but, then, it is very difficult to assess *ex ante* how effective a means of increasing resilience this mechanism may be. As mentioned above,[95] such measures may also reduce the visibility of outages for consumers, limiting competition based on the resiliency of networks. Where this interaction between operators is voluntary, the negotiation is likely to include considerations of degradation of service for the host network's customers, resulting in either an agreement that such customer's traffic will be prioritized if possible and necessary or that the costs for providing this back-up service are substantial. If this arrangement is mandated, however, the regulator would have to either accept that the impact of the outage be spread across customers of both networks, despite one network not having failed, or to try and recreate this balancing exercise undertaken in negotiations.

In effect, by mandating access there is a risk of a free-rider problem, in that one operator can benefit from the resiliency increasing activities of the other. It may be an effective means of making networks more resilient by reducing the chances of a complete outage, and will reduce much of the harm, but it can also have the opposite effect when it comes to the chance of the failure of any one particular network. The result

[94] Kellezi, P, Magic Numbers and Merger Control in the Telecommunications Sector (2015) CPI Antitrust Chronicle, 11(1).
[95] See Section 5.1

might be that a particular network is less resilient than were it entirely responsible for the experiences of customers or, worse still, that no operator has meaningful incentives to invest in resiliency. To avoid this, the government or parties can be very narrow when defining the 'trigger' for roaming, or roaming rates could be substantial to punish the operator at fault and ensure the preservation of adequate incentives. Alternatively, mechanisms other than competition would need to be relied upon to ensure adequate resiliency of each network, such as prescriptive network requirements. As resiliency is, however, an experience good, even in the presence of potentially punishing rates or, for example, administrative monetary penalties, a model of cooperation may encourage greater risk taking on the part of operators with regards resiliency. Indeed, for rates or penalties to be high enough to offset the savings associated with opting not to build redundant infrastructure, they would need to be substantial and, as with the moral hazard problem more generally, operators may bank on regulatory forbearance or a soft-touch given the financial difficulty a significant outage may cause.[96]

A similar pattern may be observed in the case of agreements for mutual support of other kinds during an outage, either voluntary or induced. For example, mandatory sales of spare parts, the use of available specialist labour, and other such forms of support may encourage operators to underinvest in their own capacity to shorten outages. On the other hand, there may also be perverse incentives on the part of competing operators providing the support, particularly if they are profiting substantially from hosting emergency traffic.

Two models of cooperation in times of crisis can be seen in the surveyed countries: in the US, and in Canada itself. Both of these models emerge out of pre-existing cooperation agreements on a less formal basis, with the US deciding to make a voluntarily set of rule mandatory,[97] and the Canadian government facilitating a MoU to replace the gentlemen's agreements that had preceded the 2022 outage.[98] In many ways, these are similar provisions. They both provide mutual assistance and mandatory roaming, and allow a host network to throttle customers of the competitor roaming on its network. There is, however, a very significant difference: the relevant events for triggering mandatory roaming are tied directly to natural disasters by the FCC. In Canada, what is needed is in three parts: 1. First, an "Impactful Emergency", which '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, cyberattacks 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.[99] Second, that the Impactful Emergency lead to a 'Critical Network Failure', meaning an unintentional and unplanned Network outage caused by, or occurring in the context of an Impactful Emergency.[100] 3. That the party suffering the outage issue a triggering event declaration for assistance or roaming.[101] The US, however, requires activation of a disaster response triggers.[102]

---

[96] Coscelli, A, Thompson, G, Resilience and Competition Policy: Economics working paper (2022) United Kingdom Competition and Markets Authority, p 4 https://www.gov.uk/government/publications/resilience-and-competition-policy-economics-working-paper

[97] Federal Communications Commission, Report and Order and Further Notice of Proposed Rulemaking (2022) FCC 22-50

[98] See: Globe and Mail, Rogers outage sparks deal in Canada between major telecoms (2022) https://www.ctvnews.ca/politics/rogers-outage-sparks-deal-in-canada-between-major-telecoms-1.6058707

[99] Innovation, Science and Economic Development Canada, Memorandum of Understanding on Telecommunications Reliability (2023) https://ised-isde.canada.ca/site/ised/en/memorandum-understanding-telecommunications-reliability

[100] Ibid.

[101] Ibid.

[102] Federal Communications Commission, Report and Order and Further Notice of Proposed Rulemaking (2022) FCC 22-50 p 4.17

This difference is significant. The design of the regime in Canada in such that Canadians are likely to more frequently benefit from the mandatory roaming provisions across a far greater swathe of potential issues with a network. In terms of allowing the public to rely more heavily on always having a connection where they expect, this is beneficial. On the other hand, the decisions to have such a wide mechanism comes with potential damage and free rider problems and it may undermine investment in redundant infrastructure or other resiliency measures that have been economic under pure competition. Indeed, in the US resiliency in the context of everything from cybersecurity to accidents is still visible to consumers, but Canadian consumers may not be made aware of the failures of their provider. In this context, unless one is discussing frequent short outages falling short of impactful emergencies, it's unclear how resiliency and competition can function on the basis of markets in Canada at all.

5.3 Regulated competition, such as regulated wholesale markets

Insofar as resiliency is concerned, the greater the extent to which competitive pressure is exerted on facilities-based operators by virtual operators, the weaker the incentives to invest in resiliency. As noted, facilities-based competition may be effective at incenting operators to increase the resiliency of their networks, up to a point. This facilities-based competition can include wholesale customers, particularly where wholesale access is sold to make use of excess capacity and gain a faster return on infrastructure investment, and if it is targeted at a market segment the facilities-based operator is not itself interested in serving. Facilities-based operators may then also compete in the wholesale market for valuable contracts representing a block of additional consumers in a business to business negotiation entailing fewer information asymmetries.[103] In this context, resiliency can be very valuable, and thus competition for wholesale business may incentivize resilient networks.

When, however, wholesale markets are created by regulation in order to intensify retail competition, these dynamics become more complex. This retail competition, fundamentally, will not turn on resiliency if wholesalers are indistinguishable from facilities-based operators. Again, the information asymmetry faced by consumers may mean that they are entirely ignorant of which infrastructure their wholesale provider uses and what this suggests about their relative merits vis-a-vis resiliency. Furthermore, by providing an alternative, less capital intensive route into the market, the regulator may remove the incentives for facilities-based entry, removing scope for the facilities-based competition that may drive resiliency. In the same vein, to the extent that a wholesale regime may be introduced with rates set to impose a haircut on margins, this will lengthen repayment periods for facilities and reduce the revenues and capital available to facilities-operating firms. Both will reduce investment in additional facilities, whether in new areas to promote facilities-based competition or increasing the resiliency of the network over an existing footprint. Similar charges may also be levelled at regulatory mechanisms such as (non-emergency) mandatory roaming and tower sharing.[104]

An important consideration is how regulated rates interplay with the need for resilient networks. If the policy is not to be unduly prejudicial to resiliency, elements of the regime must capture the need for investment in resilient or redundant infrastructure. As always, the facilities-based operators will say the rate

[103] Garrido, E, Whalley, J, Competition in wholesale markets: Do MNOs compete to host MVNOs? (2013) Telecommunications Policy, 37(11) P 1124-1141

[104] Government of Canada, Revised Frameworks for Mandatory Roaming and Antenna Tower and Site Sharing (sf10547) (2013) https://ised-isde.canada.ca/site/spectrum-management-telecommunications/en/radiocommunications/mandatory-roaming-and-antenna-tower-and-site-sharing/revised-frameworks-mandatory-roaming-and-antenna-tower-and-site-sharing-sf10547

is too low, those benefiting from wholesale will say it is too high, and only when nobody is happy will the regulator have struck the correct balance.

