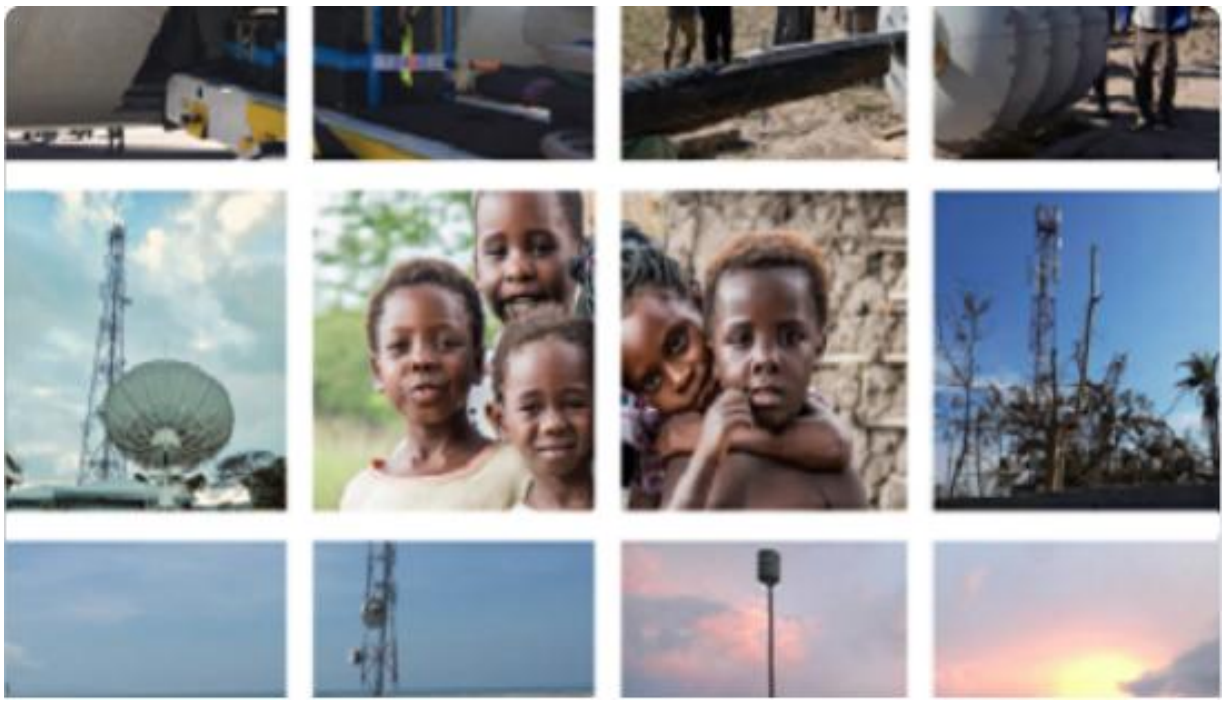
Building Resilient National ICT Infrastructure in Asia and the Pacific: Leading Practices for Addressing the Gaps



Connect2Recover

August 2024 (Updated in September 2025)

Acknowledgements

This report was prepared for the International Telecommunication Union (ITU) by Christine Apikul, under the guidance of the Regional Director, Atsuko Okuda, and Program Officer, Aamir Riaz, of the ITU Regional Office for Asia and the Pacific, with inputs from Amila Amunugama, Hasan Shaina, Jody Van Wyk, Amélie Grangeat, and Karen Woo. ITU acknowledges the continued collaboration and support of the Department of Infrastructure, Transport, Regional Development, Communications, Sport, and the Arts, Australia, in strengthening ICT infrastructure resilience in Asia and the Pacific region.

Table of Contents

Abbreviations and Acronyms

BPC	Bhutan Power Corporation
BTL	Bhutan Telecom Limited
CAP	Common Alerting Protocol
D2D	Direct-to-Device
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DSL	Digital Subscriber Line
DTH	Direct-to-Home
ESCAP	Economic and Social Commission for Asia and the Pacific
EW4All	Early Warnings for All
FTTH	Fibre-to-the-Home
FTTx	Fibre-to-the-x
GEO	Geostationary Orbit
GMDSS	Global Maritime Distress and Safety System
GNI	Gross National Income
GPRS	General Packet Radio Service
GSMA	Global System for Mobile Communications Association
HF	High Frequency
HHI	Herfindahl-Hirschman Index
ICT	Information and Communication Technology
ITU	International Telecommunication Union
IXP	Internet Exchange Point
LDC	Least Developed Country
LEO	Low-Earth Orbit
LLDC	Landlocked Developing Country
LTE	Long-term Evolution
MEO	Medium-Earth Orbit
MOCN	Multi-operator Core Network
MORAN	Multi-operator Radio Access Network

MVNO	Mobile Virtual Network Operator
NETP	National Emergency Telecommunication Plan
NICTA	National Information and Communications Technology Authority
NR	New Radio
PAGASA	Philippine Atmospheric, Geophysical and Astronomical Services Administration
PPDR	Public Protection and Disaster Relief
PTA	Pakistan Telecommunication Authority
RAN	Radio Access Network
SDG	Sustainable Development Goal
SIDS	Small Island Developing States
SMS	Short Message Service
UNDRR	United Nations Office for Disaster Risk Reduction
VHF	Very High Frequency
VSAT	Very Small Aperture Terminal
WMO	World Meteorological Organization
WWW	Women's Weather Watch
WWW	World Wide Web

Executive Summary

ITU implemented a project titled "Connect2Recover – Digital infrastructure and ecosystem reinforcement against COVID-19 in Asia-Pacific" in partnership with the Department of Infrastructure, Transport, Regional Development and Communications (DITRDC) of Australia. As part of the project activities, this study was conducted to support ITU membership in strengthening the resilience of the national ICT infrastructure while keeping the costs of services affordable.

Resilience of the national information and communication technology (ICT) infrastructure can be defined as the ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate, and recover from incidents.[1] These incidents, whether natural or human-induced, accidental or intentional, include multiple, sometimes compounding threats such as disasters, pandemics, and conflicts, as well as network or power outages and communication cable cuts. As other critical infrastructures increasingly rely on the ICT infrastructure to function and deliver services to populations, building national ICT infrastructure resilience also protects other critical infrastructures in sectors such as transport, energy, or healthcare.

Under the project, a framework was developed to assess the resilience of a country's ICT infrastructure and services. This framework helps to identify gaps in the national ICT infrastructure to prioritize actions and investments that will contribute to improving the country's overall ICT infrastructure resilience. The framework prepared for country assessments under the project is unique in that it is linked to ITU's strategies and priorities and supports the ITU and its Member States, particularly least developed countries (LDCs), landlocked developing countries (LLDCs), and small island developing States (SIDS), in accelerating progress towards building resilient national ICT infrastructure. The framework comprises a set of questions and indicators across four pillars: (i) network resilience; (ii) affordability of ICT; (iii) emergency preparedness; and (iv) early warning dissemination and communication.

This report is intended to serve as a knowledge resource for policymakers, regulators, telecom service providers, and investors from ITU membership from Asia and the Pacific (ASP) region and beyond, to support the development of affordable and resilient national ICT infrastructure. The report covers:

1. Background on the importance of resilient and affordable ICT infrastructure and its socio-economic impact.
2. Key areas to be covered in assessing the resilience of ICT infrastructure and the affordability of services.
3. Analysis of case studies from Asia and the Pacific countries and potential gaps.
4. Recommended best practices (policy, regulatory, infrastructure development) in improving infrastructure resilience and affordability of ICT services.

Network Resilience: This pillar looks at the types of connectivity in different parts of the network and their usage. It also checks the security of domain names and the allocation of spectrum for emergency communications. The analysis shows that network resilience is generally limited in these countries i.e LDCs, LLDCs and SIDS.

[1] The Critical Entities Resilience Directive (CER). Available at https://www.critical-entities-resilience-directive.com/ (accessed on 28 August 2024).

ICT Affordability: This pillar assesses the cost of mobile data, fixed-broadband, smartphones, and feature phones. It also considers market factors and policies for rural areas. Bhutan offers the most affordable mobile and fixed-broadband services among the four countries examined in this study but smartphones are expensive across all four countries.

Emergency Preparedness: This pillar examines the government's preparedness to handle risks to ICT infrastructure. It looks at policies for cybersecurity, data protection, business continuity, and disaster recovery. Most countries have policies in place, but only two have national emergency telecommunication plans, and many lack measures for a backup power supply.

Early Warning Dissemination and Communication: This pillar is based on 42 questions from a global checklist, initially validated by ITU member countries of Asia and the Pacific in 2023, focusing on governance, infrastructure, inclusivity, and trust of early warning systems. Most countries need to improve data collection and sharing for better decision-making.

Four countries, Bhutan, Lao PDR, Nepal, and the Philippines, were selected to undertake country assessments using this framework, based on requests received and the availability of data. Bhutan, Lao PDR, and Nepal are classified as Landlocked Developing Countries (LLDCs). While the Lao People's Democratic Republic (PDR) and Nepal remain Least Developed Countries (LDCs), Bhutan graduated from its LDC status in December 2023[2]. The Philippines, with its many islands, shares challenges similar to those faced by Small Island Developing States (SIDS).

Drawing on the framework employed in the project to assess the resilience of national ICT infrastructure, alongside best practices and case studies highlighted in the report, the following recommendations across the four key pillars are proposed for ITU Member States' consideration:

Bridging the Data Gaps

A key insight from this study is the lack of sufficient and accessible ICT data to comprehensively evaluate the resilience of the national ICT infrastructure. A crucial recommendation for future progress is to establish a systematic approach for collecting, analyzing, and sharing disaggregated data to measure and monitor advancements in strengthening the resilience of the national ICT infrastructure, aligned with the framework utilized for country assessments in the project. More specifically:

- Review the ICT indicators and develop standardized measures for the different types of connectivity (e.g., fixed wireless, satellite), the quality of users' experience across the different types of connectivity, and the affordability of both devices and data plans.
- Support capacity building of national and local organizations in data collection, analysis, and sharing of relevant disaggregated quantitative and qualitative data for informed decision-making, especially for designing and improving early warning dissemination and communication and assessing its effectiveness and inclusion (i.e., vulnerable groups' ability to receive, comprehend and act on the alerts).
- Establish data frameworks and mechanisms for data collection, analysis, and sharing, ensuring interoperability between systems, and incorporating safeguards such as cybersecurity, privacy, and data protection.

[2] UN office of the high representative for the LDCs, LLDCs, and SIDS. Available at https://www.un.org/ohrlls/content/list-lldcs#:~:text=RepublicOpens%20a%20new%20window,Publications

Network Resilience

To enhance network resilience, it is essential to adopt the United Nations Principles for Resilient Infrastructure as a foundation for both the development of new systems and the upgrading of existing ones. A comprehensive approach combining policies, regulations, incentives, and public financing should be implemented to accelerate ICT infrastructure development and expand broadband access to unserved and underserved areas. This effort should include exploring the potential of advanced technologies such as fixed wireless access, high-altitude platform station systems, balloons, drones, and satellite systems—including geostationary orbit (GEO), medium-Earth orbit (MEO), and low-Earth orbit (LEO)—to enhance connectivity and improve emergency preparedness.

National regulatory frameworks must be established to enable the deployment of these technologies while ensuring fair pricing, competition, operational transparency, and compliance with human rights laws. Encouraging the co-deployment of ICT infrastructure with other critical infrastructures, such as roads, railways, power transmission lines, and pipelines, can optimize resource use and enhance connectivity. Digital mapping of regional and national infrastructure assets and promoting cross-sectoral data sharing are also critical for improved planning and coordination.

Creating a favorable investment environment and streamlining business processes will attract private sector and foreign investment in ICT infrastructure development. Mechanisms should be established to mandate risk and resilience assessments as integral components of national ICT infrastructure projects. Policies should support the establishment and operation of Internet exchange points (IXPs) and high-quality Tier 4 data centers in diverse locations, including areas outside capital cities, with risk-informed site selection and standards prioritizing resilience, energy efficiency, renewable energy integration, and both cybersecurity and physical security.

To further strengthen resilience, capacity building and incentives should be provided for deploying Domain Name System Security Extensions (DNSSEC) and increasing its validation rates. Additionally, spectrum allocation for Global Maritime Distress and Safety Systems (GMDSS), public protection and disaster relief (PPDR) agencies, and amateur radio operators should be dedicated and harmonized to ensure cross-border mobility and extensive geographic coverage during emergencies. These measures collectively aim to establish a robust and resilient ICT infrastructure capable of withstanding various challenges and supporting national development.

ICT Affordability

To increase ICT affordability, it is crucial to adopt policies and regulations that promote and incentivize both passive and active infrastructure sharing. These arrangements should be closely monitored to detect and prevent collusion, anti-competitive behavior, and potential impacts on network resilience. Measures to enhance competition in the telecommunications market, such as facilitating the entry of new players like mobile virtual network operators (MVNOs) and satellite operators, should also be explored. Technologies like multi-operator core networks (MOCN) and multi-operator radio access networks (MORAN) should be promoted to improve spectral efficiency and optimize resource utilization.

National broadband plans and ICT policies should include specific targets aimed at improving the affordability of ICT devices and data plans. Evidence-based policies and interventions must be developed and implemented to address cost barriers effectively. Affordability efforts should be part of

a comprehensive strategy that tackles interconnected challenges, including the lack of digital literacy and skills, insufficient relevant content and services, online threats and risks, and societal and gender norms that hinder ICT adoption. These recommendations collectively aim to make ICT more accessible and inclusive for all.

Emergency Preparedness

To ensure preparedness for emergency telecommunications, it is essential to develop and enact comprehensive cybersecurity, data protection, and privacy legislation, if not already in place, and implement a National Emergency Telecommunication Plan (NETP) aligned with ITU guidelines. Efforts should include placing Domain Name Systems (DNS) servers at geographically and topologically diverse locations to reduce the risk of single points of failure and incentivizing service providers to implement adaptive restoration, adaptive reallocation, and predictive analytics to proactively address potential network congestion, hardware failures, and other issues.

Establishing or designating an entity responsible for national ICT infrastructure resilience and emergency preparedness is critical for coordinated efforts. Standards for the quality of ICT services during emergencies should be developed and monitored for compliance. Additionally, infrastructure sharing among network operators should be mandated during emergencies, allowing users to connect to any operational tower, regardless of ownership. Network operators must also establish robust institutional structures and plans for business continuity and disaster recovery, including maintaining power backups and ready-to-deploy communication and power solutions.

Incorporating privacy-by-design and security-by-design principles in technology deployments is vital to ensuring secure and resilient systems. Collaboration with network operators, private sector entities, and civil society organizations representing vulnerable groups should be prioritized for effective emergency preparedness and response. Regular drills engaging these stakeholders can further enhance readiness.

Efforts to enhance resilience should also focus on strengthening power infrastructure and planning for increased energy demands to support ICT systems, including data centers, in a sustainable manner by promoting renewable energy use. Finally, artificial intelligence should be leveraged for disaster connectivity mapping to optimize resource deployment and response strategies. These measures collectively aim to fortify emergency telecommunication systems and ensure their reliability during crises.

Early Warning Dissemination and Communication

To strengthen warning dissemination and communication, it is crucial to adopt international standards, such as the Common Alerting Protocol (CAP), for early warning systems. Comprehensive studies should be commissioned to assess the current reach of early warning alerts, identify dissemination gaps, and ensure accessibility for vulnerable groups, including persons with disabilities, women, older persons, children, and ethnic minorities. Evidence-based policies, regulations, and standard operating procedures must be established to generate and issue warnings that are inclusive and accessible to all.

Early warning systems should employ multiple communication channels, incorporating low-tech and no-tech solutions to reach diverse audiences effectively. Understanding the access, use, behaviors, and perceptions of at-risk groups regarding ICT is essential for selecting appropriate communication

methods. Formal mechanisms should be created to involve key stakeholders, such as businesses, infrastructure operators, community leaders, local governments, and civil society organizations representing vulnerable groups, in the design and implementation of early warning systems. Engaging media and private sector entities, including mobile network operators, is also vital, with an emphasis on exploring technologies like cell broadcasting and location-based SMS services.

Regular monitoring and evaluation of early warning dissemination strategies should be conducted along parameters such as timeliness, accuracy, relevance, and actionability, with a particular focus on the needs of vulnerable populations. A shift from general warnings to impact-based warnings that provide actionable information about hazard impacts is recommended to improve response outcomes. Capacity-building initiatives should empower organizations representing vulnerable groups to complement and enhance government-led efforts, ensuring warnings are inclusive, accessible, and actionable for all.

Additionally, early warning system planning and design must account for the maintenance and operational costs of systems and equipment, ensuring long-term functionality and reliability. These measures aim to create a robust, inclusive, and effective framework for early warning dissemination and communication.

1. Introduction: What is Resilient ICT Infrastructure and Why it Matters

Purpose and Outline of Report

To address the objectives of the project, a draft framework was developed to assess the resilience of a country's ICT infrastructure and services. This framework identifies gaps in national ICT systems to prioritize actions and investments that enhance overall resilience. Detailed in Section 2 of this report, the framework includes questions and indicators across four pillars.

1.1 What is Resilient ICT Infrastructure

Resilience of the national information and communication technology (ICT) infrastructure can be defined as the ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate, and recover from incidents.[3] These incidents, whether natural or human-induced, accidental or intentional, include multiple, sometimes compounding threats such as disasters, pandemics, and conflicts, as well as network or power outages and communication cable cuts. Strategies for national ICT infrastructure resilience include ensuring redundancy and diversity of network routes and equipment (e.g., deploying hybrid mesh and ring structure networks), setting up backup services for emergency response efforts, meeting surges in demand, and providing and maintaining an acceptable level of service during crises and emergencies. Other strategies are related to the speed and scale at which services can be restored and recovered, and the risk assessments and preparedness planning required.

The **ICT infrastructure** that includes the first, middle, and last mile needs to be able to manage a wide range of risks and threats (Figure 1).

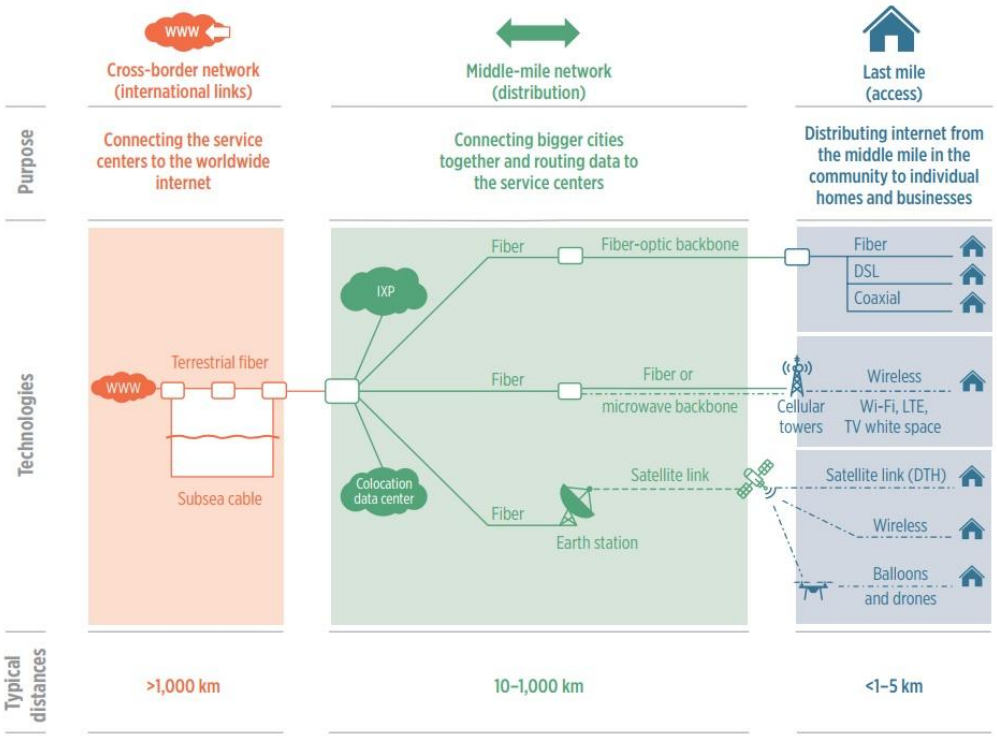


Figure 1: The ICT infrastructure

[3] The Critical Entities Resilience Directive (CER). Available at https://www.critical-entities-resilience-directive.com/ (accessed on 28 August 2024).

Notes: DSL = Digital Subscriber Line; DTH = Direct-to-Home; IXP = Internet Exchange Point; LTE = Long-term Evolution; WWW = World Wide Web (Internet).

Source: World Bank, *World Development Report 2021: Data for Better Lives* (Washington DC, 2021). Available at https://wdr2021.worldbank.org/.

The **international network (first mile)** is the point where the Internet enters a country, consisting of components like submarine cables, landing stations, satellite dishes, cross-border microwave and fibre links, and domain name systems (DNS). Countries must connect via submarine cables or cross-border terrestrial links, particularly landlocked nations. Route diversity and sufficient capacity to global hubs are crucial for ICT infrastructure resilience.

The **national backbone network (middle mile)** transmits Internet traffic across a country. High-speed Internet from the border is distributed through fibre backbones to urban and rural areas and further extended via backhaul or metro networks. Key components include fibre-optic cables, copper wires, microwave, satellite links, Internet exchange points (IXPs), data centres, and cloud platforms. Diverse, high-capacity links are essential for resilience.

The **last mile** connects users to broadcasting, communication, and Internet services through various technologies, such as fibre-to-the-x (FTTx), DSL, hybrid fibre coaxial (HFC), fixed wireless access, mobile networks (2G, 3G, 4G, and 5G), and satellite broadband. These diverse options empower users to choose solutions that best suit their needs, ensuring access continuity, especially during crises or emergencies.

1.2 Why Resilient ICT Infrastructure matters in Asia and the Pacific

Asia and the Pacific continues to be the world's most disaster-prone region. In 2022, Tonga experienced major disruptions when a volcanic eruption severed its only fibre-optic cable[4] leaving the nation without Internet connectivity for over a month. More recently, in Bangladesh, a power outage due to cyclone Remal caused over 10,000 mobile towers to go out of service in 2024.[5]

Over the past decades, climate change has increased the frequency and severity of floods, cyclones, heatwaves, droughts, and earthquakes in the region.[6] Between 2015 and 2021, the number of critical infrastructure units and facilities destroyed or damaged by disasters averaged 55,964 per year in Asia and the Pacific.[7] According to a report of the United Nations Economic and Social Commission for Asia and the Pacific (ESCAP), climate-induced disaster risk is outpacing the region's resilience, with current

[4] Tom Bateman, "Tonga is finally back online. Here's why it took 5 weeks to fix its volcano-damaged Internet cable", Euro News, 23 February 2022. Available at https://www.euronews.com/next/2022/02/23/tonga-is-finally-back-online-here-s-why-it-took-5-weeks-to-fix-its-volcano-damaged-interne.

[5] Mahmudul Hasan, "Cyclone disrupts 10,000 telecom towers, millions out of service", The Daily Star, 27 May 2024. Available at https://www.thedailystar.net/business/news/cyclone-disrupts-10000-telecom-towers-millions-out-service-3620101.