On the other hand, it may be possible for regulated access, such as through wholesale rates, could be a potent mechanism for encouraging resiliency. As in wholesale competition emerging naturally from market competition, to the extent that a wholesaler reflects a significant number of consumers and a significant amount of revenue created by infrastructure otherwise running below capacity, their business may be of significant value, particularly if they have to be in the market in any case. Furthermore, despite not owning facilities in the relevant market, a wholesaler may nonetheless face reputational risk if their service is not adequately resilient, and information asymmetries between a wholesaler and facilities-based operator may be fewer than between consumers. In this respect, a wholesale framework may have a disciplining effect with regards resiliency, but only where there are alternative facilities for the wholesaler to potentially switch to, and to switch to without significant disruption to consumers. As with the role of market competition more generally, this will therefore have an uneven impact between different geographical markets with different numbers of facilities-based operators, operating less effectively in rural areas where these are more likely to have only a single facilities-based provider. Furthermore, it may not often feasible for a wholesaler to switch without causing disruption.

An interesting question with respect to the role of regulated competition is the potential effect of including wholesale providers when designing resiliency obligations to incent this form of competition. For example, wholesalers could need to establish their own roaming arrangements in the event of an outage on the main host network to spread the additional load or avoid a total blackout. This could apply both in the context of an emergency in which mandatory roaming becomes applicable, but also for other forms of outage. By requiring or incenting wholesalers to adequately diversify based on resiliency, subject to their own sets of resiliency requirements, could retain incentives for facilities-based operators to invest in resilient infrastructure and, potentially, eliminate contention around the additional costs indirectly imposed on wholesalers by the need to invest in resilient facilities.

Given the declining popularity of regulated regimes of these types, their interplay with resiliency is not being often discussed. This is, however, a key element of the conversation in Canada as wholesale is discussed, and perhaps this exceptionalism is itself an important lesson. As will be discussed below, some of the historical competitive measure in Europe appear to have left operators sub-scale, and regulated competition and the role of wholesale may have a lot to do with this. The lack of investment in infrastructure in Europe, of course, is not just a problem of initial rollout, but also of robust infrastructure.

5.4 Resiliency Regulations

Relying on market competition, cooperation, and even regulated competition to incentivize resiliency are all indirect approaches from the perspective of government. Regulation specifically targeted at ensuring adequate levels of resiliency is a more direct approach.[105] Regulation can be separated into three major categories: those focused on means, and those focused on ends, and those which seek to continually adjust. Regulation based on ends may, for example, put in place requirements for acceptable levels of service on pain of regulatory sanction. Means regulation, in the alternative, would stipulate specific technical requirements for deployed equipment intended, with requirements designed to ensure that operators have taken adequate steps to ensure resiliency. Those regulations seeking to continually adjust may take the form

[105] While a system based on industry cooperation may fall into this category, it does not need to.

of technical or other requirements, but these requirements will be determined on an ongoing basis driven by reporting and transparency requirements. In some respects, resiliency regulations are the most straightforward way for the government to ensure that there are adequate incentives for operators to build resilient infrastructure. Such an approach does, however, come with significant downsides and notably two of the jurisdictions examined appear not to impose regulation concerning resiliency but rather to generally rely on competition.

Regulation focusing on the resiliency end, rather than the means, can be effective. An example of this is the Telecommunications Customer Service Guarantee (CSG) in Australia, which merely stipulates time periods over with faults must be repaired. [106] Such regulations may be very subtle, distinguishing between resiliency requirements for different types of services, and for outages with different causes, by carefully calibrating expectations and sanctions. For example, the CSG does not apply if there is mass service disruption and you cannot meet it for reasons beyond your control or in the event of extreme weather. As will be seen in the context of public funding,[107] a particular challenge for this form of regulation is ironing out for which forms of outage an operator should be deemed culpable. Leaving this to one side however, a clear danger with this form of regulation is that it may disincentivise the extension of network footprints and may raise costs unduly when footprints are extended. This is a difficult square to circle: while much of the harm from an outage may result from the reliance of consumers on services that are usually available that they expect to be consistent, there is also significant detriment to those same consumers if the rollout of the network is undermined and they never receive service in the first place. Of these, the latter harm seems both greater, more certain, and immediate. It is also, however, difficult for the regulator to calculate the extent to which general resiliency obligations of wider benefits to the jurisdiction will affect consumers currently without service in fact, and how to balance these interests in theory. This dynamic is not only relevant where there is currently no service, it may also undermine facilities-based competition. If resiliency obligations apply to networks even in the presence of facilities-based competition and such regulations raise costs, this will also affect which markets a facilities-based operator may be willing to enter with their own facilities. Additionally, if a regulator is interested in incenting small facilities-based operators to enter the market, such regulation may present a barrier to entry.

While it might be possible to conceive of regulation that carves out exceptions to attempt to retain desirable incentives to enter a market or build infrastructure, the need for more complex regulation itself creates significant uncertainty, even when it correctly balances competing interests between consumers faced with less reliable services and entrants who need low costs. Furthermore, it becomes more complex and costly to police. More generally, there becomes a larger question around enforcement. Just as resiliency is an experience good, evaluating compliance based on ends only functions when something has already gone wrong. Just as with other forms of risk that an operator may shoulder, such as reputational harm from an outage, the operator will balance the cost of falling short of their obligations against the cost of further measures to ensure they meet the standard. The challenge is how to introduce this same element of proportionately to the regulation and standard setting given the level of risk. When an outage occurs and there is the potential for enforcement, hindsight may suggest the risks taken were too great, but regulation has to be carefully conceived so as to not make operators invest in resiliency to a disproportionate degree, with costs passed onto consumers. The regulation will only be as effective as the proportionality of the standard and sanction for a breach: if the penalty is too low, the regulation will be ineffective at incenting

[106] Australian Government, Telecommunications (Customer Service Guarantee) Standard 2011 (2011) https://www.legislation.gov.au/Series/F2011L00413
[107] See *infra* Section 5.5

operators not to take risks, including regulatory risk; if the penalty and standard are too high, operators will be incented to overinvest. Calculating the standard and the penalty, therefore, is extremely difficult.

The same problems apply in the context of regulation focused on the means of achieving resiliency, such as by prescribing certain types of measure or network configuration. Alongside these same issues of imposing costs, designing an appropriate standard, appropriate penalties, and policing the standard, more technical regulation has to contend with keeping the standards adequately up to date, providing standards of general applicability, and allowing space for innovation and improvement. A further challenge is the information asymmetry between government and industry, with industry far better placed to evaluate both the risks of a potential deployment of a particular technology and to respond to emerging best practices. While regulation of this type does not rely on *ex post* enforcement following an outage and can be monitored and policed on an ongoing basis, this may itself also reflect a significant cost. This model is observed in South Korea through the Telecommunications Business Act,[108] and in Japan in the Telecommunications Business Law, Article 41-45.[109] Notably, this Act also criminalizes in Art 180 failure to meet resiliency standards.[110] There may however, be differences in the relationships between different governments in different countries that allow this structure to work. For example, given that Japan uses a beauty contest system for spectrum deployment, there may be different relationship with the regulator more generally.

A more dynamic observe-and-order model of regulation, as in Bill C-26 in the Canadian context, improves on some on some of these weaknesses but suffers from others. This is similar to the dynamic seen in the UK[111] and the EU in the EECC.[112] These mechanisms each rely on reporting, investigating, and risk assessments performed by industry to ensure resiliency. Such mechanism can only be as effective as the disclosure, transparency, and risk assessment tools on which regulatory orders can be based. Clearly, there will remain information asymmetries and additional costs imposed by orders made, but these can perhaps be adjusted more dynamically than in a fixed pieces of legislation, or even a set standard. Costs associated with reporting and transparency, alongside risk assessment would, however, be unavoidable. The ways in which the decisions are made also becomes critical; ongoing governmental decision-making on specific cases may increase the scope for political influence and fit poorly with a dynamic and fast-changing industry, increasing uncertainty. This is particularly the case if the relevant decision maker is not located in the independent sectoral regulator. Furthermore, such powers would need to be coordinated with the role of, for example, public funding or other forms of regulation from other arms of government to retain regulatory coherence. Fundamentally, the issue is that, by granting total flexibility, the disadvantages of rigidity do disappear but, unfortunately, also introduce a separate set of problems concerning uncertainty and regulatory risk which are major drags on investment. One promising element of the UK and EU approaches is that they commit to their standards reflecting international best practices which, while dynamic, are also predictable as ascertainable.

---

[108] Government of South Korea, Telecommunications Business Act, (2011) Art 61 and Government of South Korea, Presidential Decree related to Article 33-(2) of Telecommunications Business Act, (2011) and (2013) Art 22

[109] Government of Japan, Telecommunications Business Law (2007) https://www.japaneselawtranslation.go.jp/en/laws/view/3648/enArt 41-45

[110] Ibid Art 180.

[111] Government of the United Kingdom, Telecommunications (Security) Act (2001) https://www.legislation.gov.uk/ukpga/2021/31/contents/enacted; OFCOM, Ofcom begins new role overseeing security of telecoms networks (2022) https://www.ofcom.org.uk/news-centre/2022/ofcom-begins-new-role-overseeing-security-of-telecoms-networks#:~:text=Security%20duties,preparing%20for%20any%20future%20risks.

[112] European Parliament and the Council of the European union, DIRECTIVE (EU) 2018/1972 establishing the European Electronic Communications Code (2018) Art 40 https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1547633333762&uri=CELEX%3A32018L1972

5.5 Public Funding

In the context of ensuring resilient telecommunications networks, public funding has a clear role wherever the economic incentives are absent to invest in certain forms of resiliency. This comes with all the usual caveats, such as the difficulty of assessing from the perspective of the government where resiliency requires further investment given the risk and that operators do not have the economic incentives to fill the gap themselves. There is also the thorny problem of using public funding, whether raised directly through taxation or indirectly by levying contributions from industry, to subsidies elements of a service run privately and for profit. The most significant potential controversies surrounding the role of public funding, however, pertain to the impact of moral hazard and what responsibilities fall rightly with the state rather than private actors.

The issue of moral hazard and with whom responsibility should lie for adapting to certain types of risk or recovering from certain types of event ties directly into the changing risk profile of telecommunications networks. For example, when severe weather events occur, governments may often provide funding to assist with recovery for other forms of business and infrastructure. Indeed, they may also make specific provision that operators are not compelled to issue compensation in the event of a crisis.[113] It is difficult, then, to see what the incentive is for an operator to shoulder responsibility themselves for offsetting risks posed by severe weather events. Indeed, an operator may choose not to invest in the relevant resilient infrastructure on the basis that they expect public money to assist recovery if there is network failure, for which they would not otherwise qualify. The UK Competition and Markets Authority (CMA) describes the general issue as: 'firms supplying essential goods may be inclined to operate in a more risky way (for example, by taking on more financial risk, or by operating in a way that risks regulatory sanction) if they know they will have access to state support (bailouts or regulatory forbearance) when they are at risk of failure…'.[114] At root, setting a standard that requires operators to offset the risk of natural disasters when deploying their infrastructure may be unworkable. As above, any such regulation may impose significant costs on operators, with detrimental impact on other market dynamics, and be very difficult to assess in terms of proportionality. At the same time, the incentives created by market competition may not include preparation for such events, particularly if consumers have different expectations or hold different parties responsible for outages caused by different events. Nonetheless, such events do occur, and may increasingly do so. As such, there must be a role for the government. Similarly, while cybersecurity may form a significant part of everyday operations and ensuring resilient networks, emerging forms of hybrid warfare or cybercrime of potential state origin perhaps shift the onus from private businesses to the state. A difficult problem may be that an operator that falls prey to a cyberattack may point the finger at involvement of a foreign state, and the government may argue the opposite.

While these issues are difficult in and of themselves, and recent moves by some governments have focused on industry cooperation in response to such events rather than resiliency requirements, the key issue with the role of public funding in this space is that there appears to be no settled attribution of responsibilities between governments and private telecommunications operators. As mentioned, agreeing what forms of cyberattack are state sponsored and which are not, and the implications of this, do not seem to have been addressed. Similarly, where a 'severe weather event' for which an operator should prepare becomes a 'disaster' for which the government is responsible and should fund preparation is unclear. As

[113] See, for example, the compensation mechanisms in Australia and South Korea discussed in Section 5.9

[114] Coscelli, A, Thompson, G, Resilience and Competition Policy: Economics working paper (2022) United Kingdom Competition and Markets Authority, p 4 https://www.gov.uk/government/publications/resilience-and-competition-policy-economics-working-paper

above, fundamentally the issues are the difficulty of assessing from the perspective of the government where resiliency requires further investment given the risk and that operators do not have the economic incentives to fill the gap themselves. Within this question of operator incentives, however, has to be included the expected behaviour of the government and the market in response to certain forms of crisis.

Despite this uncertainty, many of the jurisdiction under consideration have begun to provide significant sums for resiliency projects (and other telecommunications infrastructure funds). Some of these are quite modest, such as the $40mn AUS granted to private networks in Australia.[115] As mentioned, Canada too has funds available for resiliency, and it appears this will be of greater importance in the future (although, notably, it will be funded from industry contributions).[116] The US has a very large fund in the Open-RAN space ($1.5bn USD), which may be tangentially related to resiliency via both cybersecurity but also the potential advantages of diversification and increased competition in the network equipment market.[117] There also other funds seeking to advance US leadership in the space which may also indirectly fund resiliency. Indeed, this is more similar to what is seen in Japan where the State appears to fund RnD in resiliency as oppose to actually deployment of networks.[118] In the EU, the Recovery and Resiliency Facility makes €783bn available for Member States to apply for to pay for their national recovery and resiliency plans, 20% of which must be dedicated to digital.[119]

5.6 Over the Top (OTT) and Other Services

In line with the above discussion on the nature of the harm caused by outages and the role of reliance policy in the resilience debate, there is also an absence of discussion concerning how service providers who rely on infrastructure relate to the resiliency of that infrastructure or should be subject to resiliency obligations. An important element of the reliance discussion is the role of other industry regulators in mitigating the potential harm of an outage. Alongside making provision for outages, this may extend to, for example, ensuring certain levels of resiliency in their abilities to maintain normal services. In this way, private sector contracts to provide certain services, where they rely on a particular network, may turn to a significant degree on resiliency and this may drive competition and resiliency on the telecommunications market. For example, remote surgery, dynamic power grids and connected vehicles may all choose a particular operator on the basis of their ability to guarantee resilient connections, even in the event of a significant crisis. This overlaps with emerging capabilities such network slicing, dedicated capacity for certain users, although the interplay with this prospect and current rules around net neutrality in some countries make it difficult to project how this might work.[120] Resiliency requirements on the part of private businesses may also

[115] Australian Government: Department for Infrastructure Transport, Regional Development, Communications and Arts, Mobile Network Hardening Programme (2023) https://www.infrastructure.gov.au/media-communications-arts/phone/mobile-network-hardening-program

[116] Canadian Radio-television and Telecommunications Commission, Telecom Notice of Consultation CRTC 2023-89: Call for comments – Broadband Fund policy review (2023) https://crtc.gc.ca/eng/archive/2023/2023-89.htmhttps://ntia.gov/press-release/2023/biden-harris-administration-launches-15-billion-innovation-fund-develop-more

[117] National Telecommunications and Information Administration, Biden-Harris Administration Launches $1.5 Billion Innovation Fund to Develop a More Competitive and Diverse Telecommunications Supply Chain (2023)

[118] Kim, J, Et al, E-Resilience: A Review of National Broadband Policies, Regulations, Strategies and Initiatives of China, Japan, and the Republic of Korea (2018) Asia-Pacific Information Superhighway (AP-IS) Working Paper Series https://www.unescap.org/sites/default/files/e-Resilience_CJK_final.pdf

[119] European Commission, The Recovery and Resiliency Facility (2023) https://commission.europa.eu/business-economy-euro/economic-recovery/recovery-and-resilience-facility_en

[120] For EU See: Manidaki, K, Net Neutrality Regulation in the EU: Competition and Beyond (2019) Journal of European Competition Law & Practice 10(7) 479–488, https://doi.org/10.1093/jeclap/lpz049; For Canada see: Zimmer, B, The Protection of Net Neutrality in Canada (2018) Report of the Standing Committee on Access to Information, Privacy and Ethics https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9840575/ethirp14/ethirp14-e.pdf

encourage diversification of supply and back-up providers. Alternatively, if there are arrangement for mandatory roaming during an outage,[121] the home provider for the service could negotiate special provision for such business consumers when roaming. In this way, both resiliency writ large and the resiliency of connectivity for critical infrastructure in particular may be strengthened.