[6] ESCAP, *Seizing the Moment: Targeting Transformative Disaster Risk Resilience – Asia-Pacific Disaster Report 2023* (Bangkok, 2023). Available at https://www.unescap.org/kp/2023/seizing-moment-targeting-transformative-disaster-risk-resilience.

[7] UNDRR, *The Midterm Review of the Implementation of the Sendai Framework for Disaster Risk Reduction 2015–2030: Regional Report for Asia-Pacific* (Geneva, 2023). Available at https://www.undrr.org/publication/regional-report-midterm-review-implementation-sendai-framework-disaster-risk-reduction.

annual losses from disasters and extreme climate events forecast to increase, undermining productivity and increasing inequality.[8]

Infrastructure is one of the sectors most affected by disasters. An analysis of post-disaster needs assessments in the Pacific between 2011 and 2020 shows that damage and losses to infrastructure accounted for about USD 1.45 billion or 37 per cent of the total damage and losses of the major disasters in this period.[9] It is expected that climate change will exacerbate this trend due to sea-level rises, storm surges, and swells, amongst others. This is reflected in the increasing adaptation costs for coastal protection, which, for example, amount to USD 329 million per year in Fiji (3 per cent of gross domestic product) and to USD 58 million per year in the Marshall Islands (13 per cent of gross domestic product).[10]

At the same time, the region is grappling with rising global geopolitical tensions and armed conflicts, resulting in economic uncertainty, insecurity (including cyber insecurity), and the undermining of trust.[11] Cyberthreats that are non-deliberate (e.g., system outage, cable damage) or malicious (e.g., cyberwarfare, ransomware) are on the rise. For example, the Republic of Korea experienced an outage of its government network for two days in 2023, denting the country's digital reputation.[12] In the same year, in Singapore, a distributed denial-of-service attack caused an online service outage that affected several public healthcare institutions.[13] The World Economic Forum forecasts that cyberattacks will shift targets toward less digitally literate individuals and less secure infrastructure and systems in the coming years.[14]

Societies have become highly reliant on connectivity and digital technologies for everyday needs, education, work, commerce, and social activities. Moreover, the need for information sharing, communication, and online transactions intensifies during crises and emergencies. During the COVID-19 pandemic, ICT played a vital role in keeping people informed and curbing the spread of the virus, allowing remote working and learning, providing access to essential services, and accelerating research in treatments and vaccines.

Critical infrastructure sectors such as defense, education, energy, healthcare, transportation, water systems, and financial markets are becoming increasingly reliant on Information and Communication Technology (ICT) to function effectively and efficiently. These sectors depend on ICT for everything from real-time data transmission and remote monitoring to automated control systems and decision-making processes. For instance, defense systems rely on secure communication networks for national security operations, while healthcare services use digital platforms for patient records, telemedicine, and emergency response coordination. Similarly, energy grids rely on smart technologies to optimize

[8] ESCAP, *Seizing the Moment: Targeting Transformative Disaster Risk Resilience – Asia-Pacific Disaster Report 2023* (Bangkok, 2023). Available at https://www.unescap.org/kp/2023/seizing-moment-targeting-transformative-disaster-risk-resilience.

[9] UNDRR, *The Midterm Review of the Implementation of the Sendai Framework for Disaster Risk Reduction 2015–2030: Regional Report for Asia-Pacific* (Geneva, 2023). Available at https://www.undrr.org/publication/regional-report-midterm-review-implementation-sendai-framework-disaster-risk-reduction.

[10] World Bank, *Climate Change and Disaster Management*, Pacific Possible Background Paper No. 6 (Washington, DC, 2016). Available at https://hdl.handle.net/10986/28137.

[11] World Economic Forum, *The Global Risk Report 2024*, 19th Edition (Geneva, 2024). Available at https://www.weforum.org/publications/global-risks-report-2024/.

[12] Kim Arin, "South Korea's digital reputation dented by government network outage", The Korea Herald, 19 November 2023. Available at https://www.koreaherald.com/view.php?ud=20231119000136.

[13] Eileen Yu, "DDoS attack revealed as cause of online service outage at public healthcare institutions", ZD Net, 5 November 2023. Available at https://www.zdnet.com/article/ddos-attack-revealed-as-cause-of-online-service-outage-at-public-healthcare-institutions/.

[14] World Economic Forum, *The Global Risk Report 2024*, 19th Edition (Geneva, 2024). Available at https://www.weforum.org/publications/global-risks-report-2024/.

power distribution, and transportation systems use ICT for traffic management, navigation, and safety. Water management systems also depend on sensors and monitoring tools to manage resources and ensure safety. Financial markets and trading platforms are another critical area, with high-frequency trading, stock exchanges, and payment systems all running on complex ICT infrastructure. These markets rely on near-instantaneous data processing, secure transactions, and continuous uptime to maintain liquidity and stability. As a result, disruptions to ICT infrastructure whether from cyberattacks, natural disasters, or technical failures can have far-reaching consequences, potentially affecting national security, public health, economic stability, and daily life. Ensuring the resilience and security of these critical ICT systems is now a priority for governments, industries, and financial institutions alike. These sectors have been using the ICT infrastructure to monitor and optimize system performance and improve and expand service delivery. As these networks become more interconnected, ICT infrastructure resilience is critical to the uninterrupted operation of essential services. A clear example is teleconsultation with doctors during COVID-19 lockdowns, which would not have been possible in areas with no or poor ICT connectivity. In fact, the national ICT infrastructure itself is categorized as critical infrastructure by many countries.

ICT infrastructure is vital for delivering early warnings and supporting emergency response efforts. It also plays a key role in managing disaster risks and public health threats, including environmental monitoring, analysis, and disease surveillance. To ensure its effectiveness, ICT infrastructure must be constructed or upgraded to withstand a wide range of threats. Without resilient systems, repeated cycles of response and recovery will hinder socioeconomic progress and redirect resources away from achieving the Sustainable Development Goals (SDGs). Building robust ICT infrastructure is essential for enabling emergency response, maintaining the continuity of effective policies and programs aimed at achieving SDG targets, and safeguarding both people and development gains.

1.3.1 About the Connect2Recover Project

This study is a part of the Connect2Recover project implemented by ITU in partnership with the Australian Government,[15] and is aligned with the Connect2Recover methodology for identifying connectivity gaps and strengthening resilience in the new normal.[16] The Connect2Recover project aims to support countries in reviewing the gaps in ICT connectivity and services, and ICT policies and regulations, and create an enabling environment for accelerating the resilience and affordability of ICT infrastructure and services. This project and the study are directly aligned with ITU's Regional Initiative ASP5 on the development of a secure and resilient ICT environment, and contribute to the outcomes of other regional initiatives for Asia and the Pacific, especially ASP3 on fostering the development of infrastructure to enhance digital connectivity and connecting the unconnected.[17]

2. Framework for Assessing the Resilience of National ICT Infrastructure

The framework was developed to assess the resilience of a country's ICT infrastructure and services. It comprises four pillars: (i) network resilience; (ii) affordability of ICT; (iii) emergency preparedness; and (iv) early warning dissemination and communication, that cover the critical components necessary for ensuring a country's capacity to maintain and restore ICT functions during and after disruptions,

[15] ITU, "Connect2Recover - Digital Infrastructure and Ecosystem Reinforcement Against COVID-19 in Asia-Pacific". Available at https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Pages/v2/RD%27s%20Corner/Project%20Pages/Connect2Recover---Digital-Infrastructure-and-Ecosystem-Reinforcement-Against-COVID-19-in-Asia-Pacific.aspx (accessed on 28 July 2024).

[16] ITU, *Connect2Recover: A Methodology for Identifying Connectivity Gaps and Strengthening Resilience in the New Normal* (Geneva, 2021).

[17] ITU, "Asia and the Pacific Regional Initiatives (2023–2025)". Available at https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Pages/v2/2023/ITU-Asia-and-the-Pacific-Regional-Initiatives-(2023–2025).aspx (accessed on 28 July 2024).

contributing to a comprehensive and holistic approach to national resilience building. The framework is unique in that it is aligned with ITU's Asia and the Pacific Regional Initiatives 2023–2025, outlined in the Kigali Action Plan, and is based on the work and recommendations of the ITU Radiocommunication Sector and Standardization Sector.

The next subsection examines other methodologies for assessing ICT infrastructure resilience that were also considered in preparing the framework under this project. This is followed by an overview of the critical components in the four pillars of the framework used for assessments.

In August 2023, the draft framework was validated through an online consultation session with ICT regulators of ITU member countries from Asia and the Pacific region. Feedback from the session was incorporated to finalize the framework, which aims to identify critical gaps and prioritize investments to enhance the resilience of the national ICT infrastructure. This effort supports accelerated economic and social recovery, growth, and progress toward achieving the Sustainable Development Goals (SDGs).

This framework was used to assess ICT infrastructure in Bhutan, Lao PDR, Nepal, and the Philippines, with key findings summarized in Section 3. Section 4 builds on this analysis, offering case studies, good practices, and recommendations to address identified gaps, supporting ITU Member States in strengthening ICT infrastructure resilience.

Assessment of the early warning dissemination and communication pillar is based on the responses rated on a scale of 0–6 following a combination of desk research and interviews with key informants. The questions are related to: (i) governance of the early warning system; (ii) the early warning dissemination and communication infrastructure; (iii) the extent to which the early warning system is inclusive and people-centered; and (iv) the quality and trust of the early warning system.

2.1 Other methodologies for assessing ICT Infrastructure Resilience and how the framework used for assessments under the project adds value

There are at least two frameworks that aim to assess ICT resilience. The first is the Internet Society's framework that assesses the resilience of the Internet infrastructure.[18] The framework is made up of four pillars:

i. Infrastructure – The existence and availability of physical infrastructure that provides Internet connectivity
ii. Performance – The ability of the network to provide end users with seamless and reliable access to Internet services
iii. Security – The ability of the network to resist intentional and unintentional threats through the adoption of security technologies and best practices
iv. Market readiness – The ability of the market to self-regulate and provide affordable prices to end users by maintaining a diverse and competitive market

Another framework is the ESCAP e-Resilience Framework.[19] The framework is made up of five pillars:

i. ICT infrastructure resilience
ii. ICT policy in different sectors that create an enabling environment for e-resilience

[18] Internet Society Pulse, "Internet Resilience". Available at https://pulse.internetsociety.org/resilience (accessed on 28 July 2024).
[19] ESCAP, "e-Resilience Monitoring Dashboard". Available at https://www.unescap.org/projects/e-resilience (accessed on 28 July 2024).

iii. ICT capacity in the development of new systems and applications
iv. ICT supporting digital data management
v. ICT systems at risk of exposure to hazards

The ESCAP framework looks more broadly at different aspects of resilience building (such as adult literacy, digital skills, and research and development expenditure), while the framework prepared for this project provides a detailed look into resilience gaps in the national ICT infrastructure, and does not look at organizational and individual resilience. However, it is important to recognize that gaps in digital skills and effective and safe use of ICT are fundamental pillars in ensuring resilience,[20] and must be addressed as part of a holistic approach to resilience building.

It is important to note that there are sometimes tradeoffs that need to be weighed between the different pillars, such as the potential of infrastructure sharing to improve affordability, but may reduce ICT network resilience, as fewer independent networks increase the burden on the remaining networks and the effect of any outages will be more widespread.[21]

The framework developed under the project with DITRDCA draws on the lessons and good practices from the ESCAP and Internet Society frameworks, with a focus on building the resilience of the national ICT infrastructure, considering both wired and wireless networks and infrastructure at the national level. Both ESCAP and the Internet Society developed a composite index, allowing countries to benchmark progress on a dashboard. The framework is unique in that it is linked to ITU's strategies and priorities and supports the ITU and its Member States in accelerating progress towards building resilient national ICT infrastructure.

While the framework developed under the project with DITRDCA focuses on the ICT infrastructure, it is important to view the framework in the wider context of infrastructure resilience and the interconnectedness of the ICT infrastructure resilience with the resilience of other national infrastructure systems, including energy, transport, water, waste, and wastewater. The United Nations Principles for Resilient Infrastructure provides a useful guide and introduces a commitment to "net resilience gain" in which interventions must enhance the systemic resilience of infrastructure and not negatively impact the wider context.[22]

2.2 Four Pillars of the Framework used for country assessments

2.2.1 Network Resilience

Network resilience strategies that include ensuring redundancy and diversity of network routes contribute to national ICT infrastructure resilience by enabling the rerouting of traffic, faster restoration of network services, and reduction in downtime when there are disruptions in a part of the ICT infrastructure. These disruptions can be caused due to technical failures, natural disasters, or other unexpected events. More diverse connectivity choices for users also contribute to overall resilience, enabling communication and continuity of services, as many organizations, from businesses to emergency services, rely on the ICT network to operate. A resilient network allows organizations to

[20] Refer to the ITU Strategic Plan 2024–2027 at https://www.itu.int/en/council/planning/Pages/default.aspx.
[21] ITU, "Digital Regulation Platform: The Infrastructure Sharing Imperative", 25 August 2022. Available at https://digitalregulation.org/the-infrastructure-sharing-imperative/.
[22] UNDRR, “Principles for Resilient Infrastructure”, no date.

handle increased traffic, changes in demand, and other operational challenges without significant disruptions.

The network resilience pillar looks at the types of connectivity available in the first, middle, and last mile of the network, and their usage rates. In the first mile, submarine cable build-outs will bolster and diversify international connectivity for Asia and the Pacific, adding to their resilience. In the middle mile, there are data centres, IXPs, cloud platforms, and content delivery networks that need to be resilient.

Data centres are being developed to store data and host powerful servers and computing resources that process data in real time, as well as other ICT systems and applications. Standards already exist for the resilience of data centres, which define the data centre's ability to withstand and recover from outages. Data centres can be certified as Tier 1, 2, 3, or 4, with Tier 4 being of the highest availability and most resilient.

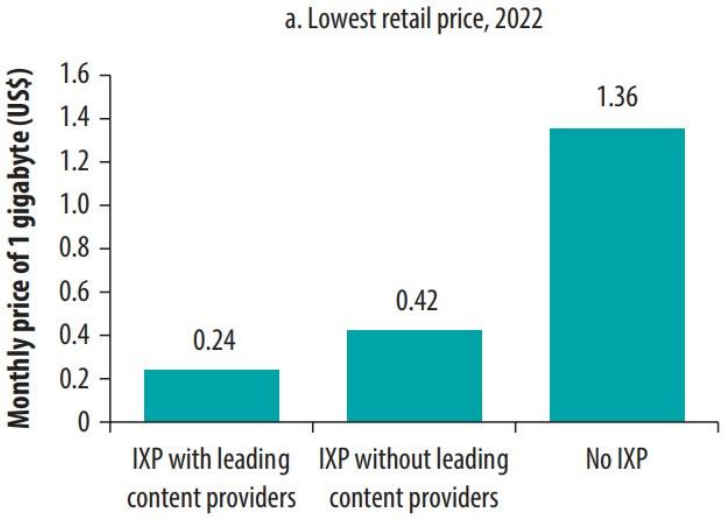
An IXP is a physical and usually neutral location where different networks meet to exchange local traffic via a switch. IXPs ensure local Internet traffic is kept within local network infrastructures, reducing Internet transit costs. Data centres are often located near major IXPs. Content and cloud providers are connecting to IXPs or sharing space in colocation data centres to provide content to users more quickly. Data centres provide storage and processing power, while IXPs optimize the flow of data between networks. IXPs also enhance the resilience of the Internet by providing multiple interconnection points. If one IXP experiences issues, traffic can be rerouted through other exchanges, minimizing disruptions. Therefore, having more IXPs offers better resilience, stability, efficiency, improved latency, increased security, less dependency on international links, and quality improvements.[23]

For example, despite the outage of the SEA-ME-WE-5 submarine cable in April 2024 that normally provides Bangladesh with 1.7 Tbps of international capacity (roughly a third of the country's total international bandwidth usage), Internet traffic at Bangladesh Internet Exchange only dropped marginally. Around 69 per cent of Bangladesh's top 1,000 websites are hosted and served locally. Akamai, Cloudflare, and Facebook provide most of their content locally, which means that their services were less affected by the cable outage.[24] This example shows that hosting content as close to a user lowers the time it takes for them to access that content and can also help alleviate the impact of international connection outages.

Another advantage of IXPs is the reduction in cost for exchanging data internationally. The price of data exchange for countries without IXPs is generally five times higher than for countries with IXPs residing in data centres that host content from leading content and cloud providers (Figure 2). This higher cost is often passed on to consumers, affecting the second pillar of affordability.

[23] Internet Society, "Internet Exchange Points (IXPs)". Available at https://www.internetsociety.org/issues/ixps/ (accessed on 28 July 2024).

[24] Robbie Mitchell, "Bangladesh Coping with Submarine Cable Outage Thanks to Indian Terrestrial Cables, Local Content Caches", Internet Society Pulse, 25 April 2024. Available at https://pulse.internetsociety.org/blog/bangladesh-coping-with-submarine-cable-outage-thanks-to-indian-terrestrial-cables-local-content-caches.



Source: PeeringDB (https://www.cable.co.uk/mobiles/worldwide-data-pricing).
Note: IXP = internet exchange point.

Figure 2: Retail price of Internet data, 2021–2022

The lack of last-mile connectivity, particularly in rural and remote parts of countries, has resulted in 34 per cent of the Asia and the Pacific region being unconnected.[25] However, promising innovations in fixed wireless access and satellite broadband to provide connectivity to areas where laying physical cables is impractical and cost-prohibitive, and enabling government policies to promote and incentivize ICT infrastructure development and expand broadband access in non-commercially viable areas, are helping to bridge the digital divide. For example, Fiji awarded telecommunication and spectrum licenses to Starlink, the satellite operator, in 2023, which is expected to boost competition, expand connectivity, and make ICT more affordable.[26] A detailed look at the potential of satellite technology for ICT infrastructure resilience is provided in Section 4.1.1.

Fixed wireless access is a type of wireless technology that enables fixed broadband access using radio frequencies instead of cables. Fixed wireless access is a viable broadband connection option, especially in areas where fibre infrastructure is unavailable. The incorporation of fixed wireless access with 5G technology has fueled the deployment of this technology throughout Asia and the Pacific as it takes advantage of the high bandwidth and low-latency capabilities of 5G networks.[27] According to a global study, about 65 per cent of service providers are offering fixed wireless access services, with growth expected to more than triple by 2029.[28] A survey, however, suggests that operators may be more interested in using 5G fixed wireless access to augment their 5G offerings than to improve broadband connectivity in unserved and underserved areas.[29] A combination of regulations, incentives, and public

[25] ITU, *Measuring Digital Development: Facts and Figures 2023* (Geneva, 2023). Available at https://www.itu.int/itu-d/reports/statistics/facts-figures-2023/.
[26] John Tanner, "Fiji consumer watchdog welcomes news of Starlink licences", 21 November 2023. Available at https://developingtelecoms.com/telecom-technology/satellite-communications-networks/15825-fiji-consumer-watchdog-welcomes-news-of-starlink-licences.html.
[27] Telecom Review Asia Pacific, "Fixed Wireless Access Transforming Digital Connectivity in Asia", 2 February 2024. Available at https://www.telecomreviewasia.com/news/featured-articles/3939-fixed-wireless-access-transforming-digital-connectivity-in-asia.
[28] Ericsson, "Fixed Wireless Access Outlook", 2024. Available at https://www.ericsson.com/en/reports-and-papers/mobility-report/dataforecasts/fwa-outlook.
[29] S&P Global, "Global 5G survey: Fixed wireless access, connected home lead consumer use cases", 26 October 2022. Available at https://www.spglobal.com/marketintelligence/en/news-insights/research/global-5g-survey-fixed-wireless-access-connected-home-lead-consumer-use-cases.

financing continues to be needed to ensure universal connectivity. Another challenge is ensuring spectrum availability for fixed wireless access.

The network resilience pillar also assesses DNS Security Extensions (DNSSEC) validation, which helps to protect the DNS. The DNS is an essential infrastructure that enables the mapping of names and services on the Internet and underpins its very functioning. Almost every activity on the Internet starts with a DNS query, i.e., a request for information sent by a user's machine to a DNS server. As a result, the impact of incidents affecting the DNS can be significant. They include incidents caused intentionally by malicious actors (e.g., cyberattacks), as well as unintentional incidents (e.g., a misconfiguration making a DNS server unavailable). As the DNS is critical to the operation of the Internet, the threats and risks to the DNS need to be mitigated.

Generally, the distributed nature of the DNS across multiple servers contributes to the resilience of the ICT infrastructure, ensuring that online services remain available even if one or more DNS servers are compromised or fail. DNSSEC is a security protocol that adds an extra layer of security to the DNS, making the Internet more resilient against various types of attacks like DNS cache poisoning. The DNSSEC prevents malicious actors from intercepting and modifying data when it is transmitted, ensuring that users are directed to legitimate websites. There are two sides to DNSSEC – signing and validating. On the one hand, DNS operators sign domain names cryptographically. On the other side, when you do anything online that uses domain names, the DNS resolver you use, often at your Internet service provider, performs DNSSEC validation to check whether DNSSEC signatures are correct. For DNSSEC to provide its extra layer of security globally, both are needed: domain names to be signed, and local DNS resolvers to check for DNSSEC signatures.[30] The Asia and the Pacific Network Information Centre regularly publishes data on the rate of DNSSEC validation per country, which is a way to assess DNS resilience.

Related to enabling communication during disasters and emergencies, the allocation of spectrum for use by amateur (ham) radio, the Global Maritime Distress and Safety System (GMDSS),[31] and public protection and disaster relief (PPDR) agencies, as recommended in ITU-R M.2015, frequency arrangements for public protection and disaster relief radiocommunication systems are assessed.[32] For the GMDSS that informs vessels of navigation hazards and weather conditions, and enables distress calls, and for PPDR agencies, it is important to have a dedicated and harmonized spectrum for cross-border mobility and wide geographical coverage during crises and emergencies.

2.2.2 Affordability of ICT

Improvement in the affordability of ICT plays an important role in resilience building as it enhances access to information and enables communication. Nations can better prepare for emergencies and natural disasters with affordable devices and services. During emergencies, timely and accurate information is vital for effective response and recovery. Affordable ICT ensures the inclusion of vulnerable and marginalized populations in accessing essential information and services, including early warnings and emergency services. During normal times, affordable ICT allows small businesses and entrepreneurs access to digital tools and platforms that can help them adapt and thrive. Affordable

[30] Dan York, "DNSSEC Validation in 2022: Africa Leads with Amazing Growth", Internet Society Pulse, 16 March 2023. Available at https://pulse.internetsociety.org/blog/dnssec-validation-in-2022-africa-leads-with-amazing-growth.
[31] ITU, Resolution 359 (REV.WRC-15): Consideration of regulatory provisions for updating and modernization of the Global Maritime Distress and Safety System. Available at https://www.itu.int/dms_pub/itu-r/oth/0c/0a/R0C0A00000C0008PDFE.pdf.
[32] ITU, Resolution 646 (REV.WRC-19): Public Protection and Disaster Relief. Available at https://www.itu.int/dms_pub/itu-r/oth/0C/0A/R0C0A00000F00133PDFE.pdf.