Other services are operator neutral, and rather provide services accessed over the internet by consumers, however they are connected. For example, search engines, e-commerce platforms, messaging services, streaming services, and emerging AI services. Given their ambivalence as to the mode of connection, such entities are unlikely to be able to create incentives for operators to increase resiliency. Nonetheless, such entities are key drivers of demand for connectivity in the first place and drive much of online traffic. This will be discussed below in the context of an alternative source of capital for increasing resiliency, but a crucial first step is to establish whether entities themselves have, or should have, obligations concerning the resiliency of their own services. Many of these services, at the current juncture, are of wide-ranging impact across the economy. To the extent that the justification for a focus on resiliency for telecommunications is based on the potential harm flowing from outage, this rationale should in some respects also apply to specific service providers with very large footprints across the population for critical activities. This subscriber numbers may even exceed the number of subscribers of any one set of telecommunications infrastructure, and may also benefit from significant network effects that make it even more difficult to switch from one to another when service is not satisfactory. The criticality of messenger services in particular is difficult to contest, particularly as successful services displace substitutes. Other, future services, such as AI services, may reach a similar level of importance.

Two examples from the surveyed countries are relevant in this regard. The first is the European Union, where the recent Digital Markets Act may result in messaging services in particular having to be interoperable to other smaller message service providers.[122] The reason that this is so striking is because of the parallels with telecommunications and the concordant reliance engendered across multiple services on the functioning of the infrastructure of one entity. With telecommunications being the original gatekeepers, controlling the gate outside the internet, and new gatekeepers on the internet itself often competing for markets or products which were traditionally the purview of telecommunications, what is observed is gatekeepers within gatekeepers, and platforms on platforms. To the extent that resilience regulation is about ensuring the proper functioning of the gate onto the internet, it should perhaps apply to these inner gates too. Of course, part of the reason that telecommunications resiliency is becoming a salient issue is because of increasing threats and the cross-cutting harm caused by outages, but there seems little reason not to consider the resiliency of these operations too. Precisely this development can be observed in South Korea, with a recent 'framing event' caused by a significant outage at a major messaging service. In legislation currently being considered within the Canadian legislature, new resiliency standards are being developed which would apply not only to telecommunications providers, but to these forms of services too.[123] As with other resiliency regulation, the approach in South Korea appears to be a more prescriptive, detailed set of technical resiliency requirements rather than a principled based approach, a reliance on some form of competition or cooperation, public funding, or consumer empowerment.

[121] As in Canada and the US
[122] See: European Commission, Questions and Answers: Digital Markets Act: Ensuring fair and open digital markets (2023) https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2349
[123] The 'Digital Service Reliability Act'.

5.7 Funding from other areas of the private sector, such as a 'sending-party-network-pays' model

To the extent that it is a shortage of capital that is responsible for the absence of infrastructure investment in a jurisdiction, and in the resiliency of infrastructure in particular, a possibility being considered in some jurisdictions is to have a different model of payment for telecommunications systems whereby not only does the consumer pay for access, but the sending party network also pays for the data transmitted. This mechanism has been discussed at length recently in both the EU and South Korea.[124] The focus of the issue in the EU has concerned the need to modernize telecommunications infrastructure, but the absence of sufficient revenues within telecommunications operators to do so. Reasons for this have been attribute to a lack of concentration and competition which is too intense, with similar circumstances in the UK driving signals that regulators will entertain consolidation. In the absence of sufficient revenues for investment however, the idea is that certain online service providers which constitute a large amount of the traffic which networks carry should also contribute to the costs of deploying and maintaining infrastructure. This issue has been controversial, and there is no guarantee that it will make it onto a statute book, but the need for resilient networks is in part motivated by the success of these online service providers and, as such, alongside their own resiliency requirements, it may be feasible to raise money to ensure continuity of both telecommunications services writ large and their own services.

The issue has also been controversial in South Korea. As in the EU, the major impetus has been the costs imposed of operators, particularly for increased traffic caused by streaming services. Following a breakdown in negotiations between the second largest ISP and a large streaming service, in December 2020, The ministry passed the revised Telecommunications Business Act in an attempt to urge foreign platform operators like streaming platforms to share costs in securing stable internet services. There are concerns over the vague and ambiguous language in the legislation and how it will be enforced. The case of the ISP remains that the streamer is obliged to share the maintenance cost burden for its increased traffic, like other Korean content providers such as stipulated in the "Netflix law".[125] As with the situation in Europe, while the debate has thus far focused almost exclusively on the need to upgrade infrastructure to deal with vast amounts of new traffic originating from a few companies, it is also the case that upgraded infrastructure also require improved redundant means to redirect traffic in the event of a problem. In terms of lesson for Canada, these developments are relevant to the conversation around how to incent or create resilient networks as they demonstrate that public funding is not the only conceivable source of potential investment funds other than from telecommunications operators themselves to increase resiliency, or even potentially resiliency enhancing activities.

5.8 Publicly Owned and Emergency Networks

The role of publicly owned and operated networks in resiliency stands in contrast to privately owned networks. In a public monopoly, resiliency in entirely a matter for political priority, with no role for competition and cooperation with the private telecommunications industry. In such circumstances, the burden for determining how much risk to bear and capital to invest in resiliency falls to the government

[124] See, in Korea e.g.: Moon-Hee, C, Netflix Still Refusing to Pay for Network Use (2022) http://www.businesskorea.co.kr/news/articleView.html?idxno=89261; and in the EU see BEREC, BEREC preliminary assessment of the underlying assumptions of payments from large CAPs to ISPs (2022) https://www.berec.europa.eu/system/files/2022-10/BEREC%20BoR%20%2822%29%20137%20BEREC_preliminary-assessment-payments-CAPs-to-ISPs_0.pdf

[125] Yonhap, By, S. Korea requires Google, Netflix and 3 others to provide stable online services this year (2022) https://www.koreaherald.com/view.php?ud=20220203000618

and, while there may be fewer concerns about access to capital, information asymmetries or promoting shareholder value, the level of resiliency may fluctuate based on political reality. Publicly networks may also compete with the private sector and, in this way both subject themselves to subject competitors to pressure concerning resiliency.

Australia is an example of a country with such a publicly owned network,[126] as is the province of Saskatchewan in Canada.[127] In both instances, state ownership of the relevant infrastructure means that resiliency is much more in the remit of the government, with no one else to take the blame when things go wrong. In that vein, it's difficult to tell to what extent public ownership is beneficial or detrimental to resiliency. There certain isn't the danger of undue risk-taking based on consumer needs, but there also be competing political priorities and businesses may not be able to raise capital in the manner of a private company. It is not possible say, however, how public ownership and resiliency interplay.

Other countries, however, may deploy small, low capacity but high resiliency networks for emergency services. This are sometimes referred to as Public Safety Broadband Networks. As discussed above, this not only reduces the reliance of emergency services on privately owned and operated networks, but this diversity of infrastructure available to emergency services reduces the likelihood of a loss of connectivity, increasing the resiliency of telecommunications networks as a whole insofar as emergency services are concerned.

Several countries have implemented this form of network. South Korea, for example, recently completed the Korea Safe-Net in 2021.[128] A total of 1.5 trillion won ($1.06 billion) was allocated to setting up the single network which enables real-time communication between eight disaster-related agencies, including the police, fire department, military and other government bodies, with the aim of coordinating a swift response among the agencies to accidents and disasters.[129] Others have an equivalent network but provided by a private business. The UK has had such a system for some time based on Motorola[130] and is in the process of upgrading it on the EE network, although there are frequent delays.[131] Similarly, the US has Firstnet, operated by AT&T.[132]

5.9 Consumer Empowerment

A key element of the extent to which competition can drive resiliency turns upon consumer rights. In particular, rights to compensation.

As discussed above, consumer compensation measures may reduce the harm imposed by an outage by attempting to correct the harm they suffer as a result. Of significant note however, is that telecommunications services are so valuable and the impact of their loss can be so wide and significant that its difficult either to truly compensate for the damage caused, or to satisfy the affected customers. The 2022

[126] NBN, About NBN Co (2022) https://www.nbnco.com.au/corporate-information/about-nbn-co
[127] Sasktel, About Us (2023) https://www.sasktel.com/about-us/company-info/vision-mission-and-values/history-site/history
[128] Ministry of the Interior and Safety, Disaster and Safety Communications Network (Korea Safe-net) (2021)
[129] Hyo-Jin, L, How emergency communication system failed in Itaewon disaster (2022)T he Korea Times https://www.koreatimes.co.kr/www/nation/2023/06/113_339282.html
[130] Airwave, Emergency Services Network (2023) https://www.airwavesolutions.co.uk/the-service/emergency-services-network/
[131] Jackson, D, UK officials acknowledge ESN risks, hope to complete public-safety broadband project by 2030 (2023) IWCE'S Urgent Communications https://urgentcomm.com/2023/04/13/uk-officials-acknowledge-esn-risks-hope-to-complete-public-safety-broadband-project-by-2030/
[132] Firstnet, Frequently Asked Questions (2023) https://www.firstnet.com/faq.html7

outage in Canada demonstrates this, with the operator spending $150mn on compensating consumers voluntarily but nonetheless facing a significant class action lawsuit.[133] There may also be differences in which types of outage an operator should pay compensation for, with failed updates on the one hand and volcanic eruptions on the other. In terms of using compensation to incentivize investment in resiliency, then, the power of compensation may be somewhat limited. Mandatory compensation cannot be crushing, and it may only apply to a subsection of all the situations a government might wish an operator to prepare for. Furthermore, compensation requirements may be particularly damaging to smaller operators and, to the extent that a regulator wishes encourage the existence of such operators, industry-wide obligations may be damaging.

To the extent that high levels of compensation can be mandated without creating negative side-effect on the health of businesses forced to both recover and reimburse consumers, the level of compensation to adequately outweigh potential savings from adopting risks by not investing in resiliency would need to be substantial. Indeed, such sums, if levied, may be better suited to forms of administrative monetary penalty rather than compensation. Where compensation may be very important is in incenting operators to recover more quickly, or to build capacity to recover as quickly as possible from an outage.

Compensation mechanisms can be observed across several of the survey countries, but provisions vary. For example, when implementing the EECC through their Telecommunications Modernization Act (TKMoG), 2021,[134] Germany allows consumers to claim can request flat-rate compensation if the fault is not cleared within two calendar days of receiving the fault report, for each day of complete downtime, starting from the following day. An exception provided is that this does apply if consumers are responsible for the fault or there is a case of force majeure. The compensation on the third and fourth day is EUR 5 or 10%, and from the fifth day, EUR 10 or 20% of the monthly service fee.[135] Notably, France in implementing the same directive its Ordinance No. 2021- 650, specifies compensation for issues such as delays in carrying numbers, loss of numbers during portability, a no-show at appointments etc. without particularly dealing with network outages.[136]

In the UK, a voluntary scheme has been established for automatic compensation. Part of the rationale is that, by limiting the level of consumer involvement required to receive payment, consumers are compensated quickly and easily by their Communications Provider for a qualifying service quality issue.[137] After two days of lack of service, customers are automatically credited £9.33 for each calendar day that the service is not repaired.[138] There are, however, a number of exceptions but, of particular note in context of resiliency, the scheme requires that 'signatories to pay automatic compensation to customers when the problem is caused by an event beyond a customer's, or the provider's control. This includes extreme

[133] Lamont, J, Rogers outage class action request likely to be heard in June (2023) https://mobilesyrup.com/2023/03/31/rogers-outage-class-action-likely-heard-june-2023/
[134] Bundesrat, Telecommunications Modernization Act (Telekommunikationsmodernisierungsgesetz) (2021) (Sec. 58 (2) sentence 1 TKG)
[135] ibid.
[136] ibid.
[137] OFCOM, Communications Providers' Voluntary Code of Practice for an Automatic Compensation Scheme (2021) https://www.ofcom.org.uk/__data/assets/pdf_file/0026/216962/Industry-Code-of-Practice-for-Automatic-Compensation.pdf
[138] OFCOM, Automatic compensation: What you need to know (2023) https://www.ofcom.org.uk/phones-telecoms-and-internet/advice-for-consumers/costs-and-billing/automatic-compensation-need-know

weather, strike, and third-party acts',[139] but not, for example, if an emergency is declared under Part 2 of the Civil Contingencies Act. [140]

In South Korea, compensation is paid on a more granular basis. In the Telecommunications Business Act, as adjusted in June 2019, operators have to provide compensation for losses unless the customer is at fault or the *force majeure* is involved.[141] As of July 2022, the Korea Communications Commission (KCC) has required major telecommunications providers to revise their compensation condition in their terms of use. Under these rules, compensation is provided when the network is down for '2 hours or more a day or 'More than 6 hours in a month' but not in the case of an emergency.[142] In Australia, consumers are allowed to claim compensation for periods of non-delivery of service, and may also be able to recover further losses.[143]

Japan, Italy, France, the US, and Canada do appear not to have mandatory compensation schemes for outages, but in the US, Canada, and Japan there appears to be a practice of providing compensation in some circumstances.[144] This practice is interesting in that, for example, compensation might not be offered voluntarily in the case of *force majeure* and, potentially, in any contexts where are simultaneous outages across competing businesses, which removes the incentive to compensate.

As in the case of compensation and reliability, it does not appear that the sums involved in providing compensation are sufficiently large to encourage resiliency by encouraging operators to invest in, for example, further network equipment in an area where they have a monopoly unless the situation involve very frequent outages for long periods of time. At most then, compensation could have a role in encouraging operators to repair equipment more quickly, but it seems likely it will do little to satisfy those impacted by any significant outage and little to improve resiliency over all. They seem at best gestural and, insofar as possible, there seems little reason not to allow voluntary compensation measures on that basis.

A significant question for Canada and the US if they sought to replicate these compensation systems is how the mechanism could be reconciled with obligations on the major operators to allow one another to roam on each other's networks in the event of a significant outage. It is reasonable to consider whether the funds for compensation should rather go to the provider of the roaming facility as to opposed to consumers, with high roaming rates thereby providing the same incentive to recover quickly. An alternative may be that compensation should only be paid in circumstances where there is no third-party on who's network consumers can roam, or that the triggering of mandatory roaming should be extremely narrow with compensations mechanisms and outages occurring in all other circumstances. As discussed in the second on cooperation, the US may be able to implement a compensation regime as serious outages do not result

---

[139] Ibid.
[140] Government of the United Kingdom, Civil Contingencies Act 2004 (2004) https://www.legislation.gov.uk/ukpga/2004/36/part/2
[141] Government of the Republic of Korea, Telecommunications Business Act (2021) Art 33
[142] In the US, see: Gadsden, T, Does your provider owe you money for their service outages? (2022) AllConnect https://www.allconnect.com/blog/get-bill-credits-for-service-outages; in Canada see: Adena, A, Rogers to spend $150 million on customer credits after July 8 outage (2022) https://www.ctvnews.ca/business/rogers-to-spend-150-million-on-customer-credits-after-july-8-outage-1.6003851
; In Japan see: The Mainichi, Japanese telecom giant KDDI to pay $1.50 to 35.89 mil. users in apology for network outage (2022) https://mainichi.jp/english/articles/20220729/p2a/00m/0bu/016000c#:~:text=TOKYO%20%2D%2D%20Japanese%20telecom%20firm,company%20announced%20on%20July%2029.
[143] ACCAN, Compensation for telecommunications outages (2016) https://accan.org.au/media-centre/hot-issues-blog/1231-compensation-for-telecommunications-outages
[144]

in mandatory roaming unless they are a natural disaster. This can be contrasted to Canada, where any sufficiently serious outage could feasibly trigger roaming.

5.10 Other Laws

A final consideration concerning the dimensions of resiliency is other areas of law that similarly apply to telecommunications infrastructure with the goal of protecting network infrastructure. An interesting contrast between some of the countries surveyed is there approach to criminalizing theft of network equipment or damage to network infrastructure. Of note is that many countries appear to suffer from this issue, particularly in recent years as the price of copper has increased. Different countries have taken different approaches, but in most instances stealing cable associated with a network is dealt with no differently from any other small-scale theft.