ICT also broadens access to educational resources and online learning platforms, and health information and services. During crises, such as pandemics, telehealth can be a crucial component of a resilient healthcare system. Moreover, affordable ICT tools help build and strengthen communities by facilitating collaboration and networking. Strong, connected communities are better equipped to support each other during times of need and work together to quickly recover from crises, enhancing their resilience.

This pillar assesses mobile data and fixed-broadband prices, relative to end-users' income. The prices are based on ICT Price Baskets defined by the ITU's Expert Group on Telecommunication Indicators, to allow internationally comparable pricing.[33] This pillar also assesses the cost of smartphones and feature phones, relative to end-users' income, as well as other factors that affect ICT affordability. They include market concentration, availability of spectrum, infrastructure, and spectrum sharing arrangements, and policies and regulations to deliver ICT services to rural and remote areas (e.g., universal access service obligations). Evidence shows that promoting a competitive market environment and infrastructure sharing are effective ways to drive down ICT prices and improve the quality of ICT services. Promoting competition enables users to benefit from greater choice from operators and spurs innovation.

Regarding infrastructure sharing, the ITU Tariff Policies Survey shows that 15–25 per cent of regulatory authorities believe that infrastructure sharing has resulted in lower end-user prices.[34] There are now various options for infrastructure sharing of passive infrastructure (e.g., towers, poles, ducts, and premises) and active assets (e.g., switches, radio access network [RAN], and spectrum). The sharing of infrastructure helps avoid duplication and can encourage co-deployment to improve coverage in rural and remote areas, as well as improve affordability. However, infrastructure sharing could potentially reduce incentives to invest in ICT infrastructure development (particularly for passive infrastructure sharing) and reduce network resilience, which regulators need to consider and put in place measures to address. Recommendation ITU-T D.264 proposes a set of possible methods to help network operators save costs and enhance efficiency through passive and active infrastructure sharing. The recommendation indicates that there is a potential saving of up to 30 per cent for passive infrastructure sharing and up to 50-60 per cent for active infrastructure sharing.[35]

2.2.3 Emergency Preparedness

Effective emergency preparedness includes safeguarding the ICT systems and infrastructure. This involves implementing measures like regular backups, disaster recovery plans, and redundant systems to ensure that data and services remain available even during a crisis. By preparing for emergencies, organizations can maintain operational continuity and recover more quickly. Emergency preparedness involves identifying potential risks to ICT systems and infrastructure and developing strategies to mitigate them. This can include assessing vulnerabilities in hardware and software and establishing protocols for responding to different types of threats. Regular training and drills help ensure that individuals and organizations are aware of potential threats and know how to respond effectively. Well-trained personnel are crucial for maintaining ICT resilience during emergencies. Having a national emergency telecommunication plan (NETP) is a key aspect of emergency preparedness and resilient

[33] ITU, "ICT Prices". Available at https://www.itu.int/en/ITU-D/Statistics/Pages/ICTprices/default.aspx (accessed on 28 July 2024).
[34] ITU, *Output Report on ITU-D Question 4/1: Economic policies and methods of determining the costs of services related to national telecommunication/ICT networks – Study period 2018–2021* (Geneva, 2021). Available at https://digitalregulation.org/wp-content/uploads/ITU-D-Question-4-1-Final-Report-2021.pdf.
[35] ITU, "Recommendation ITU-T D.264: Shared uses of telecommunication infrastructure as possible methods for enhancing the efficiency of telecommunications", 2020. Available at https://www.itu.int/rec/T-REC-D.264-202004-I.

building. A well-defined NETP helps organizations act quickly and effectively to minimize losses and damages and recover swiftly.

This pillar examines the country governments' level of preparedness to respond to the multiple risks and threats to the national ICT infrastructure. It examines the national policies, regulations, plans, and collaborations to protect the national ICT infrastructure, anticipate and detect threats, and recover quickly. The pillar assesses policies, strategies, and structures related to cybersecurity, personal data protection and privacy, data sovereignty, adoption of security-by-design approaches in the development of new ICT services, digitalization and interoperability of government services and systems, and business continuity and disaster recovery.

The pillar also analyses the country's NETP. The NETP is an overall strategic document that includes not only the regulatory framework for disaster risk management but also all activities and actions that need to be developed and implemented in each of the phases of the disaster management cycle beyond the ICT sector. The NETP enables establishing standard operating procedures, defining roles and responsibilities of different players, promoting coordination, and allowing for swift and efficient emergency response. According to ITU guidelines, a NETP should cover four phases of a disaster: mitigation, preparedness, response, and recovery. The NETP should be multi-hazard, multi-technology, and multi-stakeholder.[36]

The pillar also assesses the regulation of the quality of ICT service offered by ICT service providers to users, during normal times, as well as during a disaster or crisis. Typical quality-of-service metrics include time to provision services, network availability, latency, mean time to repair, and coverage. The quality of service achieved can either be reported by the operators and/or assessed by the regulator against the service levels offered to users. The pillar examines service providers' level of preparedness, e.g., whether service providers have contingency plans to maintain the desired quality of service following a disaster or crisis.

In addition, the pillar assesses the implementation of technical features that can enhance ICT infrastructure resilience. They include best practices for the management of DNS servers, such as placing DNS servers at topologically and geographically diverse locations to minimize the likelihood of a single point of failure, and disabling the entire system.[37] They also include the network operators' implementation of adaptive restoration and adaptive reallocation, as well as predictive analytics, to identify potential network congestion, hardware failure, and other issues.[38] Adaptive restoration offers various recovery routes by selecting optical signal parameters adaptive to their transmission quality, and adaptive reallocation reconfigures optical network resources according to the available optical wavelength slots in surviving optical cables.[39] Operators that have implemented adaptive restoration and adaptive reallocation are better prepared for network resilience. However, information on their implementation by network operators is not readily available.

Furthermore, the pillar assesses power infrastructure resilience, as a reliable and robust power supply is necessary to ensure network resilience and the continued function of the ICT infrastructure. The

[36] ITU, *ITU Guidelines for National Emergency Telecommunication Plans* (Geneva, 2020).
[37] IETF, "Selection and Operation of Secondary DNS Servers: RFC 2182 also known as BCP 16", July 1997. Available at https://datatracker.ietf.org/doc/rfc2182/.
[38] ITU, "ITU-T Y.1271: Framework(s) on network requirements and capabilities to support emergency telecommunications over evolving circuit-switched and packet-switched networks", 2014. Available at https://www.itu.int/rec/T-REC-Y.1271-201407-I/en.
[39] ITU, "ITU-T Series L Supplement 35: Framework of disaster management for network resilience and recovery", 2017. Available at https://www.itu.int/rec/T-REC-L.Sup35-201706-I/en.

availability of power, reliability of power, backup power supply, diverse sources of power, and growth in power generation are the factors considered in this pillar.

2.2.4 Early Warning Dissemination and Communication

Early warnings for all contribute to resilience by providing advance notice of potential threats, enabling individuals, organizations, and communities to take preemptive actions. For instance, an early warning of a natural disaster allows people to evacuate, businesses to secure assets and governments to mobilize resources, reducing potential damage and loss. Early warnings help in coordinating actions among various stakeholders, including government agencies, businesses and community organizations. This collective approach enhances overall resilience by ensuring that everyone is aligned and working together to prepare for, respond to and recover from emergencies.

As part of the United Nations Secretary-General's Acceleration Agenda, the Early Warnings for All (EW4All) initiative was established in 2022 to ensure that early warning systems protect everyone by 2027. The EW4All initiative is built on four pillars to deliver effective and inclusive multi-hazard early warning systems: (i) disaster risk knowledge and management; (ii) detection, observation, monitoring, analysis, and forecasting; (iii) warning dissemination and communication; and (iv) preparedness and response capabilities (Figure 3). The third pillar on warning dissemination and communication is being led by the ITU.[40]

Figure 3: Four Pillars of Multi-hazard Early Warning Systems

Source: ITU, "Early Warnings for All Initiative". Available at https://www.itu.int/en/ITU-D/Emergency-Telecommunications/Pages/Early-Warnings-for-All-Initiative.aspx (accessed on 28 July 2024).

The share of people exposed to multi-hazard risk is forecast to increase to 85 per cent of the region's population under 1.5°C warming.[41] Multi-hazard early warning systems are one of the most effective

[40] United Nations, "Early Warnings for All". Available at https://www.un.org/en/climatechange/early-warnings-for-all (accessed on 28 July 2024).

[41] ESCAP, *Seizing the Moment: Targeting Transformative Disaster Risk Resilience – Asia-Pacific Disaster Report 2023* (Bangkok, 2023). Available at https://www.unescap.org/kp/2023/seizing-moment-targeting-transformative-disaster-risk-resilience.

ways to reduce mortality from natural hazards and protect people, and could reduce disaster losses by up to 60 per cent, according to an ESCAP report.[42] However, only 26 Asia and the Pacific countries have reported the existence of multi-hazard early warning systems in their respective countries.[43] The United Nations Office for Disaster Risk Reduction (UNDRR) estimates that countries with limited to moderate multi-hazard early warning system coverage have nearly six times the mortality rate of countries with substantial to comprehensive coverage.[44]

Ensuring effective warning dissemination and communication systems must address multiple barriers. For instance, the channels that are used for communication may not be effective in reaching vulnerable groups in a timely manner, the format and language of the early warning message may not be useful and actionable, and/or the receivers of the early warning message may not be able to understand it. These barriers impede disaster risk management efforts since, without access to information, individuals cannot adequately anticipate and prepare for disasters.

It is widely recognized that multiple channels of warning distribution are necessary for redundancy, inclusivity, and the widest possible reach, but these channels must promote a consistent message to maintain trust and clarity. Building redundancy and robustness, not just of communication channels (e.g., social media, community-alert messages), but also of telecommunication and power infrastructure, makes emergency communication, including warning messages, more effective.[45]

In the countries assessed, there is information available on the governance and infrastructure of their early warning systems, but very limited information available in the public domain on inclusion, and quality, and trust. The information collected on governance and infrastructure is related to:

- The national authority and stakeholders responsible for early warning dissemination and communication.
- Legislation, mandates, and standard operating procedures related to the use of ICT for early warning systems.
- Current status on the implementation of Common Alerting Protocol (CAP)
- Establishment of the National Emergency Telecommunication Plan (NETP)
- Identification, testing, maintenance, and upgrading of the infrastructure and systems associated with early warning dissemination and communication.
- Use of mobile-based early warning communication channels, including cell broadcast technology.

Common Alerting Protocol

CAP is an international standard format for all-hazard emergency alerting and public warning across all channels developed by ITU (ITU-T Recommendation X.1303). As ICT network services and users are growing, they offer more opportunities to deliver alert messages to populations at risk. People may be reached through landline phones, mobile networks, and the Internet via email, social media, instant messaging and mobile apps, online advertising, in-home smart speakers, in-vehicle navigation systems, as well as more traditional forms of dissemination such as sirens, loudspeakers, broadcast radio and

[42] Ibid.

[43] UNDRR, *The Midterm Review of the Implementation of the Sendai Framework for Disaster Risk Reduction 2015–2030: Regional Report for Asia-Pacific* (Geneva, 2023). Available at https://www.undrr.org/publication/regional-report-midterm-review-implementation-sendai-framework-disaster-risk-reduction.

[44] UNDRR, *Global Status of Multi-Hazard Early Warning Systems 2023* (Geneva, 2023). Available at https://www.undrr.org/media/91954/download?startDownload=20240605.

[45] World Bank, *Designing Inclusive, Accessible Early Warning Systems: Good Practices and Entry Points* (Washington, DC, 2023). Available at https://www.preventionweb.net/publication/designing-inclusive-accessible-early-warning-systems-good-practices-and-entry-points.

television, cable television, emergency radio, amateur radio, satellite broadcast, and digital signage networks such as highway signs, billboards, automobile and rail traffic control systems, among others.

Sending the same alerting message over multiple communication channels increases coverage and impact and enhances trust in the alert. Using a standardized alerting format such as CAP can reduce costs and complexity by eliminating the need for multiple custom software interfaces and enabling the integration of actionable guidance directly into an alert. It ensures consistency in information transmitted over numerous communication channels and normalizes warnings from various sources. The format is compatible with existing and emerging communication formats and techniques, allowing for a single input to activate all types of alerting and public warning systems, including cell broadcasting and location-based SMS, to quickly reach people in at-risk areas.

The implementation of CAP has helped the timely flow of consistent information from alerting authorities to the public across multiple communication channels, thus increasing warning effectiveness and trust, while simplifying the warning task.

Figure 4: CAP's Role in Enabling Effective Early Warning Dissemination and Communication

Source: ITU, "Common Alerting Protocol and Call to Action". Available at https://www.itu.int/en/ITU-D/Emergency-Telecommunications/Pages/Common-Alerting-Protocol-and-Call-to-Action.aspx (accessed on 28 July 2024).

Cell Broadcasting and Location-based SMS

The action plan for the EW4All initiative calls for the promotion and implementation of geo-located mobile-based early warning services using cell broadcast and/or location-based SMS as a critical element for early warning dissemination and communication. These are proven technologies already used in several countries that are taking advantage of mobile networks and technologies to send warning messages. They can be targeted to reach only people located in an at-risk area, and their alerts are adaptable to specific requirements, such as a user's language.[46]

Cell broadcasting and location-based SMS technologies both have advantages and disadvantages and can complement each other in early warning dissemination and communication (Table 1). Cell broadcasts can send near-real-time warning messages to many mobile subscribers located in a specific area, without the risk of network congestion and without needing to know the phone numbers of the

[46] Ibid.

mobile devices. The message, instantly recognizable as an alert with a special standardized ringtone and vibration, will be displayed automatically on the screen of the end users' mobile devices if their devices are configured to support and receive alerts. In contrast, all mobile devices with a SIM can support location-based SMS. However, location-based SMS may be subject to network congestion, causing delays in disseminating warning messages.[47] Depending on the capability of users' mobile devices, text-to-speech conversion may be possible for persons with visual disabilities or for those who are illiterate.[48]

Table 1: The strengths and weaknesses of cell broadcasting

Strengths	Weaknesses
• Wide reach since it does not usually require users to opt in, download or subscribe to a service (but requires mobile network coverage and access to a compatible mobile device). • Message can be disseminated to millions of compatible mobile devices in a few seconds (near-real-time). • Does not cause network congestion. • Enables geographically-targeted dissemination of early warning messages. Enhanced targeting can reduce panic and alert fatigue, both of which can threaten the efficacy of and trust in public warnings. • Can be configured to sound an audible and unique alert tone, overriding silencing and mute settings. • Can appear automatically on the screen of a mobile device without needing to be opened, providing a visual alert. • Is privacy-enhancing. Since the message is broadcast to the user equipment and does not use the mobile number, no pre-registration is required. No mobile subscriber information is used or stored.	• Allows one-way communication only. Users cannot reply to a cell broadcast message. • Only disseminates text-based messages, although text-to-speech conversion is possible. • Does not provide a read receipt. • It is not possible to send a follow-up cell broadcast message to devices that received the first message. • Some mobile devices, particularly older devices, may not be compatible with cell broadcasting systems. • Users can choose to opt out of receiving cell broadcast messages that are not of "presidential alert" level severity. • Requires investment and installation of specific equipment before a cell broadcast service can be provided to end users. • Lack of incentive for mobile network operators to provide cell broadcast service. • Is reliant on the mobile network infrastructure, which can be vulnerable to disasters or service interruptions. • People living in areas with no mobile network coverage will not be reached.

Source: Adapted from GSMA, *Cell Broadcast for Early Warning Systems: A review of the technology and how to implement it* (London, 2023). Available at https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/wp-content/uploads/2023/11/Cell-Broadcast_R.pdf.

Key challenges for deploying cell broadcasting and location-based SMS systems include financing, coordinating stakeholders to implement the systems, and ensuring the public is aware of and trusts the systems. As commercial interest for mobile network operators to implement early warning systems

[47] For a detailed comparison of cell broadcasting and location-based SMS technologies, see: ITU, *Digital Transformation and Early Warning Systems for Saving Lives: Background Paper* (Geneva, 2023). Available at https://www.itu.int/hub/publication/d-gen-digital-transfor-01-2023/.

[48] UNDRR, *Words into Action: Engaging for Resilience in Support of the Sendai Framework for Disaster Risk Reduction 2015–2030* (Geneva, 2023). Available at https://www.undrr.org/words-into-action/guide-multi-hazard-early-warning.

is limited, clear regulatory frameworks, appropriate incentives, and public advocacy and awareness campaigns can accelerate the rollout of cell broadcasting and other mobile-based warning dissemination and communication systems. For example, a European Union Directive requires all European Union countries to implement an early warning system using mobile network communication channels by June 2022.

The European Emergency Number Association recommends deploying both cell broadcasting and location-based SMS systems for countries that have the necessary financial resources and expertise.[49] However, for countries with more limited budgets and expertise, or if funds are available for only one technology, countries can assess the risk of network congestion. The higher the risk, the more cell broadcasting should be prioritized.[50] In addition, it is recommended to combine cell broadcasting and location-based SMS with other technologies and communication channels, including sirens, billboards, radio, television, mobile alerting apps, and social media. Using CAP to ensure consistent messaging across the different channels will avoid confusion and reinforce the messages.

[49] Benoit Vivier, "8 recommendations to get the most out of Public Warning Systems", European Emergency Number Association, 21 June 2022. Available at https://eena.org/blog/8-recommendations-to-get-the-most-out-of-public-warning-systems/.

[50] ITU, *Digital Transformation and Early Warning Systems for Saving Lives: Background Paper* (Geneva, 2023). Available at https://www.itu.int/hub/publication/d-gen-digital-transfor-01-2023/.

3. Gap Analysis of Four Countries

The study selected four countries to conduct a gap analysis, based on requests and data availability, to support the development of policies and infrastructure to improve national ICT infrastructure resilience. The four countries include Bhutan, Lao PDR, Nepal and the Philippines.

Bhutan, Lao PDR, and Nepal are landlocked developing countries (LLDCs). Additionally, Lao PDR and Nepal are classified as least developed countries (LDCs). For landlocked countries, not having direct access to submarine cables means they must rely on terrestrial cables, which often traverse long distances across multiple borders. This increases the potential for higher latency and additional costs associated with securing transit agreements. Other LLDCs in the region that are likely to be facing similar challenges include Afghanistan and Mongolia.

The Philippines, the fourth country selected for the gap analysis, being an archipelago of over 7,000 islands, with about 2,000 islands inhabited, shares some common geographical features and challenges with Indonesia and small island developing States (SIDS).[51] Kiribati, Solomon Islands, Timor-Leste and Tuvalu are SIDS and LDCs.

A summary of the gap analysis by the four pillars is presented below. Generally, in the four selected countries, data is limited and not readily available to fully assess the resilience of the national ICT infrastructure. An important recommendation for the way forward is the collection, analysis and sharing of disaggregated data for measuring and monitoring progress in building the resilience of the national ICT infrastructure.

3.1 Network Resilience

In line with regional trends, mobile broadband coverage in the four countries is high, while access to fixed broadband remains a critical gap. A notable achievement is Nepal's investment in fibre-to-the-home (FTTH) networks across the country, now covering 76 out of the 77 districts. Nepal plans to shut down copper-based Internet access and migrate customers to fibre networks.

Structures, systems and measures that contribute to network resilience are generally limited in the four selected countries (Table 2). Their rate of DNSSEC validation to minimize security risks is average (although higher than the average rate for Asia, which is at 28 per cent) in Lao PDR, Nepal and the Philippines. The exception is Bhutan that has a 97 per cent validation rate, which is one of the highest globally. There needs to be cooperation among government agencies, domain name registrars and Internet service providers to promote DNSSEC deployment and increase the validation rate.

Global trends show that DNSSEC signing and validation rates vary significantly across countries. Generally, the increased vulnerability of DNS has not been matched with increased deployment of DNS security measures.[52] The gaps across countries in both signing and validation rates indicate the importance of initiatives to build capacity and incentivize the use of DNSSEC. In countries like Finland and Sweden, governments have supported DNS security capacity building, and the country code top-level domain registries have provided financial incentives to registrars and registrants for DNSSEC

[51] The Asia-Pacific SIDS include: Fiji, Kiribati, Maldives, Marshall Islands, Micronesia, Nauru, Papua New Guinea, Samoa, Solomon Islands, Timor-Leste, Tonga, Tuvalu, and Vanuatu.

[52] OECD, "Security of the Domain Name System (DNS): An Introduction for Policy Makers", OECD Digital Economy Paper No. 331, October 2022. Available at https://www.oecd-ilibrary.org/docserver/285d7875-en.pdf?expires=1717732205&id=id&accname=guest&checksum=2F840B15349C99DCF5899AA21C65A75F.

signing. Typically, the fee paid by the registrar to the registry for each domain would be lower for DNSSEC-signed domains.[53]

The number of IXPs and data centres is low in most countries, and they are often established without any backup facilities. The Philippines, however, has 10 active IXPs that are either operator-neutral or run by network operators. There is a critical need to establish high-quality data centres (Tier 4) to meet growing demand and cater for redundancy, including outside of capital cities. Standards for data centres are becoming more stringent, emphasizing resilience, energy efficiency, integration of renewable energy sources, advanced cooling technologies, and security (both cybersecurity and physical security). Data centre operators are exploring innovative approaches such as waste heat utilization, water recycling and onsite renewable energy generation to reduce their carbon footprint and enhance sustainability.[54] This entails incentivizing renewable energy adoption, establishing industry standards for energy efficiency and environmental stewardship, and fostering knowledge exchange and the sharing of best practices among industry peers.

Table 2: Summary of network resilience in four selected countries

Indicators	Bhutan	Lao PDR	Nepal	Philippines
Access Availability	DSL, FTTH, 3G/4G/5G	DSL, FTTH, 3G/4G/5G	FTTH, 3G/4G, and a small number of satellite terminals for private licensees	FTTH, DSL, fixed wireless, 3G/4G/5G, satellite broadband and VSAT in some rural areas
Fixed Household Penetration	1%	11%	43%	29%
Mobile Data Penetration	99%	84%	96%	112%
DNSSEC Validation (as of March/April 2024)	96.91%	47.30%	32.50%	45.19%
No. of IXPs (Location)	1 (Thimphu)	1 (Vientiane)	1 (Lalitpur and Kathmandu)	10 (Manila and Cebu)
No. of Data Centres (Tier Level)	3 (Tier 2)	Few (not tier certified)	7 (Tier 3)	At least 8
Terrestrial Network	Parts of the network have diverse routes.	Critical nodes have been identified and a ring topology provides network resilience.	Critical nodes are upgraded, and a ring topology provides network resilience.	Two major operators have built domestic fibre and microwave networks in self-healing loops.
International Network	Two international gateways, but both connect to Siliguri, India. A third gateway that connects to Bangladesh is being negotiated.	There are multiple points of connection to Cambodia, China, Myanmar, Thailand and Viet Nam.	Limited international gateways, relying on submarine cables through India.	Connected to 10 international submarine cables.
Spectrum for PPDR?	No	No	No	Yes (380–400 MHz)

[53] Ibid.