In the US, according to the FBI most offences are treated as misdemeanors resulting in small fines.[145] This is despite the fact that, including lost productivity, costs of property damage etc, it is estimated that cable thefts cost the US between $1.5bn ad $2bn a year.[146] Thefts in Australia, France, Germany and the UK are frequently reported online, as they are for Canada. The UK has, however, taken some steps to deal with the problem. Through its Scrap Metal Dealers Act, the UK government passed into law requirements for scrap metal dealers, including that a licence is required for metal trading and must be issued by the local authority, that any site that is caught trading without a licence may be fined up to £5000, that payments cannot be made in cash. All payments must be made through electronic bank transfer or cheque and that records of a seller's name and address must be retained, as well as a record of the receipt of the metal.[147]

6. Conclusions: Lessons for Canada

The preceding exercise reveals several important features of the resiliency debate which need to be brought into the conversations in Canada.

Firstly, that other countries are proactively looking at ways to soften the impact of outages, such a by regulating particular industries, prioritizing different types of traffic or setting emergency networks to ensure continuance communications in the event of an emergency. While Canada has taken some steps to improve communication between companies suffering outages and the public, Canada is the only country to have gone so far in relying on cooperation between competing operators in solving the issue of how to deal outages. While this may work as a sticking-plaster, preventing many full-blown outages by providing throttled services to customers of damaged networks, including business customers, this can be expected to have two effects. 1) Businesses and consumers who should take steps to prepare for the possibility are less likely to do so if the roaming and mutual support regimes are sold as having solved the problem. 2) The incentives for individual companies to invest in resiliency or resilient infrastructure in places where they have competitors with adequate capacity may disappear. This needs to be carefully monitored.

---

[145] Federal Bureau of Investigation, Copper Thefts Threaten U.S. Critical Infrastructure (2008) Intelligence Assessment (unclassified) https://www.fbi.gov/stats-services/publications/copper-thefts

[146] Clou, S, Cable theft: A growing problem around the world (2023) https://www.smart-energy.com/industry-sectors/energy-grid-management/cable-theft-a-growing-problem-around-the-world/

[147] See Government of the United Kingdom, Scrap Metal Dealers Act 2013 (2013) https://www.legislation.gov.uk/ukpga/2013/10/enacted; Hill Metal Recycling, Scrap Metal Laws in the UK (2013)

More generally, Canada needs to think carefully about the reliability and resiliency balance. Many critical services failed during the Rogers outage. This included transport, immigration, health and payment systems. In promoting resiliency, the government, and the regulator, must engage with other critical industries that increasingly rely on telecommunication infrastructure. It is simply not enough to use the sticking plaster of cooperation when this may have serious side-effect or, at the very least, mean that more public funding is needed to incentivize resilient deployment. Somebody, somewhere, needs to have the whole elephant in view: calculating the necessary level of expenditure, from whatever source, to offset potential risks with appropriate contemporary costs but having first seen can be done to reduce the risk without relying on the perfection of infrastructure. The saying is not, after all, 'put all your eggs in one basket and then really protect that basket'.

Insofar as market competition is concerned as a driver of resiliency, Canada should be aware of its outlier status first in its privileged position of having more facilities-based competition than other jurisdictions but also in talking about resiliency at the same time as discussing more forms of virtual competition that do not rely on infrastructure. No other country appears to be trying to tie the two together, and it is important that the government have a view of how they fit together. If the competitive effect of a wholesale regime is to undermine resilient builds, the question has to be whether this a price worth paying or if capital should come from somewhere else.

This raises the issue of other sections of the private sector and resiliency, and in particular businesses providing services over the internet. As a first point, it would make sense to think about resiliency in *all* sectors of the economy in order to prevent over reliance on telecommunications. A reasonable question, in particular, is why resiliency ideas currently under discussion do not entertain the imposition of obligations on entities that provide OTT communication services. These can provide other, important additional points of failure, not just for consumers but for business as well. Furthermore, to the extent that more capital is need to efficiently build resilient networks, the models considered in other jurisdictions such as South Korea and the EU could be worth investigating given that the funds raised would come from those entities putting most pressure on infrastructure and benefitting from Canadian's reliance on their services which creates the resiliency problem in the first place.

Regarding consumer compensation, the way that mandatory compensation appears to work in other jurisdictions is that it provides a token sum for pretty serious outages and does not come close to compensating consumers for the harm done. It's not financially possible and nor would it engender sensible resiliency policy within companies. It would also create a barrier to entry for small companies that can't possibly cover significant liabilities if a problem arises. One would also have to make significant carve-outs for many of the reasons that Canadians suffer outages each year, given severe weather. It's also difficult to reconcile a compensation mechanism with roaming granted on such loose terms during an outage under the existing MoU. It doesn't appear that such a compensation scheme would work, nor that it's worth trying to make it work in Canada.

As concerns public funding, while many of the existing funds in Canada can contribute to diversifying facilities, promoting facilities based competition and building resilient infrastructure, it should be noted that there is no agreed level of what counts as 'resilient'. While detailed regulation is unnecessary, it is important that funding bodies specify what the government's goal is if they are to attract sensible applications.

On the topic of broader regulation, an observe and order model is probably preferable to either a goals-based standard or detailed technical requirements so long as it is applied consistently. Other jurisdictions appear to have made this work well by tying the standards used to international best practice, and using that to inform decision-making, risk assessments, etc. Whether C-26 as currently conceived is the right vehicle for the regulation of this issue shall be left for another paper.

Finally, there appear to be two easy wins on the table for improving resiliency in Canada that do not require the teasing out of a complex balance between public and private sector incentives and funding. Canada already has a project ongoing concerning the establishment of a Public Safety Broadband Network. Other countries have successfully established these mechanism, but they take time. In the interests of long term resiliency, however, there doesn't seem to be another policy that other countries have implemented that could so dramatically improve the ability to respond to emergencies. Secondly, many countries are dealing with the issue of cable theft, and the UK has taken some steps to address the issue. Canada can go further in attempting to tackle this problem than other countries and address a significant problem faced by operators, for which the government is the only real answer.

While it is clear that resiliency and reliability, and all the different elements therein, have not been comprehensively explore in this paper, nonetheless what is striking are the number of dimensions of the problem that appear when it is considered in detail. Future research should examine more closely practices of data collection on outages, stipulations on funding, further consumer rights, and the role of satellite.

Bibliography

- ACCAN, Compensation for telecommunications outages (2016) https://accan.org.au/media-centre/hot-issues-blog/1231-compensation-for-telecommunications-outages
- Adena, A, Rogers to spend $150 million on customer credits after July 8 outage (2022) https://www.ctvnews.ca/business/rogers-to-spend-150-million-on-customer-credits-after-july-8-outage-1.6003851
- Adena, A, Rogers to spend $150 million on customer credits after July 8 outage (2022) https://www.ctvnews.ca/business/rogers-to-spend-150-million-on-customer-credits-after-july-8-outage-1.6003851
- Advisory Panel on Development of Digital Infrastructure (DC, etc.), Announcement of the Interim Report of the Advisory Panel on Development of Digital Infrastructure (DC, etc.) (2020) https://www.soumu.go.jp/menu_news/s-news/01kiban04_02000197.html
- Airwave, Emergency Services Network (2023) https://www.airwavesolutions.co.uk/the-service/emergency-services-network/
- Araki, N, ICT Standardization Trends for Disaster Relief, Network Resilience, and Recovery ITU-T (2018) NTT Technical Review, 16(10): 77-82, https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201810gls.html
- Australian Government, Telecommunications (Customer Service Guarantee) Standard 2011 (2011) https://www.legislation.gov.au/Series/F2011L00413
- Australian Government: Department for Infrastructure Transport, Regional Development, Communications and Arts, Mobile Network Hardening Programme (2023) https://www.infrastructure.gov.au/media-communications-arts/phone/mobile-network-hardening-program
- Australian Government: Department for Infrastructure Transport, Regional Development, Communications and Arts, Communications in emergencies and natural disasters (2021) https://www.infrastructure.gov.au/media-communications-arts/phone/communications-emergencies-and-natural-disasters