[54] Telecom Review Asia Pacific, "Sustainable Practices in Data Center Operations in the Asia Pacific", 23 February 2024. Available at https://www.telecomreviewasia.com/news/featured-articles/4009-sustainable-practices-in-data-center-operations-in-the-asia-pacific.

Notes: DNSSEC = Domain Name System Security Extensions; DSL = Digital Subscriber Line; FTTH = Fibre-to-the-Home; IXP = Internet Exchange Point; PPDR = Public Protection and Disaster Relief; VSAT = Very Small Aperture Terminal.

LLDCs in South Asia such as Bhutan and Nepal face major challenges in diversifying their network routes, particularly at the first mile. Lao PDR, also an LLDC, however, has been able to establish multiple points of connection with Cambodia, China, Myanmar, Thailand and Viet Nam. In the Philippines, the country is connected to multiple international submarine cables and covered by satellite systems, allowing for sufficient international capacity and diversity. Domestically, connectivity in the Philippines is also rather impressive given that it is an island nation with mountainous terrain and is highly disaster prone. Generally, across the four countries, wide gaps persist in broadband coverage between urban and rural areas, in remote areas and in sparsely populated islands. To address the gaps, countries can explore the use of fixed wireless access and satellite technologies for direct access, mobile backhaul in remote areas and backup links. The shutdown of 2G and 3G networks presents a potential opportunity to reallocate spectrum to services such as mobile broadband, fixed wireless access, and satellite communications, this transition warrants careful consideration to ensure that it does not negatively impact existing network coverage or critical network services.

While many countries have allocated spectrum for public protection and disaster relief (PPDR) to enhance emergency response interoperability, only the Philippines has done so among these countries, and only Nepal and the Philippines have regulations in place to use amateur (ham) radio for emergency communication.

3.2 Affordability of ICT

Promoting a competitive market environment and infrastructure sharing are effective ways to drive down ICT prices and improve the quality of ICT services.

The Herfindahl-Hirschman Index (HHI) is a measure of market concentration and is often used by telecommunication regulators to monitor the distribution of market power. The HHI values are between 0 and 10,000, with increasing values suggesting a higher level of market concentration. A market with an HHI of less than 1,500 is considered to be a competitive marketplace, an HHI of 1,500 to 2,500 to be a moderately concentrated marketplace, and an HHI of 2,500 or greater to be a highly concentrated marketplace.[55]

Box 1: Affordability of Broadband: Global and Regional Trends

Globally, prices for all mobile and fixed-broadband services have become cheaper. In Asia and the Pacific, 22 of 36 countries (61 per cent) have entry-level data-only mobile-broadband services (based on a 2GB data plan) at less than 2 per cent of monthly gross national income (GNI) per capita,[56] the target set by the United Nations Broadband Commission for affordable broadband.[57] Prices range from

[55] Gary Kim, "Mobile Market is Highly Concentrated and Always Will Be", Spectrum Futures, 26 October 2019. Available at https://spectrumfutures.org/mobile-market-is-highly-concentrated-and-always-will-be/.
[56] ITU, *Policy Brief: The Affordability of ICT Services 2023* (Geneva, 2024). Available at https://www.itu.int/en/ITU-D/Statistics/Documents/publications/prices2023/ICTPriceBrief2023.pdf.
[57] United Nations Broadband Commission for Sustainable Development, "2025 Broadband Advocacy Target 2: Making Broadband Affordable". Available at https://www.broadbandcommission.org/advocacy-targets/2-affordability/ (accessed on 28 July 2024).

0.16 per cent of GNI per capita in Singapore to over 16 per cent of GNI per capita in Papua New Guinea. Countries not meeting the 2 per cent target are LDCs, LLDCs and/or SIDS.[58]

It is worth noting that people are generally spending more time online and using more intensive applications, which means that a mobile subscription with 2GB of data (for which the pricings are based) is hardly sufficient. In low-income countries, a 10GB mobile data subscription consumes as much as a quarter of monthly income. Fixed-broadband services (based on a 5GB data plan) are generally less affordable, with only 14 of 36 Asia and the Pacific countries (39 per cent) having achieved the 2 per cent target.[59] Figure 5 shows the greatest reduction in cost for high-consumption mobile data and voice, while prices for fixed broadband have been stagnating.

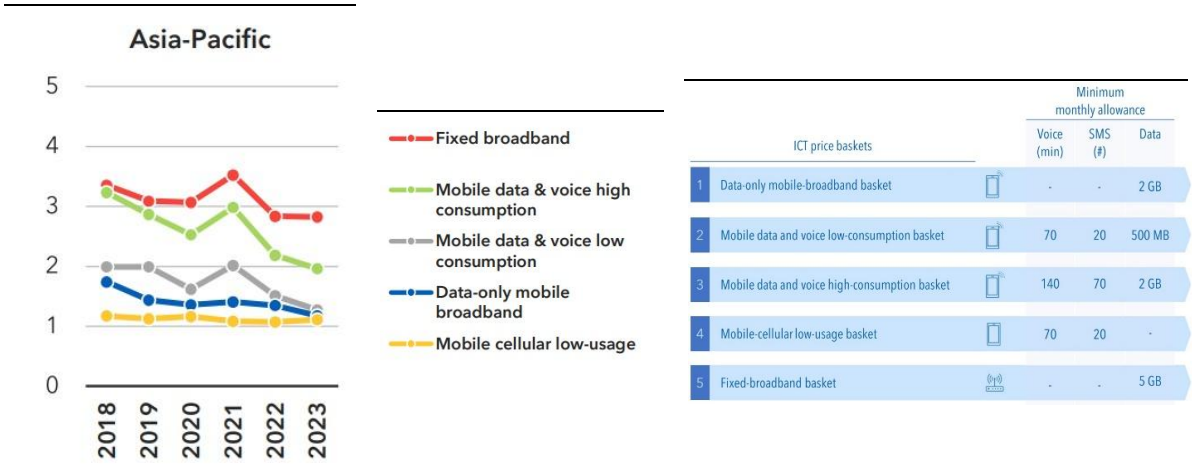


Figure 5: Affordability trend in Asia and the Pacific as a percentage of GNI per capita

Source: ITU, "The affordability of ICT services 2023" Policy Brief, March 2024. Available at https://www.itu.int/en/ITU-D/Statistics/Documents/publications/prices2023/ICTPriceBrief2023.pdf.

Box 2: Affordability of ICT Devices: Global and Regional Trends

Regarding the cost of ICT devices, similar efforts to collect internationally comparative data are not readily available. The Alliance for Affordable Internet collected this data in 2021 and 2022. Their study found that the global average cost of a smartphone is around USD 104 or 26 per cent of an average monthly income. However, in LDCs, the average person would have to spend over half of their monthly income to buy a smartphone.[60] Their study generally found that countries are not doing enough to ensure the affordability of ICT devices, as only 22 of 72 countries surveyed (31 per cent) included a target in their national broadband plans or ICT strategies that relate to the availability and/or affordability of ICT devices.[61]

The Global System for Mobile Communications Association (GSMA) also provides data on the cost of the cheapest Internet-enabled feature phone or smartphone as part of their Mobile Connectivity

[58] They include: Cambodia, Nepal, Tonga, Nauru, Tuvalu, Myanmar, Vanuatu, Marshall Islands, Fiji, Timor-Leste, Kiribati, Samoa, Afghanistan, Micronesia, Solomon Islands, and Papua New Guinea.
[59] ITU, *Policy Brief: The Affordability of ICT Services 2023* (Geneva, 2024). Available at https://www.itu.int/en/ITU-D/Statistics/Documents/publications/prices2023/ICTPriceBrief2023.pdf.
[60] Web Foundation, "How expensive is a smartphone in different countries?" 7 October 2021. Available at https://webfoundation.org/2021/10/how-expensive-is-a-smartphone-in-different-countries/.
[61] Alliance for Affordable Internet, "The cost of smartphones falls, but they remain unaffordable for billions around the world", 31 August 2022. Available at https://a4ai.org/news/the-cost-of-smartphones-falls-but-they-remain-unaffordable-for-billions-around-the-world/.

Index.[62] GSMA reported similar findings in low- and middle-income countries. While the affordability of an entry-level device across all low- and middle-income countries costs about 16 per cent of average monthly income, this increases to 40 per cent for the poorest 40 per cent of the population. ICT devices are also less affordable for women (24 per cent of average monthly income) compared to men (13 per cent of average monthly income).[63] GSMA highlighted that the affordability of an entry-level, Internet-enabled device has remained relatively unchanged. In South Asia, the affordability of mobile devices has, in fact, worsened since the COVID-19 crisis.

Overall, the high costs of ICT devices and data plans continue to be an obstacle for people to access ICT services in the region. Innovative ways of financing smartphones and other ICT devices like computers, laptops and tablets, as well as data plans (e.g., through loans, subsidies and flexible payment options) are needed to close the gap in ICT access.

As shown in Table 3, the mobile and fixed-line markets are generally highly concentrated. However, Bhutan and Nepal's fixed-line markets are exceptions, with Herfindahl-Hirschman Index (HHI) values of 2.467 and 1.421, respectively. All other markets exhibit higher HHI values, indicating less competition and more highly concentrated market dynamics. The affordability of mobile and fixed broadband services varies significantly across the four countries. Bhutan offers the most affordable prices for both service categories, requiring only 1.18% and 2.87% of GNI per capita for a standard price basket of mobile and fixed broadband, respectively. The affordability benchmark set by the Broadband Commission has been met only in Bhutan and the Philippines, with their mobile service markets requiring 1.18% and 1.78% of GNI per capita for a standard price basket of mobile broadband, respectively. This highlights the need for further efforts to improve affordability in Lao PDR and Nepal.. Devices like smartphones, however, are least affordable in Bhutan and are generally expensive across all four countries, ranging from 9 to 17 per cent of average monthly income, based on data received from the selected countries and presented in Table 3. Nevertheless, this is still lower than the global average cost of a smartphone, which is around 26 per cent of average monthly income.

Table 3: Summary of ICT affordability in four selected countries

Indicators	Bhutan	Lao PDR	Nepal	Philippines
Market Concentration: Mobile HHI Fixed HHI	5,288 2,467	3,926 4,975	5,242 1,421	4,463 3,532
Fixed Broadband Basket (GNI per capita)	2.87	7.23	10.29	10.21
Mobile Data and Voice Low Consumption Basket (GNI per capita)	1.18	4.03	2.48	1.78
Smartphone to Monthly Income Ratio	17%	13%	9%	13%
Infrastructure Sharing	Yes, only passive infrastructure	Not available	Yes, only passive infrastructure	Yes, only passive infrastructure

[62] GSMA Mobile Connectivity Index. Available at https://www.mobileconnectivityindex.com/index.html (accessed on 28 July 2024).
[63] GSMA, *The State of Mobile Internet Connectivity Report 2023* (2023). Available at https://www.gsma.com/r/somic/.

Rural Connectivity Policy	National Broadband Master Plan	- Ten-Year National Digital Economy Development Strategies (2021–2030) - Five-Year Technology and Communications Development Plans (2021–2025)	License obligations	National Broadband Plan indicates a rural technology roadmap
Universal Access Fund	Universal Service Fund	Rural Telecommunication Development Fund	Rural Telecommunication Development Fund	Section 17 of the Republic Act No. 10929 creates the Free Public Internet Access Fund to finance the Free Internet Access Program in Public Places
Mobile Spectrum Availability	Spectrum for 5G has been awarded in the 2.6GHz, 3.5GHz and 26GHz bands	538.8MHz assigned	200.9MHz assigned	530.9MHz assigned

Notes: GNI = Gross National Income; HHI = Herfindahl-Hirschman Index.

Two per cent of monthly GNI per capita is the target set by the United Nations Broadband Commission for affordable broadband.

The HHI is a measure of market concentration. The HHI values are between 0 and 10,000 with increasing values suggesting a higher level of market concentration.

In Bhutan, there are six players in the fixed-line market and two mobile network operators, with state-owned Bhutan Telecom having over 60 per cent of the mobile market share. In Lao PDR, there are four mobile network operators – Unitel Laos, Lao Telecom, ETL and TPlus, with Lao Telecom and ETL also providing fixed-line services. In Nepal, there are over five players in the fixed-line market and two mobile network operators, with state-owned Nepal Telecom having over 60 per cent of the market share. Previously, there were three mobile network operators, but with United Telecom's license revoked, the competition in Nepal's mobile sector has been reduced. In the Philippines, while a third mobile network operator (DITO) was awarded a license in 2019, the two major operators (Globe and PLDT) still hold over 90 per cent of the market share combined. The two major operators also have about 70 per cent of the fixed-broadband market, thus giving them significant market power in the telecommunications sector.

A competitive telecommunication market can drive affordability. However, many countries are facing market saturation. In places where operators face limited room for revenue growth, the focus has shifted to cost optimization through the sharing of infrastructure and virtualization of networks.

In the four countries analyzed, infrastructure sharing remains limited. Bhutan, Nepal, and the Philippines focus solely on promoting passive sharing, while Lao PDR does not have any form of infrastructure sharing in place. Regulators can play a key role in encouraging infrastructure sharing to help operators reduce costs, particularly when expanding coverage to rural and remote areas. For instance, Bhutan offers free use of the national shared fiber backbone to operators, provided they

extend managed infrastructure to all 20 dzongkhags (municipal districts). Incentives such as waiving or reducing regulatory fees or tax rates can further promote infrastructure sharing. However, it is crucial for regulators to closely monitor these arrangements to prevent collusion, anti-competitive practices, and any compromise to network resilience.[64]

Active infrastructure sharing is becoming more common and is particularly crucial for 5G deployment due to the high capital investments required. Some mobile network operators have engaged in active infrastructure sharing through technologies such as multi-operator core network (MOCN) and multi-operator radio access network (MORAN), which have allowed operators to pool their spectrum resources, driving spectral efficiency.

According to responses from the four countries, rural connectivity requirements have been formally addressed either through policy mandates or regulatory obligations in all administrations. This proactive approach plays a significant role in enhancing service affordability, as it ensures that underserved and remote areas are included in national digital development plans. By embedding rural connectivity into legal and policy frameworks, governments contribute to reducing the digital divide and promoting equitable access to ICT services.

Effective spectrum management plays a crucial role in promoting competition, expanding network coverage, and enhancing service affordability. Market-based auction mechanisms for spectrum allocation are considered the best practice. Measures such as spectrum caps, coverage obligations in auctions, prioritizing new entrants, and requiring operators to host mobile virtual network operators (MVNOs) have been effective in driving competition, reducing costs, and making services more affordable. In recent years, there have been spectrum auctions with innovative designs, such as combining ascending and reverse auctions (i.e., incentive auctions). For example, the communication regulator of Austria used an incentive auction mechanism in the 5G-pioneer spectrum multi-band auction conducted in September 2020. Successful bidders of the ascending auction had the possibility to earn a price discount on the spectrum fee by accepting coverage obligations. The price discount and level of coverage were determined by a reverse auction (i.e., winning bids would be the lowest cost of deployment and/or the highest level of coverage). The auction resulted in 80 per cent of municipalities previously underserved receiving high-quality mobile broadband coverage.[65]

Some countries, like Australia and Japan, have encouraged the growth of MVNOs to stimulate competition. MVNOs are companies that provide mobile services but do not own the network infrastructure themselves. Instead, they purchase network capacity from mobile network operators. Utilizing network capacity without having to own it frees up costs that are then passed down to the consumer. MVNOs also tend to be more effective in targeting niche segments, which can improve ICT affordability for underserved groups (e.g., women, students, older persons, ethnic minorities, migrants). Moreover, as MVNOs are focused primarily on providing a service rather than maintaining networks, they can better support these vulnerable and marginalized groups in the use of ICT services. Some MVNOs offer value-added services in addition to basic mobile services, such as custom applications and content services. The main challenges for MVNOs include navigating and complying with the complex regulatory environment and high competition with other MVNOs and mobile network operators. Although MVNOs can bring additional revenue to mobile network operators, they tend to view MVNOs as competitors. It is therefore crucial for regulators to have clear rules and

[64] ITU, "Digital Regulation Platform: The Infrastructure Sharing Imperative", 25 August 2022. Available at https://digitalregulation.org/the-infrastructure-sharing-imperative/.

[65] OECD, "Bridging Connectivity Divides", Digital Economy Papers No. 315, July 2021. Available at https://www.oecd-ilibrary.org/docserver/e38f5db7-en.pdf?expires=1721455447&id=id&accname=guest&checksum=6385451D30A3735C15C717620178BC37.

guidelines to facilitate the entry of MNVOs.[66] Simplifying licensing procedures, access to spectrum, and clear guidelines on interconnection arrangements between MVNOs and mobile network operators (e.g., interconnection rates, quality of service, dispute resolution mechanisms) are some of the ways to ease MVNOs' entry into the market.

Another consideration for boosting competition is through satellite communication services, especially since the pricing for geostationary orbit (GEO), medium-Earth orbit (MEO), and low-Earth orbit (LEO) satellite services has become more competitive and performance has improved (see Section 4.1.1 for a discussion on satellite communication services).

3.3 Emergency Preparedness

As shown in Table 4, most (at least three of four) countries have in place policies for cybersecurity, data protection and privacy, and procedures for business continuity and disaster recovery of government functions. The national computer emergency response teams or computer incident response teams in the respective countries are actively engaged in supporting business continuity and disaster recovery. Most of these teams are led by government agencies such as Bhutan's Government Technology Agency, Lao PDR's Ministry of Post and Telecommunications, and the Philippines' Department of ICT. However, only one of the four countries (Nepal) has drafted the NETP, highlighting the need for increased efforts to raise awareness and encourage the development of NETPs in other countries. The Philippines' Department of ICT is in the process of drafting its NETP in line with ITU's guidelines, with plans for release in 2024.

The establishment of mechanisms for resilience assessments of ICT infrastructure and the development of standards for quality of service, especially during emergencies, are critical gaps that need to be addressed. Although countries may be monitoring and reporting on the quality of service of mobile services, many have not mandated quality of service standards to ensure network reliability. Quality of service standards can motivate operators to meet minimum service levels, minimize outages, enhance service availability, and reduce mean-time-to-repair. The Nepal Telecommunications Authority (NTA) has set a quality-of-service baseline for telecommunication services but has not defined the service levels for emergency situations.

Another significant gap is the limited application of network automation to predict and address network issues, particularly during outages. Advanced capabilities like adaptive restoration, adaptive reallocation, and predictive analytics enable automated traffic rerouting, quicker network service restoration, and reduced downtime, yet these remain underutilized. All four countries have ensured topological redundancy of name servers, but not all name servers are geographically redundant. For example, in Lao PDR, all name servers are in Vientiane. BCP-16 recommends placing name servers at both topologically and geographically diverse locations to minimize the likelihood of a single point of failure.

The reliability of the electricity supply is crucial for keeping the ICT infrastructure working. Countries need to continue enhancing the resiliency of their power network and plan for the potential increase in energy demand to power the ICT infrastructure, including data centres. In Lao PDR, the Lao National Data Centre reported having a redundant power supply, but it is not clear whether other critical ICT infrastructure and equipment in Lao PDR, especially in rural and remote areas, have prepared a

[66] Telecom Review Asia Pacific, "MVNO Regulations and Market Entry Challenges in Asia-Pacific Countries", 19 April 2024. Available at https://telecomreviewasia.com/news/featured-articles/4161-mvno-regulations-and-market-entry-challenges-in-asia-pacific-countries.

redundant power supply. The Philippines, Bhutan, and Nepal reported that they do not have measures in place to ensure redundant power supply for the ICT infrastructure. Various backup power options should be explored, including solar power and other renewable energy sources, uninterruptible power supply, backup generators, and battery storage.

The Maldives is investing in renewable energy to enhance the resilience of its power system. In December 2022, the country opened its first 5 MW solar facility outside the capital as part of a programme to develop 50 MW of solar and battery capacity, supported by the World Bank. The Maldives is also expanding rooftop solar capacities, which increased from 1.5 MW to 21.5 MW between 2009 and 2019. To improve grid stability, high-voltage connections are being built between the islands. These efforts improve resilience and are also cost-effective by reducing expenditure on expensive fuel imports.[67] The combination of this diverse set of interventions marks a turning point for the Maldives, moving it away from reacting to emergencies to more sustainable, longer-term solutions.

Table 4: Summary of emergency preparedness in four selected countries

Indicators	Bhutan	Lao PDR	Nepal	Philippines
Cybersecurity Policy		✓	✓	✓
Data Protection and Privacy Policy	✓	✓	✓	✓
Government Procedures for Business Continuity and Disaster Recovery	✓	✓		✓
Country-level Mechanism to Conduct Resilience Assessments of ICT Infrastructure				✓
National Emergency Telecommunication Plan			✓	
Quality of Service Standard			✓	
Name Server Redundancy	✓	✓	✓	✓
Adaptive Restoration and Reallocation				
Predictive Analytics				
Redundant Power Supply for Critical ICT		✓		

Note: Yellow-shaded rows indicate critical gaps that need to be addressed.

3.4 Early Warning Dissemination and Communication

As shown in Table 5, most of the indicators or questions related to early warning dissemination and communication are rated 1 (not known) or 2 (not started), indicating an urgent need to step up efforts in data collection, analysis, and sharing for informed decision-making. This includes commissioning studies to better understand the current reach of the early warning alerts and messages at national and local levels, and identify gaps in early warning dissemination and communication, particularly to vulnerable groups such as women, persons with disabilities, children, older persons, and ethnic minorities, among others.One such study is an assessment of multi-hazard early warning systems in seven Pacific SIDS that takes stock of the capacities, gaps, and needs across the four pillars of multi-hazard early warning systems (see Box 3).

Box 3: Gaps in Warning Dissemination and Communication in Pacific SIDS

An assessment of the multi-hazard early warning systems of seven Pacific SIDS – Cook Islands, Fiji, Kiribati, Nauru, Niue, Tokelau, and Tuvalu – shows that these countries are working towards functional multi-hazard early warning systems. The study assesses all four pillars of multi-hazard early warning

[67] UNDRR, *GAR Special Report 2023: Mapping Resilience for the Sustainable Development Goals* (Geneva, 2023).

systems (Figure 3) and identifies many bottlenecks and barriers in the early warning systems of Pacific SIDS that share commonalities with the findings from this study.

Related to the pillar on warning dissemination and communication, the Pacific SIDS study assessed three areas: (i) whether organizational and decision-making processes are in place and operational; (ii) whether communication systems and equipment are in place and operational; and (iii) whether impact-based early warnings are communicated effectively to prompt action by vulnerable groups.

Globally, there is a shift from the issuance of general warnings to impact-based warnings that provide details about the likely impact of a hazard with actionable information. An example of a general warning may be: "In the next 24 hours, a tropical cyclone is likely to impact the target area", while an impact-based warning may be phrased as follows: "Road closure due to heavy rain is expected tomorrow. Follow the alternative route to avoid flood prone areas. Leave for work at least one hour earlier than normal to avoid significant delays." The successful implementation of impact-based forecasting and warning requires close operational cooperation and shared standard operating procedures between national meteorological and hydrological services, disaster managers, and other stakeholders such as local authorities, infrastructure authorities and mobile network operators. Engagement with organizations representing vulnerable groups such as women, persons with disabilities and ethnic minorities is important to ensure that warnings reach and are acted upon by all vulnerable groups.

From the assessment, the gaps related to warning dissemination and communication include the following:

Operational decision-making

- Poor coordination between warning issuers and the media
- Lack of standard operating procedures for early warning issuance and dissemination
- Lack of progress in using private sector resources for disseminating warnings

Communication systems and equipment

- Insufficient upgrade and modernization, maintenance, and utilization of communication systems and equipment to increase the efficiency and timely dissemination of warnings
- Lack of systematic assessment of the effectiveness and appropriateness of communication channels used for warning dissemination and communication

Impact-based early warning

- Lack of tools to assess warning and communication services along key parameters such as timeliness, accuracy, relevance, and actionability
- Lack of systematic assessment of warning dissemination and communication strategies
- Inadequate tailoring of ICT systems to different population groups
- Slow progress in developing clear, actionable warning messages tailored to different population groups
- Lack of mechanisms to verify that warnings are received and understood by at-risk groups, especially vulnerable groups
- Lack of mechanisms for feedback from end users

Addressing these gaps is crucial to the upgrading and enhancement of existing early warning systems in countries, aligning them with the overarching objective of reducing fatalities and protecting critical infrastructure and assets from future disaster events.

Source: Lalit Kumar Dashora and others, "Readiness Stocktaking of Multi-Hazard Early Warning Systems in Pacific Small Island Developing States", *Asia-Pacific Sustainable Development Journal*, ESCAP, vol. 31, No. 3 (May 2024), pp. 47-76.

According to an ESCAP report, the biggest investments are needed in building local capacities to respond effectively and rapidly to early warning alerts, followed by investments to expand global satellite data use and strengthen networks and services that disseminate early warning messages.[68]

Table 5: Summary of early warning dissemination and communication in four selected countries

Indicators	Bhutan	Lao PDR	Nepal	Philippines
GOVERNANCE				
At what stage is the country in establishing ICT-specific legislations or mandates that enable the ICT ministry, agency and/or regulator to respond to disaster early warning?	1	1	2	1
To what extent is the government enforcing the functions, roles and responsibilities of each actor at all levels to be part of and included in the warning communication strategies and standard operating procedures?	5	2	2	1
At what stage is the government in designating a WMO-registered alerting authority to issue warnings?	5	6	5	5
To what extent is the government identifying stakeholders for specific roles and responsibilities, including regional or cross-border early warning to neighboring countries?	1	1	2	1
At what stage is the government in establishing a regulatory environment to plan and implement interoperability solutions for data and voice communication?	1	2	1	1
To what extent has the government identified relevant network operators and service providers to be involved in providing emergency communication services?	6	2	5	2
How often have regular coordination, planning and review meetings been taking place?	1	2	5	1
At what stage is the country in the adoption of CAP in accordance with ITU-T Recommendation X.1303?	1	2	2	5
At what stage is the country in establishing an NETP?	1	2	5	3
At what stage is the government in establishing policies for the mobile handset manufacturer/importer to support cell broadcast?	1	2	2	6
At what stage is the government in identifying a call tree, communication protocols and authority levels of individual stakeholders?	1	2	2	1
INFRASTRUCTURE				
To what extent have early warning infrastructure and systems been identified, established, tested, maintained and upgraded?	3	3	3	6
To what extent have ICT infrastructure service providers been able to provide data about the scale of communication outages, and their progress on restoration as part of the warning establishment?	1	1	2	1
How many times have assessments been conducted to understand which population groups can be reached by which services?	1	1	2	6
To what extent has cell broadcast facility been enabled in mobile networks?	5	1	2	5
At what stage is the establishment of consensus to utilize private sector resources where appropriate?	1	1	2	1
To what extent are systems in place to send warnings via mobile networks?	3	2	2	5
To what extent have equipment maintenance and upgrade been implemented and redundancies enforced for backup in the event of a failure?	1	1	2	1

[68] ESCAP, *Seizing the Moment: Targeting Transformative Disaster Risk Resilience – Asia-Pacific Disaster Report 2023* (Bangkok, 2023). Available at https://www.unescap.org/kp/2023/seizing-moment-targeting-transformative-disaster-risk-resilience.

Indicators	Bhutan	Lao PDR	Nepal	Philippines
To what extent have key stakeholders been provided with ICT tools needed to communicate during emergency operations?	1	1	2	4
At what stage is the identification of public mobile apps related to early warning?	1	1	2	3
To what extent are automated systems in place to mitigate impacts in case of events with a short time frame for reaction?	1	1	2	5
INCLUSION				
To what extent have warning alerts and messages been tailored to the specific needs of those at risk?	1	2	3	1
To what extent has warning communication reached the entire population, including foreigners, seasonal populations, roamers, and communities in remote locations?	5	1	1	5
To what extent have mandatory technical standards for barrier-free access been established for all ICT-related services?	2	1	1	6
How many early warning local committees have been trained to read the signs of extreme weather events?	1	2	2	1
How many times have assessments been conducted on the capacity of the vulnerable population?	1	2	2	1
To what extent have warnings been tested with women and vulnerable groups to ensure that their needs are addressed?	2	2	2	1
To what extent have multiple channels of communication been used for warning dissemination?	1	2	2	1
What kinds of technological advances have been used to eliminate barriers in mobile phones for early warning dissemination?	1	2	2	1
How many professional and volunteer networks have been formed to ensure that warnings are widely received by last-mile stakeholder groups?	1	2	2	1
To what extent has CAP been applied in various platforms and media to ensure consistency and inclusivity in communicating warning messages?	1	2	2	5
QUALITY AND TRUST				
To what extent are the public and other stakeholders aware of which authorities issue the warnings and that they trust warning messages received?	1	1	1	1
How often have the warning communication strategies been evaluated and provided feedback?	1	1	2	6
To what extent has social media been utilized to share information in a regulated environment during a disaster?	2	2	2	4
To what extent have impact-based early warning messages been used to communicate risk clearly and provide advice on actions that can be taken to reduce risks?	5	1	4	5
How many public mobile apps related to early warning have been identified and informed for secure service facilitation?	1	2	2	1
What kinds of mechanisms have been put in place to activate features targeting specific communities?	1	2	2	1
What kinds of mechanisms have been put in place to inform the community when the threat has ended?	1	1	2	1
How many studies have been conducted to understand how people access and interpret early warning messages?	1	1	1	1
To what extent have communities been involved in the development of early warning messaging?	1	1	2	1
What kinds of two-way communication feedback mechanisms are established with communities to allow them to share real-time information to support continued improvement?	1	1	2	1
How many early warning drills are conducted considering multiple hazards?	1	1	2	1

Notes: The assessment is based on a set of questions, with responses rated on a scale of 0–6 following a combination of desk research and interviews with key informants.

0 = No Response; 1 = Not Known; 2 = Not Started; 3 = Nascent Stage; 4 = Intermediate Stage; 5 = Developed Stage; 6 = Mature Stage.

CAP = Common Alerting Protocol; ICT = Information and Communication Technology; NETP = National Emergency Telecommunication Plan; WMO = World Meteorological Organization.

Based on the responses received and the available data, all four countries, Bhutan, Lao PDR, Nepal, and the Philippines, have WMO-designated national authorities responsible for disseminating early warning messages. This reflects a foundational level of institutional preparedness for emergency communication. However, the implementation of the Common Alerting Protocol (CAP), which standardizes the format for exchanging public warnings and emergency alerts, varies across countries. Among them, only the Philippines has implemented CAP. In contrast, Bhutan, Nepal, and Lao PDR have yet to adopt this protocol, which may limit the effectiveness and interoperability of their alert systems. In terms of regulatory requirements for cell broadcast technology, which enables mass dissemination of alerts via mobile networks, only the Philippines has such regulations in place. The absence of these requirements in Bhutan, Nepal, and Lao PDR highlights a gap in leveraging mobile infrastructure for rapid and wide-reaching emergency communication.

Some notable good practices in early warning dissemination and communication include Bhutan's Code of Practice for SMS Cell Broadcast (SMS CB) Services, Lao PDR's Standard Operating Procedures for Flood Early Warning, Nepal's smart siren system using GSM SIM that has been implemented in 34 flood-prone area to warn people in their local language, and the Philippines' Free Mobile Disaster Alerts Act of 2014 that mandates operators to provide free mobile disaster alerts through Cell Broadcast Services.

It is significant to note that only the Philippines has an established process for conducting regular assessments of the effectiveness of its early warning dissemination mechanisms and strategies. This includes evaluating how alerts are communicated to the public, the responsiveness of systems, and the integration of feedback for continuous improvement. In contrast, Bhutan, Nepal, and Lao PDR currently lack formal processes or frameworks to routinely assess the performance and impact of their early warning systems. This gap may hinder efforts to identify weaknesses, improve outreach, and ensure that alerts are timely, accurate, and accessible to all segments of the population. Regular assessments are essential for maintaining the reliability and trustworthiness of early warning systems, especially in regions vulnerable to natural disasters and other emergencies. Establishing such mechanisms can help these countries strengthen their preparedness and response capabilities.

Building on the previous findings, it is also important to highlight that, based on the responses received and the available data, none of the four countries, Bhutan, Lao PDR, Nepal, and the Philippines, have early warning channels that are specifically tailored to address the needs of persons with disabilities and other vulnerable communities. In most cases, the status was reported as "not known," indicating a lack of data available on established measures or clarity on inclusive communication practices during emergencies. This presents a significant gap in ensuring equitable access to life-saving information, particularly for populations that may face additional barriers in receiving and responding to alerts. Strengthening inclusivity and enabling feedback loops are essential steps toward building more responsive, trusted, and people-centered early warning systems.

Lao PDR's early warning system is being strengthened as part of the Climate Risk and Early Warning Systems initiative supported by the Government of France, World Meteorological Organization (WMO), UNDRR and the World Bank, which aims to provide financing to support early warning systems in LDCs and SIDS. Lao PDR has been implementing community-based flood early warning systems that can be leveraged and strengthened through the use of ICT to improve early warning dissemination and communication to vulnerable communities.

Nepal is finalizing its multi-hazard early warning system framework, with the National Disaster Risk Reduction and Management Authority leading a dedicated task team that acts as the coordination mechanism for the EW4All initiative in Nepal.[69] Similar to Lao PDR, Nepal has also established community-based flood early warning systems with the support of non-governmental organizations, which can be leveraged and strengthened with ICT to reach vulnerable populations.[70]

The Philippine Atmospheric, Geophysical and Astronomical Services Administration (PAGASA) is the National Meteorological and Hydrological Services agency of the Philippines, mandated to issue early warnings. PAGASA maintains a multi-hazard early warning system and has been using the country's cell broadcast system to issue alerts to Filipinos. PAGASA has adopted CAP for multiple types of hazards and launched a project to develop multi-hazard impact-based forecasting and early warnings.

Implementing a multi-channel early warning dissemination and communication strategy that aims for 100 per cent population coverage while addressing the specific needs of vulnerable groups is considered the best practice. This strategy may include technologies such as cell broadcasting and location-based SMS systems. Establishing feedback mechanisms is essential to ensure the approach evolves over time, adapting to the information needs of various groups.

Despite advancements in technology, exploring the wide range of technologies, including older technologies such as radio communication and broadcasting for early warning and emergency response, should not be overlooked to strengthen resilience and ensure that those without access to ICT will receive early warnings. Recognizing the value of radio technology, the Philippines' Department of ICT Regional Office 10 has established a resilient radio communication network using very high frequency (VHF) and high frequency (HF) radio technology across five disaster-prone provinces of Northern Mindanao in preparation for disaster response communication.[71]

The latest report on the EW4All initiative[72] shows that the indicator on "the number of people that are covered by early warning information through local governments or through national dissemination mechanisms" has the highest scores and has seen the greatest improvement in scores since reporting began in 2015. This is due to increasing access to mobile broadband, with 4G network coverage reaching 88 per cent of the world's population. However, lack of affordability continues to be a barrier to ICT access, particularly in low-income economies and these digital solutions must be seen as part of a wider set of communication channels. Low-tech and no-tech solutions play an important part in reinforcing messages carried through other channels and are invaluable in less affluent areas where access to technology is limited, yet communities are often exposed to the greatest risk. Low-tech and no-tech solutions are also robust during power failures and are essential in communities where literacy rates are low or multiple languages are spoken.

[69] WMO, "Nepal holds national consultation – Early Warnings for All and WITH All", 22 September 2023. Available at https://wmo.int/media/news/nepal-holds-national-consultation-early-warnings-all-and-all.
[70] Dinanath Bhandari, "Community-centred flood early warning system in Nepal", South Asia Nadi Sambad, 15 June 2021. Available at https://www.preventionweb.net/news/community-centred-flood-early-warning-system-nepal; Mirianna Budimir and others, "Communicating complex forecasts: An analysis of the approach in Nepal's flood early warning system", *Geoscience Communication*, vol. 3, No. 1 (2020). Available at https://gc.copernicus.org/articles/3/49/2020/.
[71] ITU, "WSIS Stocktaking Success Stories 2024", Zero Draft, 7 May 2024. Available at https://www.itu.int/net4/wsis/forum/2024/Files/outcomes/draft/WSISStocktakingSuccessStories2024_Draft.pdf.
[72] UNDRR, *Global Status of Multi-Hazard Early Warning Systems 2023* (Geneva, 2023). Available at https://www.undrr.org/media/91954/download?startDownload=20240605.

4. Good Practices and Case Studies to Address Gaps

Based on findings from the gap analysis, this section presents some good practices and case studies that can support ITU Member States in addressing the gaps and accelerate progress towards building resilient and affordable national ICT infrastructure.

4.1 Network Resilience

Enhancing network resilience involves increasing network coverage and redundancy, and broadening connectivity choices. In building redundancy and broadening connectivity choices, particularly in rural and remote areas, there are several emerging technologies that can be explored, including fixed wireless access, high-altitude platform station systems, balloons, drones, and satellite systems. With advancements in satellite technology and a reduction in deployment costs, the leveraging of satellite technologies to connect rural and remote areas and diversify connectivity choices can promote network resilience. Section 4.1.1 discusses the different satellite communication services available and presents a case study from Papua New Guinea that shares the process in reviewing the licensing rules and requirements for satellite communication services.

Investment in fibre backhaul connectivity and FTTx technologies is needed for enhancing resilience, especially in preparation for pandemics like COVID-19, which is likely to require more connectivity and network capacity. However, with the high cost of fibre deployment, especially in the last mile, given the cost of civil work, regulatory and policy measures to promote and accelerate fibre deployment, as well as innovative solutions to reduce cost, need to be explored. A potential solution is the co-deployment of the ICT infrastructure with other infrastructures such as roads and highways, railways, power transmission lines, and pipelines. This is discussed in Section 4.1.2 with a case study from Bhutan highlighting their experience in the co-deployment of the ICT and power infrastructure.

4.1.1 Non-Terrestrial Networks

Non-terrestrial networks offer the opportunity to extend network coverage into rural and remote areas and provide an additional connectivity choice for end users, including emergency responders during crises when terrestrial communication systems are damaged or overloaded, thus strengthening the resilience of the ICT infrastructure.

Non-terrestrial networks are networks or segments of networks that use either uncrewed aircraft systems like high-altitude platform stations, balloons and drones that typically operate between 8km and 50km altitudes, as well as GEO, MEO, and LEO satellites to carry transmission equipment, relay nodes, or a base station.[73] Case Study 5 in Section 4.3 shares India's experience in trialing the use of tethered balloons and drones to restore connectivity during emergencies.

GEO, MEO, and LEO satellites for communication services are becoming more accessible and affordable in Asia and the Pacific and offer promising potential for enhancing ICT infrastructure resilience. Traditionally, GEO and MEO satellites have been deployed for communication services due to their wide coverage. However, their high latency (as well as high cost) means that they have been used mostly for backup for emergency communication or to connect the remotest areas with no existing infrastructure. Meanwhile, the advancement of LEO satellite technologies, which have a lower latency as they are closer to Earth, has resulted in their growing popularity for widening network coverage and

[73] Joern Krause, "Non-Terrestrial Networks (NTN)", 14 May 2024. Available at https://www.3gpp.org/technologies/ntn-overview.

enhancing resilience. The new generation of LEO satellite constellations (grouping satellites together) has improved their coverage and throughput, and at a reduced price compared to traditional GEO satellites, although their quality of service still appears to lag behind fibre connections.

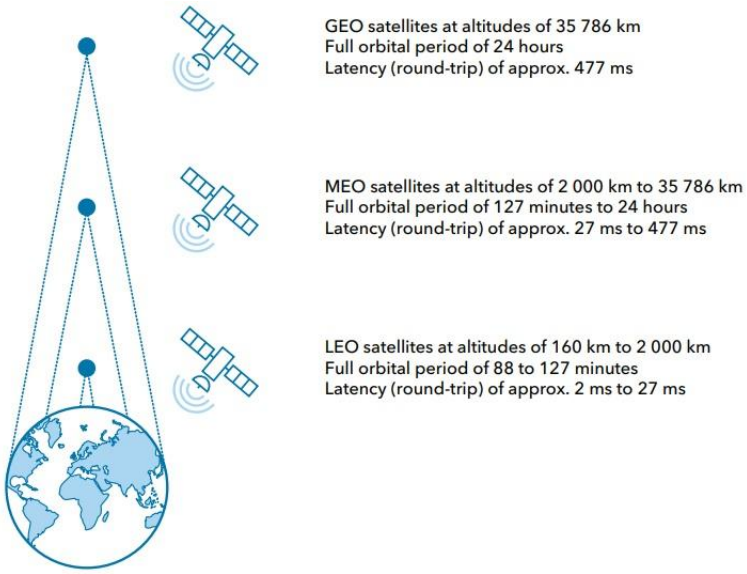


Figure 6: Comparison of GEO, MEO and LEO satellite characteristics

Source: ITU, *The Last-Mile Internet Connectivity Solutions Guide: Sustainable Connectivity Options for Unconnected Sites* (Geneva, 2020). Available at https://www.itu.int/en/ITU-D/Technology/Documents/LMC/The%20Last-Mile%20Internet%20Connectivity%20Solutions%20Guide.pdf.

In Papua New Guinea, the Department of ICT reported that for its planned rollout of the Government Private Network to connect provincial government buildings across the nation, as mandated under the Digital Government Act 2022, LEO services offered by Starlink can potentially cut down the annual budget by 70–90 per cent compared to GEO satellite services serving the same buildings with the same bandwidth.[74]

LEO satellite constellations offer promising potential to connect rural and remote areas. It is also a viable option for LLDCs that are dependent on terrestrial fibre connectivity. Satellite connectivity can serve as a substitute for complex bilateral and multilateral negotiations required to extend fibre connectivity to their country.[75]

In addition to connecting to a ground station, satellites can now connect directly with mobile devices. With the use of the 5G new radio (NR) standard from 3GPP that incorporates integration for non-terrestrial networks, devices will be able to connect seamlessly between traditional cellular base

[74] Department of ICT, Government of Papua New Guinea, "Response to Public Consultation Discussion Paper - LEO/MEO Satellite Services and PNG", 12 September 2023. Available at https://www.nicta.gov.pg/cp-0-29/.
[75] John Garrity and Arndt Husar, "Digital Connectivity and Low Earth Orbit Satellite Constellations: Opportunities for Asia and the Pacific", Asian Development Bank Sustainable Development Working Paper Series No. 76, April 2021. Available at https://www.adb.org/publications/digital-connectivity-low-earth-orbit-satellite-opportunities.

stations and satellite systems (when out of range of terrestrial connectivity).[76] Advancements in direct-to-device (D2D) connectivity are expected to reduce the cost of deployment and operations, as it eliminates costs associated with ground station set-up and maintenance and network integration. These financial savings may be passed on to consumers via lower tariffs. There is also the added benefit of mobility for end users.

Lynk Global, a satellite-to-phone connectivity startup, launched initial D2D services on standard mobile phones (including those operating on 2G networks) in June 2023 in parts of the Cook Islands, Palau and Solomon Islands.[77] The business model adopted is slightly different; instead of providing services directly to consumers, Lynk Global enters into an agreement with local network operators. Through this business model, Lynk Global is leveraging the local operators' existing spectrum rights in orbit, while enabling the local operators to expand network coverage and grow their subscribers. Initial services are for SMS only via its three LEO satellites to users that previously relied on VHF radio networks, with plans to expand to voice calls and Internet access by 2026. Affordability and quality of service will influence the adoption rate. Moreover, the Lynk Global rollout will serve as a backup system during emergency outages.[78]

To enable the wide adoption of satellite services as part of the national ICT infrastructure, several challenges need to be addressed. They include:[79]

- Regulatory constraints – Simplifying licensing processes and reducing regulatory fees for satellite terminals and spectrum could speed up deployment and bring connectivity more quickly to localities that need them the most.
- Spectrum scarcity – Just as mobile technology relies on spectrum frequency availability for the transmission of data, communication satellites also require spectrum for the transmission of satellite signals. But the spectrum is scarce and can be expensive. As a result, close collaboration among telecommunication and satellite operators in spectrum sharing and the sustainable use of spectrum is needed.
- Satellite-enabled device availability – Policies and incentives are needed to increase the supply and demand for satellite-enabled devices, although the 3GPP 5G NR standard means that D2D satellite services would be compatible with most mobile devices, enabling seamless shift between satellite and land-based (2G, 3G, 4G, 5G, and Wi-Fi) networks.
- Global space weather monitoring – Since conditions in near-Earth space can drastically affect a satellite's operations, global space weather monitoring is needed to mitigate the effects of disruptions in real time and better understand how and why they happen.
- Space sustainability – While satellites are predominantly powered by solar energy and use only a small amount of fuel to maintain orbit, their footprint includes the growing problem of space debris and the risk of collisions. The proximity of LEO satellites to Earth may trigger unpredictable changes to the climate. International guidelines and best practices have been developed to minimize space debris, and satellite operators are developing solutions to avoid collision. For example, Starlink built

[76] Armita Satari, "Satellite disruption: how LEO and D2D are impacting telecoms", Telecoms.com, 8 March 2024. Available at https://www.telecoms.com/satellite/satellite-disruption-how-leo-and-d2d-are-impacting-telecoms.
[77] Liam Pye and Lucy Pilgrim, "Palau National Communications Corporation: Bridging the Digital Divide", APAC Outlook, 3 June 2024. Available at https://www.apacoutlookmag.com/technology/palau-national-communications-corporation-bridging-the-digital-divide.
[78] Jason Rainbow, "Lynk Global plans to go public to fund direct-to-smartphone satellites", Space News, 18 December 2023. Available at https://spacenews.com/lynk-global-plans-to-go-public-to-fund-direct-to-smartphone-satellites/; Jason Rainbow, "The promise of direct-to-device", Space News, 14 July 2023. Available at https://spacenews.com/the-promise-of-direct-to-device/.
[79] ITU and World Bank, "Regulation of NGSO Satellite Constellations", Digital Regulation Platform, 28 March 2024. Available at https://digitalregulation.org/regulation-of-ngso-satellite-constellations/.

an autonomous collision avoidance mechanism into each satellite and uses a US Department of Defense database of debris tracking coupled with the satellite's propulsion system to move the satellites out of collision paths.