- Australian Government: Department for Infrastructure Transport, Regional Development, Communications and Arts, Mobile Network Hardening Programme (2023) https://www.infrastructure.gov.au/media-communications-arts/phone/mobile-network-hardening-program
- Australian Government: Department of Infrastructure, Transport, Regional Development, Communications and Art, Provision of Satellite Connections to Emergency Services and Evacuation Centres https://www.infrastructure.gov.au/media-communications-arts/phone/provision-satellite-connections-emergency-services-and-evacuation-centres
- Bank of England, Building Operational Resilience and Impact Tolerances for Important Business Services (2021) https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/publication/2021/building-operational-resilience-impact-tolerances-for-important-business-services.pdf
- BEREC, BEREC preliminary assessment of the underlying assumptions of payments from large CAPs to ISPs (2022) https://www.berec.europa.eu/system/files/2022-10/BEREC%20BoR%20%2822%29%20137%20BEREC_preliminary-assessment-payments-CAPs-to-ISPs_0.pdf
- Boureau, M, Feasey R, Addressing Threats to Digital Infrastructure (2022) in CERRE, *Global Governance for the Digital Econsystems* (2022) 143-178, 155.
- Bundesrat, Telecommunications Modernization Act (Telekommunikationsmodernisierungsgesetz) (2021) (Sec. 58 (2) sentence 1 TKG)
- California Public Utilities Commission, Decision 21-02-029 (2021) S 5.4.4. https://docs.cpuc.ca.gov/PublishedDocs/Published/G000/M366/K625/366625041.PDF
- Canadian Radio-television and Telecommunications Commission, Broadband Fund: About the Broadband Fund (2023) https://crtc.gc.ca/eng/internet/fnds.htm
- Canadian Radio-television and Telecommunications Commission, Canadian Common Carrier Ownership and Control Requirements (2010) https://crtc.gc.ca/eng/dcs/current/faq_57.htm
- Canadian Radio-television and Telecommunications Commission, Communications Market Reports (2023) https://crtc.gc.ca/eng/publications/reports/PolicyMonitoring/
- Canadian Radio-television and Telecommunications Commission, Telecom Regulatory Policy CRTC 2021-130 (2021) https://crtc.gc.ca/eng/archive/2021/2021-130.htm; Canadian Radio-television and Telecommunications Commission, Telecom Notice of Consultation CRTC 2023-56: Notice of hearing – Review of the wholesale high-speed access service framework (2023) https://crtc.gc.ca/eng/archive/2023/2023-56.htm
- Canadian Radio-television and Telecommunications Commission, Telecom Notice of Consultation CRTC 2023-39: Call for comments – Development of a regulatory framework to improve network reliability and resiliency – Mandatory notification and reporting about major telecommunications service outages (2023) https://crtc.gc.ca/eng/archive/2023/2023-39.htm
- Canadian Radio-television and Telecommunications Commission, Telecom Notice of Consultation CRTC 2022-147-2: Telecommunications in the Far North, Phase II (2022) https://crtc.gc.ca/eng/archive/2022/2022-147-2.htm
- Canadian Radio-television and Telecommunications Commission, Telecom Notice of Consultation CRTC 2023-89: Call for comments – Broadband Fund policy review (2023) https://crtc.gc.ca/eng/archive/2023/2023-89.htm
- Canadian Radio-television and Telecommunications Commission, Telecom Regulatory Policy CRTC 2021-130 (2021) https://crtc.gc.ca/eng/archive/2021/2021-130.htm
- Canadian Radio-television and Telecommunications Commission, Telecom Notice of Consultation CRTC 2023-56: Notice of hearing – Review of the wholesale high-speed access service framework (2023) https://crtc.gc.ca/eng/archive/2023/2023-56.htm
- Canadian Telecommunications Network Resiliency Working Group, Telecommunications Network Resiliency in Canada: A Path Forward (2023) https://ised-isde.canada.ca/site/spectrum-management-telecommunications/sites/default/files/attachments/2023/CTNR%20Recommendations%20v1.0%20Final%20(EN).pdf
- CBC News, No power overnight for some B.C. Hydro customers, Bell's mobile network also damaged (2021) https://www.cbc.ca/news/canada/british-columbia/service-outage-bc-storm-1.6249986

- Christensen Associates, Key Cost Drivers of Mobile Wireless Services in Canada: Implications for Pricing (2020) https://www.lrca.com/wp-content/uploads/2020/10/Key-Cost-Drivers-of-Mobile-Wireless-Services-in-Canada-Implications-for-Pricing-US-Included.pdf
- Clou, S, Cable theft: A growing problem around the world (2023) https://www.smart-energy.com/industry-sectors/energy-grid-management/cable-theft-a-growing-problem-around-the-world/
- Coscelli, A, Thompson, G, Resilience and Competition Policy: Economics working paper (2022) United Kingdom Competition and Markets Authority, p 4 https://www.gov.uk/government/publications/resilience-and-competition-policy-economics-working-paper
- Crandall Robert, How Canada's wireless spectrum policy drives up mobile rates (2022) Policy Options https://policyoptions.irpp.org/magazines/october-2021/how-canadas-wireless-spectrum-policy-drives-up-mobile-rates/
- CTV, What we know about the network system failure that led to the Rogers outage (2022) https://www.ctvnews.ca/business/what-we-know-about-the-network-system-failure-that-led-to-the-rogers-outage-1.5982790
- European Commission, The Recovery and Resiliency Facility (2023) https://commission.europa.eu/business-economy-euro/economic-recovery/recovery-and-resilience-facility_en
- European Parliament and The Council of the European Union, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (2022) OJ L 333, 27.12.2022, p. 80–152 https://eur-lex.europa.eu/eli/dir/2022/2555
- European Parliament and the Council of the European union, DIRECTIVE (EU) 2018/1972 establishing the European Electronic Communications Code (2018) https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1547633333762&uri=CELEX%3A32018L1972
- European Parliament and the Council of the European Union, Regulation of The European Parliament and of The Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (2022) OJ L 333, 27.12.2022, p. 1–79
- Evans, P, Rogers says services mostly restored after daylong outage left millions offline (2022) CBC https://www.cbc.ca/news/business/rogers-outage-cell-mobile-wifi-1.6514373
- Farooqui S et al, Industry Minister to meet with telecoms after 'unacceptable' Rogers outage (2022) Globe and Mail, https://www.theglobeandmail.com/business/article-2022-rogers-communications-outage/
- Federal Bureau of Investigation, Copper Thefts Threaten U.S. Critical Infrastructure (2008) Intelligence Assessment (unclassified) https://www.fbi.gov/stats-services/publications/copper-thefts
- Federal Communications Commission, Report and Order and Further Notice of Proposed Rulemaking (2022) FCC 22-50 https://docs.fcc.gov/public/attachments/FCC-22-50A1.pdf
- Federal Communications Commission, Report and Order and Further Notice of Proposed Rulemaking (2022) FCC 22-50
- Federal Communications Commission, Wireless Network Resiliency During Disasters (2022) https://www.fcc.gov/wireless-network-resiliency-during-disasters
- Finextra, Rogers outage shuts down Canadian banks' ATMs, POS and internet banking (2022)
- Firstnet, Frequently Asked Questions (2023) https://www.firstnet.com/faq.html7
- Gadsden, T, Does your provider owe you money for their service outages? (2022) AllConnect https://www.allconnect.com/blog/get-bill-credits-for-service-outages
- Gadsden, T, Does your provider owe you money for their service outages? (2022) AllConnect https://www.allconnect.com/blog/get-bill-credits-for-service-outages;
- Galasso, C., McNair, J., Fujii, M. et al. Resilient infrastructure. Commun Eng 1, 27, 28 (2022). https://doi.org/10.1038/s44172-022-00032-5
- Garrido, E, Whalley, J, Competition in wholesale markets: Do MNOs compete to host MVNOs? (2013) Telecommunications Policy, 37(11) P 1124-1141
- Gheist, M, Responding to the Rogers Outage: Time to Get Serious About Competition, Consumer Rights, and Communications Regulation (2022) https://www.michaelgeist.ca/2022/07/responding-to-the-rogers-outage-time-to-get-serious-about-competition-consumer-rights-and-communications-regulation/