- Security of satellite telecommunication – Resources need to be allocated to address the security of satellite telecommunication, especially since satellites tend to have a very long lifespan, which means that their technology will become outdated. Therefore, regular security updates are needed, as well as the implementation of other cybersecurity best practices, such as the use of encryption and authentication protocols.

Case Study 1 analyses Papua New Guinea's experience in reviewing and developing licensing rules and requirements for LEO satellite services.

Case Study 1: Papua New Guinea's Process of Licensing for LEO and MEO Satellite Services

Context

Papua New Guinea's National Information and Communications Technology Authority (NICTA), the regulator of telecommunication, recognizes the value of LEO and MEO satellite services in offering broadband services in rural and remote areas. NICTA conducted a transparent public consultation process over a two-month period in 2023 on the licensing rules and requirements for LEO and MEO satellite service providers.

Contribution to Resilience Building

To ensure competitive fairness, contribution to Papua New Guinea's economy, regulatory compliance and consumer protection, the public consultation sought comments on whether additional or different conditions of license should be applied to LEO and MEO satellite service providers compared to other terrestrial network services.

The public consultation received 12 responses that were published on their website. A discussion paper was prepared to guide the public consultation process and a report was published at the end of the process summarizing the results of the public consultation and NICTA's next steps. These are good practices that promotes transparency and builds trust and should be adopted by other countries.

According to the report issued by NICTA, LEO satellite service providers will need to apply for a license with NICTA. However, there will be no restrictions on where LEO services are permitted, and the use of LEO and MEO solutions will be allowed in the universal access and service scheme administered by NICTA to provide ICT connectivity to rural and remote areas. NICTA reported that further review will be required on whether the licensing terms and conditions need to be adjusted, particularly related to quality of service and security, but this will not delay the licensing of LEO and MEO satellite service providers.

Key Takeaways

Transparency builds public trust in the government, which is especially important during crises. Transparency also enables greater ease in promoting collaborations and establishing partnerships to building resilient ICT infrastructure. Moreover, decision-making is strengthened by the inclusion of representatives from all stakeholder segments.

Source: NICTA, "Operator Licensing for the Provision of Low Earth Orbit Satellite Services in PNG", 21 June 2024. Available at https://www.nicta.gov.pg/cp-0-29/.

4.1.2 Infrastructure Co-Deployment

Fibre-optic cable co-deployment along infrastructure such as roads and highways, railways, power transmission lines, and pipelines has been proven to save significant costs and resources.[80] Most of the cost savings in co-deployment are derived from eliminating overlapping civil works. Other benefits of co-deployment include the ease of obtaining rights of way and various other permits and approvals, minimization of disruptions to road traffic or the functioning of utilities as a result of repeated civil works, and streamlining of maintenance and repairs. The avoidance of duplication in construction works can also contribute to reduced social and environmental disruptions.

Co-deployment of transmission lines, especially by placing them in underground access ducts, improves the resilience of critical infrastructure.[81] A project of the Asian Development Bank in Bengaluru city in the state of Karnataka, India, which includes transitioning overhead power distribution lines to underground ducts and the parallel installation of fibre-optic communication cables to protect them from natural hazards, is expected to reduce technical and commercial losses by up to 30 per cent.[82] Case Study 2 details Bhutan's experience in co-deploying the ICT infrastructure with the power infrastructure.

Case Study 2: Bhutan's ICT and Power Infrastructure Co-Deployment

Context

In 2003, in order to meet the growing demand for telecommunication services and increase the capacity of the national backbone network, Bhutan Telecom Limited (BTL), the state-owned telecom operator, and Bhutan Power Corporation (BPC) entered into a co-deployment agreement and laid the first fibre-optic cable system in the country that connected with the Indian fibre-optic cable system to access the submarine cable for international connectivity. Prior to the installation of the fibre-optic cable system, BTL maintained a satellite earth station for international connectivity, which incurred high operational costs and tariff rates. The co-deployment of fibre-optic cables over power transmission lines significantly reduced costs. Based on the agreement between BTL and BPC, BPC would receive maintenance and lease fees, as well as the right to access 12 of the 24 cables. In addition to cost savings, this arrangement generated revenue for BPC and reduced BPC's capital expenditure on its communication infrastructure.

Contribution to Resilience Building

Subsequently, in 2011, to encourage new operators to enter the market and promote a level playing field, the Government of Bhutan consolidated all the fibre assets of BTL and BPC. Both BTL and BPC were given fair compensation for surrendering their fibre assets. The government then allocated licensed operators with a pair of fibre each at no lease charges to keep the price of Internet and telecommunication services low and affordable.

[80] Inter-American Development Bank, *Digital transformation infrastructure sharing in Latin America and the Caribbean* (Washington, DC., 2020). Available at https://publications.iadb.org/en/digital-transformation-infrastructure-sharing-latin-america-and-caribbean.

[81] Arndt Husar, Yoonee Jeong and John Garrity, "Cross-Sector Infrastructure Co-deployment: Closing Digital Connectivity Gaps through Collaboration and Sharing", Asian Development Bank Sustainable Development Working Paper Series No. 86, July 2023. Available at https://www.adb.org/publications/cross-sector-infrastructure-co-deployment.

[82] Asian Development Bank, "ADB Approves $190 Million Loan to Upgrade Power Distribution System in Bengaluru", December 2020. Available at https://www.adb.org/news/adb-approves-190-million-loan-upgrade-power-distribution-system-bengaluru.

Following the consolidation of fibre assets, BPC was mandated to carry out the installation of fibre-optic cables on all existing and planned power transmission lines. The BPC was further mandated to operate and maintain the consolidated fibre assets for which a fund was provided by the government.

However, to maintain and expand the ICT network, challenges persist, particularly in the limited accessibility to sites to fix faults or damages after disasters and natural calamities, since most of the power transmission tower routes do not follow the road path. The Government of Bhutan has mandated telecom operators to follow best practices for contingency planning and business continuity.

Key Takeaways

Government intervention to support infrastructure co-deployment can contribute to significant cost savings and accelerate rollout. However, ensuring network resilience over the long term, considerations for the expansion, operation and maintenance of the ICT infrastructure need to be incorporated right from the start at the planning and design stage.

Source: ESCAP, "ICT Co-Deployment with the Electricity Infrastructure: The Case of Bhutan", Asia-Pacific Information Superhighway Working Paper Series, May 2019. Available at https://www.unescap.org/sites/default/files/ICT%20Co-Deployment%20with%20the%20Electricity%20Infrastructure%2C%20The%20Case%20of%20Bhutan.pdf.

4.2 Affordability of ICT

Good practices for improving ICT affordability include promoting competition, lowering barriers for investment and increasing regulatory certainty. Strategies to consider include: lifting foreign investment restrictions; simplifying licensing requirements and reducing licensing fees; ensuring effective and efficient interconnection among the different actors; encouraging infrastructure sharing and co-deployment of ICT infrastructure with non-ICT infrastructure (see Section 4.1.2); and streamlining and harmonizing right-of-way access. Case Study 3 details India's experience in improving right-of-way access. Section 4.2.1 then proceeds to examine some good practices for improving device affordability.

Case Study 3: India Eases Right-of-Way Access

Context

In the effort to expedite the rollout of 5G networks in India, the Department of Telecommunications issued the Indian Telegraph Right of Way Rules in 2016 with amendments to the rules in 2017, 2021, 2022 and 2023. They are part of the government's process to improve the ease of doing business in India and support the ICT sector in expanding, upgrading and maintaining ICT networks more quickly and efficiently.

Contribution to Resilience Building

The Indian Telegraph Right of Way Rules are considered a key enabler for expediting the deployment of the ICT infrastructure, including fibre-optic cables, mobile towers and 5G small cells on existing street infrastructure.

The rules aim to standardize administrative charges across the country to a maximum of INR1,000 per km for fibre, and a maximum of INR10,000 per application for mobile towers. No charge will be levied for erecting poles or small cells under the control of the central authority. However, a fee of INR1,000 per pole will be charged for establishment of poles, small cells, and telegraph lines that are not in the

control of a central authority. For the use of street infrastructure to deploy telecommunication equipment, a cost of INR150 annually in rural areas and INR300 annually in urban areas will be charged.

The right-of-way rules also mandate the development of an electronic single-window application and clearance process to fast-track decisions on right-of-way permits to within 60 days after application. The amended rules are doing away with the need for approval from a government authority for installing infrastructure over private property. Telecommunication licensees can enter into an agreement with private property owners and will not require any permission from any government authority for installing telecommunication infrastructure such as towers, poles or fibre-optic cables. Moreover, licensees can submit a single application for multiple small cell sites.

In the latest amendments in 2023, the rules allow licensees to temporarily set up ICT infrastructure above ground when their existing underground infrastructure is damaged. This helps restore ICT services quickly to minimize disruption in services to users. The government has also directed that the relevant authority charge no fees for this temporary set-up.

Key Takeaways

The right-of-way rules and their amendments standardize administrative charges for right-of-way access, create an electronic single-window application and clearance process to fast-track right-of-way permit approval, and allow the temporary setup of ICT infrastructure during disasters when existing infrastructure is damaged at no charge. These are good practices for consideration by other countries to facilitate a transparent, cost-effective and rapid upgradation and expansion of the ICT infrastructure, pave the way for the deployment of 5G small cells, and improve resilience.

Sources: Drishti, "Indian Telegraph Right of Way – Amendment Rules, 2022", 29 August 2022. Available at https://www.drishtiias.com/daily-updates/daily-news-analysis/indian-telegraph-right-of-way-amendment-rules-2022; Times of India, "COAI lauds the government's Right of Way rules amendments", 18 August 2023. Available at https://timesofindia.indiatimes.com/gadgets-news/coai-lauds-the-governments-right-of-way-rules-amendments/articleshow/102837383.cms; Tax Guru, "Indian Telegraph Right of Way (Amendment) Rules, 2023", 7 August 2023. Available at https://taxguru.in/corporate-law/indian-telegraph-amendment-rules-2023.html.

4.2.1 Device Affordability

The gap analysis presented in Section 3 finds that the high cost of devices continues to be an obstacle for people to access ICT services in the region and receive early warnings and other critical information. A good practice is reducing the various taxes and tariffs on infrastructure equipment as well as user devices. At the same time, innovative ways of financing smartphones and other ICT devices like computers, laptops and tablets are needed to close the gap in device ownership.

Findings from a study by the Broadband Commission Working Group on Smartphone Access provide some key insights on improving the affordability of smartphones. They include:[83]

- Device financing through affordable loans and flexible payment options –
  - Allow customers to choose the frequency of their instalments to enable them to control their finances and increase confidence in loan repayments.
  - Design targeted financing for marginalized communities, such as women, people from remote locations, and low-income individuals.

[83] Broadband Commission, "Working Group Report on Smartphone Access: Strategies Towards Universal Smartphone Access", September 2022. Available at https://www.broadbandcommission.org/wp-content/uploads/dlm_uploads/2022/09/Strategies-Towards-Universal-Smartphone-Access-Report-.pdf.

    - Integrate device financing initiatives with mobile money to support customer repayment practices and provide potential financiers with creditworthiness data.
    - Use device lock technologies to reduce the cost of device financing.
    - Take a holistic approach by increasing customer engagement with the financing service and guiding them through the whole process of acquiring and using a smartphone.
- Reform taxes and import duties on smartphones –
    - Design tax reforms to consider the benefits of mobile broadband penetration.
    - Set a long-term, balanced approach to taxation to meet domestic revenue collection objectives and provide a conducive environment for digital inclusion and economic development.
    - Examine the total cost and net impact of mobile ownership when designing tax reforms.
    - Reduce taxes for devices below certain thresholds to incentivize smartphone manufacturers to cut prices to make their smartphones eligible for tax reduction/exemption.
- Improvement of device distribution channels in rural and remote areas –
    - Partner with local retail chains and community organizations with whom local customers already engage and have high levels of trust.
    - Invest in training sales agents so they can effectively assist customers through the process of smartphone purchase and acquisition.
    - Provide agents with sample devices to help first-time and price-sensitive customers decide on smartphone purchases.
- Device subsidies are one of the most universal ways of making smartphones affordable to customers who do not have mobile Internet access. However, even if customers can pay the subsidized upfront cost of smartphones, they may not be able to afford the ongoing maintenance, data usage costs and electricity for phone charging. There is also the risk of theft or the opportunity for black market sales of subsidized devices while sellers pocket the difference. Recommendations include the following –
    - Identify partners willing to finance the large investments required for device subsidy and ask governments to consider the development and coordination of national device and connectivity subsidy programmes in collaboration with partners.
    - Reduce the ongoing costs of smartphone ownership by pairing device subsidy with data bundles.
    - Encourage better utilization of universal access service funds, including smartphone affordability and adoption.
    - Budget for device swapping during upgrading of networks (e.g., from 2G and 3G to 4G networks).
    - Partner with providers of complementary services, such as advertisers.
- Reuse of pre-owned devices. Currently, there are no quality standards for refurbishing pre-owned devices. This leads to variable quality of refurbished models for retail, often resold at close to market value. Both could negatively impact the perception of customers. Disposing of refurbished devices in importing countries remains another challenge – one that impacts the environment. Recommendations include the following –
    - Pursue strategic sourcing of devices to reduce the total costs of collecting devices for refurbishment and benefit from economies of scale.
    - Standardize device quality testing and assurance to ensure that only devices that satisfy the required standards are imported.
    - Establish regulations on the importation, resale and disposal of pre-owned devices that also avoid putting an undue burden on the distribution of refurbished devices.

Case Study 4 highlights Pakistan's effort to bridge the gaps between women and men's access to and use of ICT through the adoption of a multi-stakeholder approach to develop and implement its Digital Gender Inclusion Strategy.

Case Study 4: Pakistan's Digital Gender Inclusion Strategy

Context

A national survey conducted by the Pakistan Telecommunication Authority (PTA), the regulator of telecommunication, to inform the nation's Digital Gender Inclusion Strategy, revealed a significant gender gap in mobile phone ownership. In the survey, 51 per cent of men and 41 per cent of women reported that women in their families did not own mobile phones, indicating that women face barriers in owning mobile devices. GSMA's Mobile Gender Gap Report 2024 reported similar findings with 87 per cent of men owning mobile devices (including basic phones, feature phones and smartphones) compared with 49 per cent of women, representing a gap of 38 per cent. Specifically on the ownership of smartphones, there is a 26 per cent gap between men and women, with 52 per cent of men owning smartphones compared with 26 per cent of women. GSMA research finds the top barriers to mobile ownership for women (and men) who still do not own a phone are affordability (primarily of devices, but also data), literacy and digital skills, and social norms.

Contribution to Resilience Building

In the effort to bridge the gender digital divide, PTA launched the Digital Gender Inclusion Strategy in 2024, which adopts a comprehensive approach to addressing the challenges women face in accessing and using ICT services. This includes enhancing digital literacy, improving ICT affordability, investing in relevant content and services, ensuring online safety, and challenging prevailing social norms. The strategy was developed following a multi-stakeholder consultative process and nationwide surveys.

Improving the affordability of mobile devices is one of the priorities of the strategy, with plans to provide subsidies, discounts and tax exemptions for women, and partnerships with the private sector to improve access to affordable devices and data for women.

The Action Plan for Pakistan Digital Inclusion Forum for Gender Equity provides concrete interventions to address the multiple and interrelated challenges identified, which will be implemented through a partnership approach through a series of working groups established. They include working groups on research and data collection, affordability, access, security and safety, women's digital literacy and skills, and inclusion and social norm change. For each working group, the action plan sets out actions and targets for the short (6 months), medium (1 year) and long (3 years) term.

Specifically for the working group on affordability, the target is to have at least 25 per cent more women able to afford mobile phones and the Internet by 2027. Priority areas for interventions include the following:

- Review and revise the telecommunication taxation structure
- Develop policies to reduce the manufacturing and import costs of mobile devices
- Develop business models for providing affordable devices and data for women

Key Takeaways

Globally, the gender digital divide persists, which means that even with universal coverage of ICT networks, not everyone will be able to access and use the ICT services, and receive critical information and services that are available through ICT devices, including early warning messages. The process of developing a Digital Gender Inclusion Strategy is a good practice for resilience building. Improving the affordability of devices and data should be a key priority, but it needs to be part of a holistic strategy that addresses other interrelated barriers, such as the lack of digital literacy and skills, and prevailing social and gender norms.

Sources: GSMA, *The Mobile Gender Gap Report 2024* (2024); PTA, *Digital Gender Inclusion Strategy* (2024). Available at https://pta.gov.pk/category/digital-gender-inclusion-strategy-1520570539-2024-07-13.

4.3 Emergency Preparedness

Emergency preparedness requires a comprehensive approach that considers policy, regulatory, technical and safeguard measures to incentivize organizations to prepare for emergencies and ensure minimal disruptions to information and communication networks during disasters. The establishment or designation of an entity responsible for national ICT infrastructure resilience and emergency preparedness is a good practice. Case Study 5 highlights India's comprehensive approach to emergency preparedness. Case Study 6 details the Republic of Korea's experience in designing and developing a dedicated public safety network for emergency preparedness and response, taking into consideration the needs of first responders for real-time, high-quality information gathering and communication, the cost-effectiveness and sustainability of the system, and the need to continuously keep pace with emerging technologies that could add value to the system. Case Study 7 highlights the critical role that mobile network operators play in emergency preparedness and response, and they should be engaged in emergency preparedness and response.

Case Study 5: India's Comprehensive Approach to Emergency Preparedness

Context

India's Department of Telecommunications has established a dedicated disaster management division tasked with maintaining network connectivity in the event of any disaster or calamity, and disseminating messages, alerts and warnings regarding potential disasters. In addition, the Department of Telecommunications has implemented a comprehensive set of policies to prepare for emergencies.

Contribution to Resilience Building

Mandating infrastructure sharing during emergencies

The government has mandated infrastructure sharing among network operators during emergencies, allowing users to connect to any functioning tower in the affected area, regardless of ownership.

Mandating that network operators maintain power backups and equipment for business continuity and disaster recovery

Power outages are a frequent cause of network disruptions during disasters. The government has mandated that network operators maintain power backups for such situations. Additionally,

regulations require network operators to have a minimum stock of portable base stations and satellite equipment to restore service in case of damaged towers.

Trialing innovative technologies for emergency connectivity

The Department of Telecommunications is trialing the use of tethered balloons and drones to restore connectivity during emergencies. The use of balloons and drones for network restoration offers several advantages. These aerial platforms can cover extensive areas, providing connectivity to a broad region and offering immediate solutions without the need for extensive ground infrastructure. This flexibility is particularly valuable in remote or hard-to-reach areas where traditional network set-ups may be impractical. Additionally, balloons and drones can be rapidly deployed, significantly reducing the downtime experienced by affected communities. Trials are set to be conducted between June 2024 and June 2025 to assess whether this approach can be scaled and applied in real-world disaster scenarios.

Incorporating privacy-by-design and security-by-design principles in technology deployments

Incorporating balloons and drones into the disaster response strategy can enhance communication during emergencies. While the potential benefits are clear, implementing balloons and drones raises privacy and security concerns. The definition of "emergency" and the duration for which these platforms will be used post-emergency need to be clearly outlined. Drones, in particular, are often associated with surveillance, and their use in public areas must be carefully regulated to prevent potential privacy violations.

Key Takeaways

The establishment or designation of an entity responsible for national ICT infrastructure resilience is a good practice. Other good practices for emergency preparedness include: (i) mandating infrastructure sharing during emergencies; (ii) mandating that network operators maintain power backups and equipment for business continuity and disaster recovery; (iii) trialing innovative technologies for emergency connectivity, such as balloons and drones; and (iv) incorporating privacy-by-design and security-by-design principles in technology deployments.

Sources: Telecom Review Asia Pacific, "DoT Explores Balloon and Drone Deployment to Ensure 5G Connectivity During Emergencies", 4 June 2024. Available at https://www.telecomreviewasia.com/telecomreviewasia.com/news/technology-news/4282-dot-explores-balloon-and-drone-deployment-to-ensure-5g-connectivity-during-emergencies; Times of India, "How and when DoT wants to use balloons and drones for 5G", 3 June 2024. Available at https://timesofindia.indiatimes.com/technology/tech-news/how-and-when-dot-wants-to-use-balloons-and-drones-for-5g/articleshow/110645185.cms; Hema Kadia, "DoT Testing Drones & Balloons for 5G Emergency Connectivity", TeckNexus, 5 June 2024. Available at https://tecknexus.com/5gnews-all/dot-testing-drones-balloons-for-5g-emergency-connectivity/.

Case Study 6: Republic of Korea's LTE-based Public Safety Network Dedicated to Emergency Preparedness and Response

Context

The Republic of Korea's Public Safety Network was developed between 2002 and 2021 to enhance the country's disaster response capabilities by enabling communication through a unified network during disaster situations. This achievement marked the world's first nationwide disaster safety communication network based on 4G long-term evolution (LTE) technology.

The Public Safety Network supports real-time situational awareness, video streaming and the sharing of high-quality images during disaster situations for gathering mission-critical intelligence and enabling more effective communication to improve response management. The Public Safety Network is also used to provide day-to-day support to emergency services.

Contribution to Resilience Building

The Public Safety Network was allocated spectrum in the 700MHz Band 28 (a PPDR spectrum), which is shared with two other service users – LTE-R for railways and LTE-M for maritime services. The network allows the three service users to share the RAN to reduce interference and save costs. All three service users have access to the same command centres located across the country.

The network is not designed based on subscriber growth predictions like a traditional mobile network. Instead, it focuses on economies of scale and channel capacity for core services across geographical areas. This allows more users to access limited base station resources at any given time. The Public Safety Network will integrate the Internet of Things platform, drones and wearable devices during the first stage, and 5G, artificial intelligence, m-Workspace and robotics by 2025.

Key Takeaways

In designing and developing a dedicated system for emergency preparedness and response, it is important to take into consideration the needs of first responders for real-time, high-quality information gathering and communication, the cost-effectiveness and sustainability of the system, and the need to continuously keep pace with emerging technologies that could add value to the system.

Sources: ITU, "WSIS Stocktaking Special Report: The Republic of Korea's ICT Journey 2015–2023 Timeline", 2024. Available at https://www.itu.int/net4/wsis/forum/2024/Files/outcomes/draft/WSISStocktakingSpecialReport_ROKTimeline.pdf; Samsung, "Samsung to Deploy the World's First 3GPP Standard Based Public Safety LTE Solution in Korea" Press Release, 11 February 2016. Available at https://www.samsung.com/global/business/networks/insights/press-release/samsung-to-deploy-the-worlds-first-3gpp-standard-based-public-safety-lte-solution-in-korea/; ATDI, "PS-LTE for public safety networks", 20 April 2021. Available at https://atdi.com/managing-public-safety-networks/.

Case Study 7: Role of Mobile Network Operators in the Philippines during Typhoon Rai

Context

Typhoon Rai was the strongest storm to hit the Philippines and the second deadliest disaster globally in 2021, after the Haiti earthquake. Nearly 8 million people were affected by the typhoon, with many communities suffering compounding effects due to the ongoing COVID-19 pandemic. Across the Visayas and northern Mindanao, many people lost their homes and there was widespread damage to livelihoods, agriculture and infrastructure. Power lines, water supplies and communication networks were destroyed and interrupted in many communities. The disruption of power and communication networks posed communication challenges, disrupting emergency response efforts.

Contribution to Resilience Building

Mobile network operators are mandated by law to participate in emergency preparedness and response

The mobile industry has been working closely with government authorities in the Philippines in preparedness, early warning and response. The country has a well-established system for disaster risk management at the national level, led by the National Disaster Risk Reduction and Management

Council (NDRRMC) under the Office of Civil Defense. In addition, provincial and local governments must establish their own Disaster Risk Reduction and Management Office. Mobile network operators are required to support disaster preparedness and response activities in the Philippines. The Philippines' Free Mobile Disaster Alert Act of 2014 mandates network operators to issue free public warnings via mobile phones.

In emergency response, the needs of different groups of people must be considered

Both Globe and PLDT, the two main telecom operators in the Philippines,[84] were active in the response to Typhoon Rai, supporting the government, first responders and residents of the Philippines. Prior to the typhoon's landfall, both Globe and PLDT activated a quick response team to ensure continuity of operations and prepositioned backup power generators and network equipment, and emergency communication stations (for free calls, free Wi-Fi, and free charging) to be deployed in areas forecasted to be affected by the typhoon. Additionally, the mobile network operators worked with governments to preposition aid and supplies in key areas to allow them to best support customers, employees and the wider community in the immediate aftermath of a disaster.

Multiple ready-to-deploy communication and power solutions for emergency response is necessary

Globe ensures resilience through flexible, ready-to-deploy solutions for emergency response. These solutions include Cellsite-on-Wheels and Tower-on-Wheels, both of which can handle up to 1,000 simultaneous calls within a 3–5km radius. Power backup solutions include fuel cells, batteries, power generators and Generators-on-a-Truck. Additionally, the company has a complete mobile cell phone network system called Cellsite-on-a-Light-Truck, which is powered by mobile generators. Globe also has a Network-in-a-Box, which is a transportable cell site that can be easily carried like a backpack by personnel, and a deployable mobile command centre to manage resources on ground. Globe has been supporting the government in its response and rescue operations through the deployment of emergency equipment, as well as Globe personnel from strategic locations to disaster-affected areas, by land and air. Globe has strengthened partnerships with local government units, trade distributors and communities across the Philippines for the provision of free calls and SMS, charging stations, and Internet connectivity in disaster-affected areas.

Emergency planning and institutional structures in place to support response is key

Their quick actions in preparing for the impact of Typhoon Rai was possible because the government and mobile network operators already had systems and protocols in place to respond to disasters. Both Globe and PLDT have developed strong preparedness plans and structures. For example, Globe has a Service Command Centre that continuously monitors conditions that can rapidly escalate into emergencies or disasters. The Service Command Centre also guides Globe in its business continuity plans and participates in simulation drills organized by the government. These types of drills and simulations allow organizations to practice their response procedures, refine their strategies and ensure that their plans are effective.

Globe frequently updates their business continuity plan to include response procedures to extreme weather events and preferred local partners to help reinstall electricity and water supplies. Moreover, Globe's mobile network towers are built to be flood resistant and can withstand wind speeds of up to 350km/hour.

[84] The government awarded a third telecom operator license to DITO in 2019.

Key Takeaways

Mobile network operators can play a key role in restoring connectivity faster, supporting community needs better and working with the government for a coordinated response. Mobile network operators, as well as other private sector companies and civil society organization representing vulnerable groups should be engaged in emergency response efforts. Regular drills that engage these different actors are essential for emergency preparedness.

Mobile network operators with institutional structures and plans in place for emergency response are better prepared for crises. Moreover, multiple ready-to-deploy communication and power solutions for emergency response are necessary.

Source: GSMA, "The Role of Digital and Mobile-Enabled Solutions in Addressing Climate Change", February 2021; GSMA, "Typhoon Rai Response: The role of the mobile industry", March 2022. Available at https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/wp-content/uploads/2022/03/Typhoon-Rai-Response_Final.pdf.

4.4 Early Warning Dissemination and Communication

For early warning systems to be effective, warning dissemination and communication should be accessible by all and sent in ways that everyone can access and understand, including persons with disabilities and those who are illiterate. Ensuring that early warnings are impact based with clear information on the early actions that should be taken as a result of hazards is essential. This requires community consultations to translate technical disaster- and climate-related information into user-friendly, inclusive and locally relevant messages for the community.

Three case studies from Cambodia (Case Study 8), India (Case Study 9) and Fiji (Case Study 10) detail the evolution of their early warning systems and discuss some good practices as well as the challenges they encounter. A good practice that is consistently highlighted is the establishment of multiple communication channels for early warning dissemination and communication, which includes geo-located mobile-based channels such as cell broadcasting and/or location-based SMS. This can better ensure that warning messages are received by all people in the alerting area, regardless of age, gender or ability.

The establishment of policies, regulations and/or standard operating procedures for generating and issuing warnings that are accessible to the whole population, especially the most vulnerable is another good practice. They should include considerations of the information and communication needs of vulnerable groups such as persons with disabilities, older persons, people living in remote areas without access to connectivity, women and girls, individuals with low literacy levels, indigenous peoples, and migrants. Implementing CAP helps to standardize the warning message content, ensuring consistency in the information transmitted over numerous communication channels, increasing warning effectiveness and trust.

Multi-stakeholder participation and capacity building in designing and developing the early warning systems are key. It is therefore important to develop formal mechanisms for different stakeholders, such as business and infrastructure operators, community leaders and local government representatives, and civil society organizations representing vulnerable groups, to actively participate in the design and implementation of the early warning systems. System and equipment maintenance is often reported as a major challenge, which needs to be factored in during the early warning system design and planning phase.

Case Study 8: Cambodia's EWS1294

Context

Since 2013, the National Committee for Disaster Management, with support from People in Need, a non-governmental organization, has developed Cambodia's first national early warning system, called EWS1294, which provides disaster-related information to national and provincial authorities, and enables authorities to disseminate warning messages to communities. EWS1294 started as an interactive voice response system with the short code 1294 for flood early warning information and dissemination. It was first piloted in three flood-prone villages in Pursat province and has today expanded nationwide, delivering multi-hazard early warning messages across multiple communication channels. When the COVID-19 pandemic broke out in early 2020, provincial officials utilized the system to deliver safety information to the public.

Contribution to Resilience Building

Sensors from the solar-powered water gauges installed throughout the country continuously monitor water levels and send the acquired data to the EWS1294 dashboard via the Cambodian cellular network. When the set water threshold is reached, the system informs provincial disaster management authorities about the risk. Under the technical supervision of the National Committee for Disaster Management, authorities from the Provincial Committees for Disaster Management disseminate alerts to the population via the EWS1294 dissemination dashboard to multiple communication channels through the implementation of CAP. Early warning messages are disseminated through SMS, Facebook and Telegram in text format, and radio broadcasting, loudspeakers and the interactive voice response system in audio format to address the literacy barrier. To receive early warning messages through the interactive voice response system, individuals need to subscribe to the service by calling 1294 free of change.

Key Takeaways

Capacity building and the delegation of responsibilities to local authorities for early warning is essential for timely and effective early warning. Local governments play an important role in linking with national and regional-level early warning mechanisms, and establishing good rapport with communities in their jurisdiction, including the best ways to disseminate early warnings and encourage early actions, and ensuring that vulnerable groups are not left behind.

Sources: UNDRR, *Words into Action: Engaging for Resilience in Support of the Sendai Framework for Disaster Risk Reduction 2015–2030* (Geneva, 2023). Available at https://www.undrr.org/words-into-action/guide-multi-hazard-early-warning; People in Need, "Cambodia's Early Warning System 1294: An Adaptable Technology Promoting Safety for All", 22 March 2022. Available at https://www.peopleinneed.net/cambodias-early-warning-system-1294-8693gp; People in Need, "Empowering Resilience: People in Need's Global Impact Through Early Warning Systems", 17 December 2023. Available at https://www.peopleinneed.net/empowering-resilience-people-in-needs-global-commitment-to-early-warning-systems-for-a-safer-tomorrow-11063gp.

Case Study 9: Early Warning Dissemination System in Odisha, India

Context

The Odisha region of India stretches over a 480km coastline and has been categorized as a high-risk area affected by cyclones, foods, droughts, heatwaves and tsunamis, to which the region's residents are especially vulnerable given their fragile socioeconomic situation. The Odisha State Disaster Management Authority, in collaboration with governmental and non-governmental organizations,

private sector companies such as Tele Communication Consultants of India Ltd. and L&T, and the World Bank, made Odisha the first Indian state to have an early warning system in place for people living along the coastline.

Contribution to Resilience Building

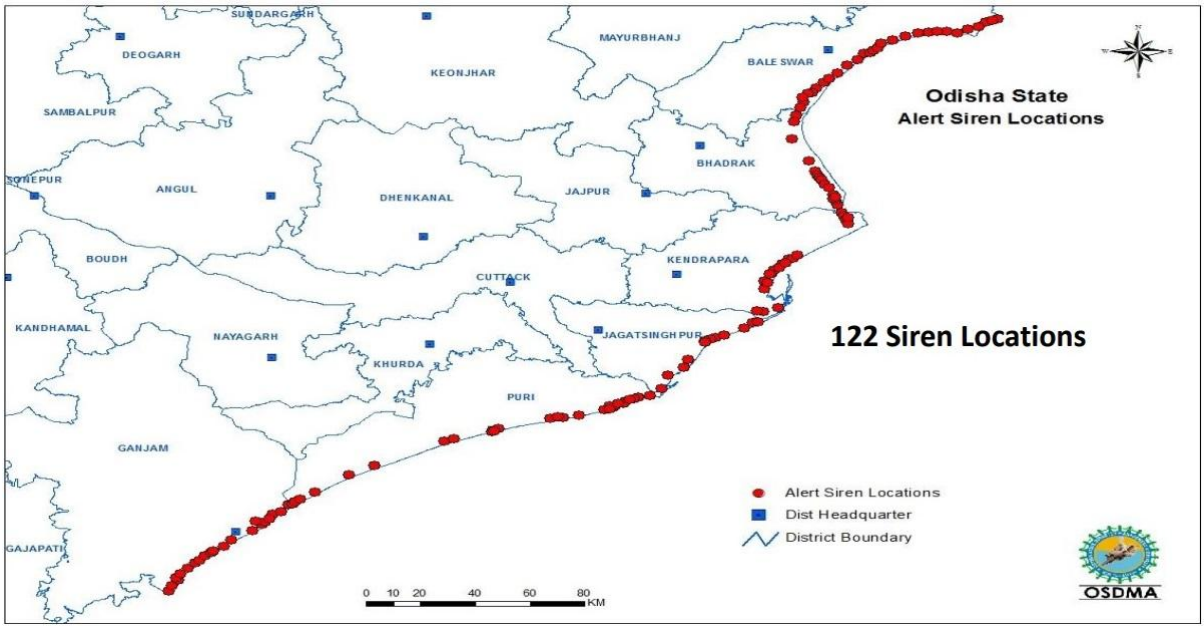
Standard operating procedures were established for disseminating warning messages from the state-level emergency operation centre to 6 district-level and 22 block-level emergency operation centres, and to 1,205 coastal villages that are highly prone to cyclones, floods and tsunamis.

Multiple channels for early warning dissemination were established using technologies such as SMS, digital mobile radio, mobile voice and data satellite systems, and 122 siren towers installed along the coast to warn villagers and fisherfolks at sea. The siren towers were often established in the premises of government buildings or on cyclone shelters for ease of access, operation and maintenance. A cell broadcast system is in place since 2023.

The sirens can disseminate three kinds of alert messages – tones, pre-recorded voice messages and live audio streaming. Pre-recorded voice messages are available in five languages including Odia, English, Hindi, Telugu and Bengali. Live audio streaming can be done from the state-level or block-level emergency operation centres. Commercial power supply along with diesel generators, uninterruptible power supply systems and solar power systems are used in the siren towers. The Odisha State Wide Area Network and VHF radio networks are used as primary channels for communication, and the general packet radio service (GPRS) network as the secondary channel for redundancy. The siren is connected with 1,200 Watt hooters, which can cover 1.5km radius of its surrounding.

CAP is already incorporated in Odisha's SMS-based warning dissemination system, which has been successfully used during COVID-19 and Cyclone Amphan in 2020. CAP is in the process of being incorporated in the siren system.

Figure 7: Location of Coastal Alert Sirens Installed



Key Takeaways

Leadership from the Odisha State Disaster Management Authority in mobilizing resources, overseeing, monitoring and conducting quality audits of the early warning dissemination system was a critical success factor. The private sector played a key role in providing technical inputs, ensuring systems integration, and system and equipment maintenance.

Sources: Odisha State Disaster Management Authority, "Early Warning Dissemination System (EWDS)". Available at https://www.osdma.org/preparedness/early-warning-communications/ewds/ (accessed on 28 July 2024); Special Relief Commissioner, "Coastal Siren Integration with Common Alerting Protocol (CAP) in Odisha", presentation, no date. Available at https://ndma.gov.in/sites/default/files/PDF/CAP-ERSS-Workshop/Session-3/Session-3-PPT-4-Odisha.pdf (accessed on 28 July 2024); Dinalipi "Cell broadcast alert system tested successfully in Odisha", 25 October 2023. Available at https://www.dinalipi.com/index.php/cell-broadcast-alert-system-tested-successfully-in-odisha/.

Case Study 10: Inclusive Early Warning Dissemination and Communication in Fiji

Context

The concept for Women's Weather Watch (WWW) began in 2004 when femLINKpacific, a feminist media organization, interviewed women in remote communities who had been affected by the floods in the north of Fiji. These interviews found that local women had been excluded from designing, planning and implementing disaster relief and reduction efforts. In 2009, following Cyclone Mick, femLINKpacific again observed that women were excluded from relief efforts, leading to the official launch of WWW.

Contribution to Resilience Building

WWW began with simple SMS messaging, with a focus on supporting female community leaders to better understand and pass on climate-related information and warnings to their communities. In 2017, WWW launched a bulk SMS system with Digicel, and began utilizing online media platforms, community radio, a podcast and a comic series called HEROWINS to disseminate messages and awareness.

Since then, WWW has evolved into a communication platform, led by Fijian women, to monitor climate-related disasters in communities. It centres on two-way communication between communities and the WWW hub during emergencies and across disaster cycles (i.e., response, recovery, preparedness, mitigation).

In preparation for disasters, WWW consults with local and diverse women in communities to translate the technical climate-related information and weather warnings sent by the Fiji Meteorological Service into early warning messages that are understandable to the local communities and in the local language. Messages go through an approval process with government officials to ensure that they are in line with national disaster communication and information standards. These warning messages are then stored in a digital message bank for quick access and use during disasters.

During a disaster scenario, when a warning is received by the Fiji Meteorological Service, the corresponding WWW message is retrieved from the message bank and sent through various channels, including the bulk SMS system, two-way community radio, and online social media platforms such as Facebook and Viber.

WWW members can send live updates via SMS back to the WWW hub, which is a powerful tool for monitoring the situation on the ground in real time. In many cases, WWW alerts and warnings reach rural communities before authorities and humanitarian actors can disseminate warnings and relief.

This WWW model has been replicated in Vanuatu through the Women I Tok Tok Tugeta network with inclusive and relevant early warning messages reaching 80 per cent of its population, and in Papua New Guinea through the Meri Gat Pawa, Meri Gat Infomesen (Women Have Power, Women Have Information) initiative with inclusive and relevant early warning messages reaching over 50 per cent of its population.

Ensuring that persons with disabilities are receiving early warning messages, the Fiji Disabled Peoples Federation established an emergency operations centre in 2018 that is activated during a crisis. Once the emergency operation centre receives email notifications from the National Disaster Management Office and the National Meteorological Services, the emergency operation centre mobilizes the Fiji Disabled Peoples Federation network of organizations to disseminate early warning messages through established communication protocols and channels in ways that are accessible to persons with disabilities.

Key Takeaways

These women-led and disability-inclusive initiatives complement and enhance the effectiveness of government-led early warning systems. It is important to integrate and build the capacity of such community- and women-led networks and initiatives to ensure that early warning dissemination and communication is inclusive, accessible and actionable for all. This should include investment in capacity building of women, persons with disabilities and other vulnerable groups, including in enhancing climate and disaster risk knowledge, and digital literacy and communication skills. It should also provide an enabling environment for them to participate in decision-making processes. For example, government-led committees, advisory groups and other decision-making bodies on early warning should include women and representatives from communities and local partners, to ensure the systems and services remain relevant to local needs.

Source: UNDRR, “Inclusive and Accessible Multi-Hazard Early Warning Systems: Learning from Women-Led Early Warning Systems in the Pacific", 2022. Available at https://www.undrr.org/publication/inclusive-and-accessible-multi-hazard-early-warning-systems-learning-women-led-early.

5. Recommendations

The ICT infrastructure has kept the economy and international trade going during the COVID-19 pandemic, but unfortunately, it has not been a lifeline for all. Without access to high-quality ICT connectivity, millions of people continue to face greater exclusion. We need to build back better from the crisis. The COVID-19 pandemic has provided an opportunity to rethink and reformulate strategies for national ICT infrastructure resilience towards current and future threats and crises. It is important to have an ICT infrastructure that can ensure redundancy and diversity of network routes and equipment and can increase the speed and scale at which resources can be mobilized and accessed for restoration of services when hit by crises, disasters and other shocks.

Based on the framework used for assessing the resilience of national ICT infrastructure, as well as the good practices and case studies presented in this report, a summary of the recommendations across the four pillars for building the resilience of the national ICT infrastructure is presented below for ITU member States' deliberation.

Bridging Data Gaps

A notable limitation highlighted in this study is the unavailability and insufficiency of data required to comprehensively assess the resilience of the national ICT infrastructure. To address this, a key recommendation is to establish a systematic approach for collecting, analyzing, and sharing disaggregated data. This would support the effective measurement and monitoring of progress in enhancing the resilience of the national ICT infrastructure, based on the assessment framework developed during the project. More specifically:

- Review the ICT indicators and develop standardized measures for the different types of connectivity (e.g., fixed wireless, satellite), the quality of users' experience across the different types of connectivity, and the affordability of both devices and data plans.
- Support capacity building of national and local organizations in data collection, analysis and sharing of relevant disaggregated quantitative and qualitative data for informed decision-making, especially for designing and improving early warning dissemination and communication and assessing its effectiveness and inclusion (i.e., vulnerable groups' ability to receive, comprehend and act on the alerts).
- Establish data frameworks and mechanisms for data collection, mapping, analysis and sharing, ensuring interoperability between systems, and incorporating safeguards such as cybersecurity and privacy and data protection.

Network Resilience

Summary of recommendations aimed at strengthening network resilience focuses on enhancing reliability, robustness, and adaptability of national ICT infrastructure to ensure continued service availability in the face of disruptions, whether due to natural hazards, technical failures, or other unforeseen events.

- Adopt the United Nations Principles for Resilient Infrastructure in the development of new infrastructure systems and the upgrading of existing infrastructure systems.
- Develop and implement a combination of policies, regulations, incentives and public financing to promote and accelerate ICT infrastructure development and expand broadband access in unserved and underserved areas.

- Explore the potential of fixed wireless access, high-altitude platform station systems, balloons, drones, and GEO, MEO and LEO satellite systems for expanding broadband connectivity to unserved and underserved areas, and for emergency preparedness.
- Develop national regulatory frameworks to enable the deployment of new ICT infrastructure and systems while ensuring fair pricing and competition, transparency in operations and agreements, and compliance with human rights law.
- Encourage the co-deployment of the ICT infrastructure with other infrastructures such as major roads and highways, railways, power transmission lines, and pipelines.
- Support the digital mapping of regional and national infrastructure assets and promote cross-sectoral data sharing.
- Create a favorable investment environment and improve the ease of doing business to encourage private sector and foreign investment in the ICT infrastructure.
- Establish mechanisms that mandate risk and resilience assessments as part of national ICT infrastructure development.
- Adopt policies to support the establishment and operation of IXPs in diverse locations, including outside capital cities.
- Promote and support the establishment of high-quality data centres (Tier 4) in diverse locations, including outside of capital cities.
- Ensure risk-informed selection of IXP and data centre locations and create standards for their development to promote resilience, energy efficiency, integration of renewable energy sources, and security (both cybersecurity and physical security).
- Build capacity and incentivize DNSSEC deployment and increase the validation rate.
- For GMDSS, PPDR agencies, and amateur radio operators, dedicate and harmonize the spectrum for cross-border mobility and wide geographical coverage during crises and emergencies.

Affordability of ICT

These recommendations focus on reducing the cost barriers to access and usage of ICT services, particularly for underserved populations, by promoting fair pricing, fostering competition, encouraging infrastructure sharing, and supporting targeted policy interventions.

- Adopt policies and regulations to promote and incentivize passive and active infrastructure sharing.
- Monitor infrastructure sharing arrangements for any signs of collusion and anti-competitive behavior, as well as reduced network resilience.
- Explore ways to boost competition in the telecommunications market, for example, by facilitating the entry of new players such as MVNOs and/or satellite operators.
- Raise awareness and promote the use of technologies such as MOCN and MORAN to drive spectral efficiency.
- Include targets in national broadband plans or ICT policies and strategies that relate to improving the affordability of ICT devices and data plans.
- Develop and implement evidence-based policies and interventions to improve device and data affordability.
- Improve the affordability of devices and data as part of a holistic strategy that addresses other interrelated barriers such as the lack of digital literacy and skills, lack of relevant content and services, online threats and risks, and prevailing social and gender norms.
- Diversify IXP landscape to improve resilience, performance, and competitiveness.
- Promote the coordinated deployment of infrastructure alongside other public works, such as roads, by utilizing shared rights of way to enhance efficiency and reduce deployment costs.

Emergency Preparedness

The recommendations focused on enhancing emergency preparedness aim to ensure that ICT systems remain operational during a crisis by strengthening early warning systems, improving coordination among stakeholders, establishing contingency plans, and building the capacity of relevant institutions to respond effectively to emergencies.

- Develop and implement an NETP in line with ITU guidelines.
- Build capacity and incentivize the implementation of adaptive restoration and adaptive reallocation, as well as predictive analytics, to better identify potential network congestion, hardware failure and other issues.
- Establish or designate an entity responsible for national ICT infrastructure resilience and emergency preparedness.
- Develop standards for quality of ICT services, especially during emergencies, and monitor their compliance.
- Mandate infrastructure sharing among network operators during emergencies, allowing users to connect to any functioning tower in the affected area, regardless of ownership.
- Mandate that network operators establish institutional structures and plans for business continuity and disaster recovery, including multiple ready-to-deploy communication and power solutions for emergency response.
- Mandate that network operators maintain power backups and equipment for business continuity and disaster recovery.
- Incorporate privacy-by-design and security-by-design principles in technology deployments according to the cybersecurity, data protection, and privacy legislations.
- Engage network operators, other private sector companies and civil society organizations representing vulnerable groups in emergency preparedness and response efforts.
- Conduct regular drills that engage these different actors for emergency preparedness.
- Enhance the resilience of the power infrastructure and plan for the potential increase in energy demand to power the ICT infrastructure, including data centres, in a sustainable manner, encouraging the use of renewable energy sources.
- Place DNS servers at topologically and geographically diverse locations to minimize the likelihood of a single point of failure.
- Leverage artificial intelligence for disaster connectivity mapping to support informed decision-making across all phases of disaster management.