- Globe and Mail, Rogers outage sparks deal in Canada between major telecoms (2022) https://www.ctvnews.ca/politics/rogers-outage-sparks-deal-in-canada-between-major-telecoms-1.6058707
- Gorman, M, N.S. premier blasts telecom companies in wake of Fiona, calls on Ottawa to step in with regulation (2022) CBC https://www.cbc.ca/news/canada/nova-scotia/premier-tim-houston-telecommunications-hurricane-fiona-1.6598450
- Government of Canada, Bill C-26: An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts: Charter Statement (2023) https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c26_1.html
- Government of Canada, Government of Canada delivers on commitment to reduce cell phone wireless plans by 25% (2022) https://www.canada.ca/en/innovation-science-economic-development/news/2022/01/government-of-canada-delivers-on-commitment-to-reduce-cell-phone-wireless-plans-by-25.html
- Government of Canada, Revised Frameworks for Mandatory Roaming and Antenna Tower and Site Sharing (sf10547) (2013) https://ised-isde.canada.ca/site/spectrum-management-telecommunications/en/radiocommunications/mandatory-roaming-and-antenna-tower-and-site-sharing/revised-frameworks-mandatory-roaming-and-antenna-tower-and-site-sharing-sf10547
- Government of Japan, Telecommunications Business Act. (Act No. 86 of December 25, 1984) (1984) Art 8
- Government of Japan, Telecommunications Business Law (2007) https://www.japaneselawtranslation.go.jp/en/laws/view/3648/enArt 41-45
- Government of the Republic of Korea, Telecommunications Business Act, (2011) Art 61 and Government of South Korea, Presidential Decree related to Article 33-(2) of Telecommunications Business Act, (2011) and (2013) Art 22
- Government of the Republic of Korea, Telecommunications Business Act (2021) Art 33
- Government of the United Kingdom, Civil Contingencies Act 2004 (2004) https://www.legislation.gov.uk/ukpga/2004/36/part/2
- Government of the United Kingdom, Scrap Metal Dealers Act 2013 (2013) https://www.legislation.gov.uk/ukpga/2013/10/enacted;
- Government of the United Kingdom, Telecommunications (Security) Act (2001) https://www.legislation.gov.uk/ukpga/2021/31/contents/enacted; OFCOM, Ofcom begins new role overseeing security of telecoms networks (2022) https://www.ofcom.org.uk/news-centre/2022/ofcom-begins-new-role-overseeing-security-of-telecoms-networks#:~:text=Security%20duties,preparing%20for%20any%20future%20risks.
- Hill Metal Recycling, Scrap Metal Laws in the UK (2013)
- https://www.finextra.com/newsarticle/40611/rogers-outage-shuts-down-canadian-banks-atms-pos-and-internet-banking
- Hyo-Jin, L, How emergency communication system failed in Itaewon disaster (2022)T he Korea Times https://www.koreatimes.co.kr/www/nation/2023/06/113_339282.html
- Ian Scott, Speech to CTS (Nov, 2022)
- Innovation, Science and Economic Development Canada, Memorandum of Understanding on Telecommunications Reliability (2023) https://ised-isde.canada.ca/site/ised/en/memorandum-understanding-telecommunications-reliability;
- Innovation, Science and Economic Development Canada, Memorandum of Understanding on Telecommunications Reliability (2023) https://ised-isde.canada.ca/site/ised/en/memorandum-understanding-telecommunications-reliability
- Jackson, D, UK officials acknowledge ESN risks, hope to complete public-safety broadband project by 2030 (2023) IWCE'S Urgent Communications https://urgentcomm.com/2023/04/13/uk-officials-acknowledge-esn-risks-hope-to-complete-public-safety-broadband-project-by-2030/
- Kellezi, P, Magic Numbers and Merger Control in the Telecommunications Sector (2015) CPI Antitrust Chronicle, 11(1).
- Kim, J, Et al, E-Resilience: A Review of National Broadband Policies, Regulations, Strategies and Initiatives of China, Japan, and the Republic of Korea (2018) Asia-Pacific Information Superhighway (AP-IS) Working Paper Series https://www.unescap.org/sites/default/files/e-Resilience_CJK_final.pdf
- Lamont, J, Rogers outage class action request likely to be heard in June (2023) https://mobilesyrup.com/2023/03/31/rogers-outage-class-action-likely-heard-june-2023/

- Manidaki, K, Net Neutrality Regulation in the EU: Competition and Beyond (2019) Journal of European Competition Law & Practice 10(7) 479–488, https://doi.org/10.1093/jeclap/lpz049;
- Ministry of the Interior and Safety, Disaster and Safety Communications Network (Korea Safe-net) (2021)
- Moon-Hee, C, Netflix Still Refusing to Pay for Network Use (2022) http://www.businesskorea.co.kr/news/articleView.html?idxno=89261;
- National Telecommunications and Information Administration, Biden-Harris Administration Launches $1.5 Billion Innovation Fund to Develop a More Competitive and Diverse Telecommunications Supply Chain (2023)
- NBN, About NBN Co (2022) https://www.nbnco.com.au/corporate-information/about-nbn-co
- OFCOM, Automatic compensation: What you need to know (2023) https://www.ofcom.org.uk/phones-telecoms-and-internet/advice-for-consumers/costs-and-billing/automatic-compensation-need-know
- OFCOM, Communications Providers' Voluntary Code of Practice for an Automatic Compensation Scheme (2021) https://www.ofcom.org.uk/__data/assets/pdf_file/0026/216962/Industry-Code-of-Practice-for-Automatic-Compensation.pdf
- Posadzki, A, Rogers outage may weigh on decision around $26-billion takeover of Shaw, Champagne says (2022) Globe and Mail https://www.theglobeandmail.com/canada/article-house-of-commons-committee-to-study-rogers-network-outage-impacts-and/
- PWC, The Importance of a Healthy Telecommunications Industry to Canada's High Tech Success (2020) p10 *available on request*
- PWC. The global economic impact of 5G. (2021) https://www.pwc.com/gx/en/tmt/5g/global-economic-impact-5g.pdf
- Reuters, Eastern Canada's Halifax declares emergency over wildfire (2023) https://nypost.com/2023/05/29/eastern-canadas-halifax-declares-emergency-over-wildfire/
- Sasktel, About Us (2023) https://www.sasktel.com/about-us/company-info/vision-mission-and-values/history-site/history
- See: European Commission, Questions and Answers: Digital Markets Act: Ensuring fair and open digital markets (2023) https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2349
- Soni, A, Mehta, C, Canada clears C$20 bln Rogers-Shaw deal with tough conditions (2023) Reuters https://www.reuters.com/markets/deals/canadas-decision-rogers-shaw-deal-may-come-friday-2023-03-31/
- Statistics Canada, Canada's Population Clock (2023) https://www150.statcan.gc.ca/n1/pub/71-607-x/71-607-x2018005-eng.htm
- Statistics Canada, Infrastructure Statistics Hub (2023) https://www150.statcan.gc.ca/n1/pub/71-607-x/71-607-x2018013-eng.htm
- TELUS Communications, Reforming Canadian spectrum policy for 5G and beyond (2022) telus.com/spectrumpolicy
- Temporary National Coordination Office, A Public Safety Broadband Network (PSBN) for Canada (2022) https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-psbn/2021-psbn-en.pdf
- The Mainichi, Japanese telecom giant KDDI to pay $1.50 to 35.89 mil. users in apology for network outage (2022) https://mainichi.jp/english/articles/20220729/p2a/00m/0bu/016000c#:~:text=TOKYO%20%2D%2D%20Japanese%20telecom%20firm,company%20announced%20on%20July%2029.
- World Bank, Climate Change Knowledge Portal: Canada (2023) https://climateknowledgeportal.worldbank.org/country/canada/climate-data-historical#:~:text=Canada%20has%20a%20wide%20range,cold%20winters%20and%20warm%20summers).
- Yonhap, By, S. Korea requires Google, Netflix and 3 others to provide stable online services this year (2022) https://www.koreaherald.com/view.php?ud=20220203000618
- Zimmer, B, The Protection of Net Neutrality in Canada (2018) Report of the Standing Committee on Access to Information, Privacy and Ethics https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9840575/ethirp14/ethirp14-e.pdf