Early Warning Dissemination and Communication

These recommendations aim to strengthen the effectiveness, inclusiveness, and reach of early warning messages to protect lives and livelihoods by enhancing systems, processes, and strategies.

- Adopt CAP, the international standard for early warning message generation, that enables the exchange of emergency alerts and public warnings over all kinds of ICT networks.
- Conduct studies to better understand the current reach of early warning alerts, and identify gaps in early warning dissemination and communication, especially for vulnerable groups (e.g., persons with disabilities, women, older persons, children, ethnic minorities, etc.).
- Establish evidence-based policies, regulations and/or standard operating procedures for generating and issuing warnings that are accessible to all, especially vulnerable groups.
- Establish multiple communication channels for early warning dissemination and communication, incorporating low-tech and no-tech solutions.

- In identifying appropriate communication channels for early warning dissemination and communication, gain a better understanding of at-risk groups' access to and use of ICT, including their behaviors and perceptions.
- Develop formal mechanisms for different stakeholders, such as business and infrastructure operators, community leaders and local government representatives, and civil society organizations representing vulnerable groups, to actively participate in the design and implementation of the early warning system.
- Promote media and private sector engagement in early warning dissemination and communication, including with network operators, and explore the potential for deploying cell broadcasting and/or location-based SMS systems.
- Develop a mechanism to regularly monitor and evaluate early warning dissemination and communication along key parameters such as timeliness, accuracy, relevance and actionability, especially for vulnerable groups.
- Shift from the issuance of general warnings to impact-based warnings that provide details about the likely impact of a hazard with actionable information.
- Build the capacity of organizations representing vulnerable groups to complement and enhance the effectiveness of government-led early warning dissemination and communication, ensuring that it is inclusive, accessible and actionable for all.
- Factor in system and equipment maintenance arrangements and costs in the early warning system design and planning phase.
- Establish a regular coordination mechanism among stakeholders, including government agencies, the private sector, non-governmental organizations, regional bodies, and community organizations.

Conclusion

ICT resilience is undeniably essential for enabling timely emergency response, maintaining continuity in the implementation of effective policies and programs, and achieving the targets set under the Sustainable Development Goals (SDGs). Resilient ICT systems serve as the backbone of inclusive and sustainable progress, helping safeguard both people and development gains in the face of growing global uncertainties. To meet the demands of an increasingly complex risk landscape, ICT infrastructure must be designed and continuously upgraded to withstand and recover from a wide range of threats, including natural disasters, pandemics, armed conflicts, network or power outages, and physical disruptions such as communication cable cuts. Without robust systems in place, countries risk falling into repeated cycles of response and recovery, which can stall socioeconomic development and divert attention and resources from long-term goals.

In addition to infrastructure resilience, service affordability remains a critical factor in ensuring equitable access to digital services, particularly for underserved and remote communities. Service affordability enables broader participation in the digital economy, supports education and healthcare delivery, and enhances social inclusion. Equally important is emergency preparedness, which relies heavily on the strength and responsiveness of ICT infrastructure. National Emergency Telecommunication Plans, Early warning systems, real-time communication channels, and inclusive dissemination mechanisms are vital for protecting lives and minimizing service disruption during emergencies.

As mentioned earlier, this study is intended to serve as a knowledge resource for policymakers, regulators, telecom service providers, and investors from ITU membership from Asia and the Pacific (ASP) region and beyond, to support the development of an affordable and resilient National ICT Infrastructure. However, the study also faced challenges due to limited data availability across several key indicators, which constrained the depth of analysis in some areas. This underscores the need for improved data collection, monitoring, and reporting frameworks to support evidence-based policymaking and targeted interventions.

The recommendations presented in this report advocate for a shift away from short-term, reactive measures toward a comprehensive and holistic approach to ICT infrastructure resilience. This must be prioritized, especially in LDCs, LLDCs, and SIDS, where vulnerabilities are often more pronounced. By fostering collective action and accelerating progress in these regions, we can ensure that no one is left behind in the digital transformation journey. Strengthening ICT infrastructure resilience is not just a technical necessity; it is a strategic investment in a more equitable, prosperous, and sustainable future for all.

Bibliography

Alliance for Affordable Internet, “The cost of smartphones falls, but they remain unaffordable for billions around the world”, 31 August 2022. Available at https://a4ai.org/news/the-cost-of-smartphones-falls-but-they-remain-unaffordable-for-billions-around-the-world/.

Armita Satari, "Satellite disruption: how LEO and D2D are impacting telecoms", Telecoms.com, 8 March 2024. Available at https://www.telecoms.com/satellite/satellite-disruption-how-leo-and-d2d-are-impacting-telecoms.

Arndt Husar, Yoonee Jeong and John Garrity, "Cross-Sector Infrastructure Co-deployment: Closing Digital Connectivity Gaps through Collaboration and Sharing", Asian Development Bank Sustainable Development Working Paper Series No. 86, July 2023. Available at https://www.adb.org/publications/cross-sector-infrastructure-co-deployment.

Asian Development Bank, “ADB Approves $190 Million Loan to Upgrade Power Distribution System in Bengaluru", December 2020. Available at https://www.adb.org/news/adb-approves-190-million-loan-upgrade-power-distribution-system-bengaluru.

Broadband Commission, "Working Group Report on Smartphone Access: Strategies Towards Universal Smartphone Access", September 2022. Available at https://www.broadbandcommission.org/wp-content/uploads/dlm_uploads/2022/09/Strategies-Towards-Universal-Smartphone-Access-Report-.pdf.

Broadband Commission for Sustainable Development, "2025 Broadband Advocacy Target 2: Making Broadband Affordable". Available at https://www.broadbandcommission.org/advocacy-targets/2-affordability/

Benoit Vivier, "8 recommendations to get the most out of Public Warning Systems", European Emergency Number Association, 21 June 2022. Available at https://eena.org/blog/8-recommendations-to-get-the-most-out-of-public-warning-systems/

Budimir and others, "Communicating complex forecasts: An analysis of the approach in Nepal's flood early warning system", *Geoscience Communication*, vol. 3, No. 1 (2020). Available at https://gc.copernicus.org/articles/3/49/2020/

Dan York, "DNSSEC Validation in 2022: Africa Leads with Amazing Growth", Internet Society Pulse, 16 March 2023. Available at https://pulse.internetsociety.org/blog/dnssec-validation-in-2022-africa-leads-with-amazing-growth

Department of ICT, Government of Papua New Guinea, "Response to Public Consultation Discussion Paper - LEO/MEO Satellite Services and PNG", 12 September 2023. Available at https://www.nicta.gov.pg/cp-0-29/

Dinanath Bhandari, "Community-centred flood early warning system in Nepal", South Asia Nadi Sambad, 15 June 2021. Available at https://www.preventionweb.net/news/community-centred-flood-early-warning-system-nepal;

Eileen Yu, "DDoS attack revealed as cause of online service outage at public healthcare institutions", ZD Net, 5 November 2023. Available at https://www.zdnet.com/article/ddos-attack-revealed-as-cause-of-online-service-outage-at-public-healthcare-institutions/

Ericsson, "Fixed Wireless Access Outlook", 2024. Available at https://www.ericsson.com/en/reports-and-papers/mobility-report/dataforecasts/fwa-outlook

ESCAP, *Seizing the Moment: Targeting Transformative Disaster Risk Resilience – Asia-Pacific Disaster Report 2023* (Bangkok, 2023). Available at https://www.unescap.org/kp/2023/seizing-moment-targeting-transformative-disaster-risk-resilience

ESCAP, “e-Resilience Monitoring Dashboard”. Available at https://www.unescap.org/projects/e-resilience (accessed on 28 July 2024).

ESCAP, *Seizing the Moment: Targeting Transformative Disaster Risk Resilience – Asia-Pacific Disaster Report 2023* (Bangkok, 2023). Available at https://www.unescap.org/kp/2023/seizing-moment-targeting-transformative-disaster-risk-resilience.

ESCAP, *Seizing the Moment: Targeting Transformative Disaster Risk Resilience – Asia-Pacific Disaster Report 2023* (Bangkok, 2023). Available at https://www.unescap.org/kp/2023/seizing-moment-targeting-transformative-disaster-risk-resilience.

Gary Kim, "Mobile Market is Highly Concentrated and Always Will Be", Spectrum Futures, 26 October 2019. Available at https://spectrumfutures.org/mobile-market-is-highly-concentrated-and-always-will-be/.

[1] ITU, *Policy Brief: The Affordability of ICT Services 2023* (Geneva, 2024). Available at https://www.itu.int/en/ITU-D/Statistics/Documents/publications/prices2023/ICTPriceBrief2023.pdf.

GSMA, *Cell Broadcast for Early Warning Systems: A review of the technology and how to implement it* (London, 2023). Available at https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/wp-content/uploads/2023/11/Cell-Broadcast_R.pdf

GSMA Mobile Connectivity Index. Available at https://www.mobileconnectivityindex.com/index.html (accessed on 28 July 2024).

GSMA, *The State of Mobile Internet Connectivity Report 2023* (2023). Available at https://www.gsma.com/r/somic/.
ITU, "Digital Regulation Platform: The Infrastructure Sharing Imperative", 25 August 2022. Available at https://digitalregulation.org/the-infrastructure-sharing-imperative/.

GSMA, *The Mobile Gender Gap Report 2024* (2024); PTA, *Digital Gender Inclusion Strategy* (2024). Available at https://pta.gov.pk/category/digital-gender-inclusion-strategy-1520570539-2024-07-13

GSMA, "The Role of Digital and Mobile-Enabled Solutions in Addressing Climate Change", February 2021; GSMA, "Typhoon Rai Response: The role of the mobile industry", March 2022

IETF, "Selection and Operation of Secondary DNS Servers: RFC 2182 also known as BCP 16", July 1997. Available at https://datatracker.ietf.org/doc/rfc2182/.

Internet Society Pulse, "Internet Resilience". Available at https://pulse.internetsociety.org/resilience (accessed on 28 July 2024).

Internet Society, "Internet Exchange Points (IXPs)". Available at https://www.internetsociety.org/issues/ixps/ (accessed on 28 July 2024).

Inter-American Development Bank, *Digital transformation infrastructure sharing in Latin America and the Caribbean* (Washington, DC., 2020). Available at https://publications.iadb.org/en/digital-transformation-infrastructure-sharing-latin-america-and-caribbean

ITU, "Connect2Recover - Digital Infrastructure and Ecosystem Reinforcement Against COVID-19 in Asia-Pacific". Available at https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Pages/v2/RD%27s%20Corner/Project%20Pages/Connect2Recover---Digital-Infrastructure-and-Ecosystem-Reinforcement-Against-COVID-19-in-Asia-Pacific.aspx (accessed on 28 July 2024).

ITU, *Connect2Recover: A Methodology for Identifying Connectivity Gaps and Strengthening Resilience in the New Normal* (Geneva, 2021).

ITU, "Asia and the Pacific Regional Initiatives (2023–2025)". Available at https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Pages/v2/2023/ITU-Asia-and-the-Pacific-Regional-Initiatives-(2023–2025).aspx (accessed on 28 July 2024).

ITU Strategic Plan 2024–2027 at https://www.itu.int/en/council/planning/Pages/default.aspx

ITU, "Digital Regulation Platform: The Infrastructure Sharing Imperative", 25 August 2022. Available at https://digitalregulation.org/the-infrastructure-sharing-imperative/

ITU, *Measuring Digital Development: Facts and Figures 2023* (Geneva, 2023). Available at https://www.itu.int/itu-d/reports/statistics/facts-figures-2023/
ITU, Resolution 359 (REV.WRC-15): Consideration of regulatory provisions for updating and modernization of the Global Maritime Distress and Safety System. Available at https://www.itu.int/dms_pub/itu-r/oth/0c/0a/R0C0A00000C0008PDFE.pdf

ITU, Resolution 646 (REV.WRC-19): Public Protection and Disaster Relief. Available at https://www.itu.int/dms_pub/itu-r/oth/0C/0A/R0C0A00000F00133PDFE.pdf.

ITU, "ICT Prices". Available at https://www.itu.int/en/ITU-D/Statistics/Pages/ICTprices/default.aspx (accessed on 28 July 2024).

ITU, *Output Report on ITU-D Question 4/1: Economic policies and methods of determining the costs of services related to national telecommunication/ICT networks – Study period 2018–2021* (Geneva, 2021)
Available at https://digitalregulation.org/wp-content/uploads/ITU-D-Question-4-1-Final-Report-2021.pdf

ITU, "Recommendation ITU-T D.264: Shared uses of telecommunication infrastructure as possible methods for enhancing the efficiency of telecommunications", 2020. Available at https://www.itu.int/rec/T-REC-D.264-202004-I

ITU, *ITU Guidelines for National Emergency Telecommunication Plans* (Geneva, 2020).

ITU, "ITU-T Y.1271: Framework(s) on network requirements and capabilities to support emergency telecommunications over evolving circuit-switched and packet-switched networks", 2014. Available at https://www.itu.int/rec/T-REC-Y.1271-201407-I/en

ITU, "ITU-T Series L Supplement 35: Framework of disaster management for network resilience and recovery", 2017. Available at https://www.itu.int/rec/T-REC-L.Sup35-201706-I/en.

ITU, "Common Alerting Protocol and Call to Action". Available at https://www.itu.int/en/ITU-D/Emergency-Telecommunications/Pages/Common-Alerting-Protocol-and-Call-to-Action.aspx

ITU, *Digital Transformation and Early Warning Systems for Saving Lives: Background Paper* (Geneva, 2023). Available at https://www.itu.int/hub/publication/d-gen-digital-transfor-01-2023/.

ITU, *Policy Brief: The Affordability of ICT Services 2023* (Geneva, 2024). Available at https://www.itu.int/en/ITU-D/Statistics/Documents/publications/prices2023/ICTPriceBrief2023.pdf

ITU, "WSIS Stocktaking Success Stories 2024", Zero Draft, 7 May 2024. Available at https://www.itu.int/net4/wsis/forum/2024/Files/outcomes/draft/WSISStocktakingSuccessStories2024_Draft.pdf

ITU and World Bank, "Regulation of NGSO Satellite Constellations", Digital Regulation Platform, 28 March 2024. Available at https://digitalregulation.org/regulation-of-ngso-satellite-constellations/

ITU, "WSIS Stocktaking Special Report: The Republic of Korea's ICT Journey 2015–2023 Timeline", 2024. Available at https://www.itu.int/net4/wsis/forum/2024/Files/outcomes/draft/WSISStocktakingSpecialReport_ROKTimeline.pdf;

Joern Krause, "Non-Terrestrial Networks (NTN)", 14 May 2024. Available at https://www.3gpp.org/technologies/ntn-overview.

Jason Rainbow, "Lynk Global plans to go public to fund direct-to-smartphone satellites", Space News, 18 December 2023. Available at https://spacenews.com/lynk-global-plans-to-go-public-to-fund-direct-to-smartphone-satellites/; Jason Rainbow, "The promise of direct-to-device", Space News, 14 July 2023. Available at https://spacenews.com/the-promise-of-direct-to-device/

John Tanner, "Fiji consumer watchdog welcomes news of Starlink licences", 21 November 2023. Available at https://developingtelecoms.com/telecom-technology/satellite-communications-networks/15825-fiji-consumer-watchdog-welcomes-news-of-starlink-licences.html

John Garrity and Arndt Husar, "Digital Connectivity and Low Earth Orbit Satellite Constellations: Opportunities for Asia and the Pacific", Asian Development Bank Sustainable Development Working Paper Series No. 76, April 2021. Available at https://www.adb.org/publications/digital-connectivity-low-earth-orbit-satellite-opportunities.

Kim Arin, "South Korea's digital reputation dented by government network outage", The Korea Herald, 19 November 2023. Available at https://www.koreaherald.com/view.php?ud=20231119000136

Liam Pye and Lucy Pilgrim, "Palau National Communications Corporation: Bridging the Digital Divide", APAC Outlook, 3 June 2024. Available at https://www.apacoutlookmag.com/technology/palau-national-communications-corporation-bridging-the-digital-divide

Mahmudul Hasan, "Cyclone disrupts 10,000 telecom towers, millions out of service", The Daily Star, 27 May 2024. Available at https://www.thedailystar.net/business/news/cyclone-disrupts-10000-telecom-towers-millions-out-service-3620101.

NICTA, "Operator Licensing for the Provision of Low Earth Orbit Satellite Services in PNG", 21 June 2024. Available at https://www.nicta.gov.pg/cp-0-29/.

OECD, “Security of the Domain Name System (DNS): An Introduction for Policy Makers”, OECD Digital Economy Paper No. 331, October 2022. Available at https://www.oecd-ilibrary.org/docserver/285d7875-en.pdf?expires=1717732205&id=id&accname=guest&checksum=2F840B15349C99DCF5899AA21C65A75F

OECD, "Bridging Connectivity Divides", Digital Economy Papers No. 315, July 2021. Available at https://www.oecd-ilibrary.org/docserver/e38f5db7-en.pdf?expires=1721455447&id=id&accname=guest&checksum=6385451D30A3735C15C717620178BC37

Odisha State Disaster Management Authority, "Early Warning Dissemination System (EWDS)". Available at https://www.osdma.org/preparedness/early-warning-communications/ewds/(accessed on 28 July 2024)

People in Need, "Cambodia’s Early Warning System 1294

Robbie Mitchell, "Bangladesh Coping with Submarine Cable Outage Thanks to Indian Terrestrial Cables, Local Content Caches", Internet Society Pulse, 25 April 2024. Available at https://pulse.internetsociety.org/blog/bangladesh-coping-with-submarine-cable-outage-thanks-to-indian-terrestrial-cables-local-content-caches.

Samsung, "Samsung to Deploy the World’s First 3GPP Standard Based Public Safety LTE Solution in Korea" Press Release, 11 February 2016.

S&P Global, "Global 5G survey: Fixed wireless access, connected home lead consumer use cases", 26 October 2022. Available at https://www.spglobal.com/marketintelligence/en/news-insights/research/global-5g-survey-fixed-wireless-access-connected-home-lead-consumer-use-cases.

Telecom Review Asia Pacific, "Fixed Wireless Access Transforming Digital Connectivity in Asia", 2 February 2024. Available at https://www.telecomreviewasia.com/news/featured-articles/3939-fixed-wireless-access-transforming-digital-connectivity-in-asia

Telecom Review Asia Pacific, "Sustainable Practices in Data Center Operations in the Asia Pacific", 23 February 2024. Available at https://www.telecomreviewasia.com/news/featured-articles/4009-sustainable-practices-in-data-center-operations-in-the-asia-pacific

Telecom Review Asia Pacific, "DoT Explores Balloon and Drone Deployment to Ensure 5G Connectivity During Emergencies", 4 June 2024. Available at https://www.telecomreviewasia.com/telecomreviewasia.com/news/technology-news/4282-dot-explores-balloon-and-drone-deployment-to-ensure-5g-connectivity-during-emergencies

Telecom Review Asia Pacific, “MVNO Regulations and Market Entry Challenges in Asia-Pacific Countries", 19 April 2024. Available at https://telecomreviewasia.com/news/featured-articles/4161-mvno-regulations-and-market-entry-challenges-in-asia-pacific-countries.

The Critical Entities Resilience Directive (CER). Available at https://www.critical-entities-resilience-directive.com/ (accessed on 28 August 2024).

Tom Bateman, "Tonga is finally back online. Here's why it took 5 weeks to fix its volcano-damaged Internet cable", Euro News, 23 February 2022. Available at https://www.euronews.com/next/2022/02/23/tonga-is-finally-back-online-here-s-why-it-took-5-weeks-to-fix-its-volcano-damaged-interne

UNDRR, *The Midterm Review of the Implementation of the Sendai Framework for Disaster Risk Reduction 2015–2030: Regional Report for Asia-Pacific* (Geneva, 2023). Available at https://www.undrr.org/publication/regional-report-midterm-review-implementation-sendai-framework-disaster-risk-reduction

UNDRR, “Principles for Resilient Infrastructure”.

UNDRR, *The Midterm Review of the Implementation of the Sendai Framework for Disaster Risk Reduction 2015–2030: Regional Report for Asia-Pacific* (Geneva, 2023). Available at https://www.undrr.org/publication/regional-report-midterm-review-implementation-sendai-framework-disaster-risk-reduction.

UNDRR, *Global Status of Multi-Hazard Early Warning Systems 2023* (Geneva, 2023). Available at https://www.undrr.org/media/91954/download?startDownload=20240605.

UNDRR, *Words into Action: Engaging for Resilience in Support of the Sendai Framework for Disaster Risk Reduction 2015–2030* (Geneva, 2023). Available at https://www.undrr.org/words-into-action/guide-multi-hazard-early-warning

UNDRR, *GAR Special Report 2023: Mapping Resilience for the Sustainable Development Goals* (Geneva, 2023).

UNDRR, *Global Status of Multi-Hazard Early Warning Systems 2023* (Geneva, 2023). Available at https://www.undrr.org/media/91954/download?startDownload=20240605

UNDRR, *Words into Action: Engaging for Resilience in Support of the Sendai Framework for Disaster Risk Reduction 2015–2030* (Geneva, 2023). Available at https://www.undrr.org/words-into-action/guide-multi-hazard-early-warning

UNDRR, "Inclusive and Accessible Multi-Hazard Early Warning Systems: Learning from Women-Led Early Warning Systems in the Pacific", 2022.

United Nations, "Early Warnings for All". Available at https://www.un.org/en/climatechange/early-warnings-for-all

Web Foundation, "How expensive is a smartphone in different countries?" 7 October 2021. Available at https://webfoundation.org/2021/10/how-expensive-is-a-smartphone-in-different-countries/

WMO, "Nepal holds national consultation – Early Warnings for All and WITH All", 22 September 2023. Available at https://wmo.int/media/news/nepal-holds-national-consultation-early-warnings-all-and-all

World Bank, *Climate Change and Disaster Management*, Pacific Possible Background Paper No. 6 (Washington, DC, 2016). Available at https://hdl.handle.net/10986/28137

World Bank, *World Development Report 2021: Data for Better Lives* (Washington DC, 2021). Available at https://wdr2021.worldbank.org/.

World Bank, *Designing Inclusive, Accessible Early Warning Systems: Good Practices and Entry Points* (Washington, DC, 2023). Available at https://www.preventionweb.net/publication/designing-inclusive-accessible-early-warning-systems-good-practices-and-entry-points.

World Economic Forum, *The Global Risk Report 2024*, 19th Edition (Geneva, 2024). Available at https://www.weforum.org/publications/global-risks-report-2024/

World Economic Forum, *The Global Risk Report 2024*, 19th Edition (Geneva, 2024). Available at https://www.weforum.org/publications/global-risks-report-2024/.